HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

VÉDETT TÁRGYALÓ KIALAKÍTÁSÁNAK ALAPVETŐ BIZTONSÁGI KÉRDÉSEI

BASIC SAFETY ISSUES OF THE DESIGN OF PROTECTED MEETING ROOMS

BRÉDA Gábor

(ORCID ID:0000-0001-7868-6637)

bredagabi@freemail.hu

Absztrakt

Napjainkban az információ birtoklása és annak megfelelő helyen és időben való felhasználása egyértelmű előnyt jelent a birtokosa számára. Az információk megszerzése és továbbítása nem jelent akadályt, mint az elmúlt századokban. Mivel az adat és az információ digitális rögzítése, valamint áramoltatása az infokommunikációs rendszerekben a technológiák tervezett alapfunkciója nehéz gátat szabni az információk rendszerbe történő szelektív bekerülésének és így azok terjedésének. Jelen korunkban fokozottabb igény merülhet fel olyan személyes kommunikáció megvalósítására, ahol a megbeszélés tárgya biztosítható módon kizárólag a jelenlévő felek közt hangzik el és az elhangzott információ a kommunikációs környezeten belül marad, harmadik fél vagy információszerző technológia teljes kizárásával. A téma szempontjából az ilyen "bizalmi" kommunikációra alkalmas környezet megvalósítása a cél. Megvizsgálom a kommunikációból eredő fizikai jelenségeket és áttekintem egy védett tárgyaló alapvető védelmének elvi követelményeit saját megközelítés alapján.

Kulcsszavak: *információ védelem, védett tárgyaló, biztonsági rés, objektumvédelem, védett helyiség*

Abstract

In the rushing world of today it is an evident advantage to possess information and to use it in an adequate time and place. The acquisition and transmission of information is not as much of an obstacle as it used to be in the past centuries. As the digital record and transmission of data and information are the basic functions of info-communication devices, it is hard to obstacle information from the selective inclusion in the system, and therefore, it is spreading. In the history of mankind, the demand has never been as high for the realization of oral, face-to-face communication, in which the participants are undoubtedly the only ones in possession of the spoken information, that is only stored in the memory of the participants. The aim is the realization of an environment that is suitable for confidential communication. The problem is that today in Hungary there are no universal regulations for the design or the organization of the protection efficiency control for protected meeting rooms that would give precise definitions for the design and operation. Looking into the subject, I will review the conceptual requirements for the basic placement and protection of such facilities, based on my approach.

Keywords: *information protection, protected meeting room, security gap, facility protection, protected area*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.14.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.23.

BEVEZETÉS

Az adat, mint az információ legkisebb egysége általában valamilyen adathordozón, rögzített formában áll rendelkezésre. Tulajdonképpen mindegy, hogy hagyományos papír alapú, vagy digitális adathordozóról van szó, kézzel fogható meghatározható méretű tárgyról beszélünk, amely a méreteitől függően a biztonságtechnika és a kriptográfia módszereivel, bevált szisztémák alkalmazásával jól védhető az illetéktelen hozzáférés elől. Az adatok nyersen, önmagukban nem feltétlenül fejeznek ki értelmezhető hasznos információt. Ahhoz, hogy információvá váljanak, fel kell dolgozni azokat [1]. Az adatfeldolgozás napjainkban szinte kizárólag számítástechnikai eszközökkel történik, és a feldolgozást követően informatikai eszközön rögzül. Az informatikai eszközök és hálózatok védelmével, mint az információs társadalom alapvető információmegosztói környezetével külön fejlesztő és kutatócsoportok, valamint nemzeti és nemzetközi szervezetek foglalkoznak, hogy a tárolt és továbbított digitális tartalmak az adat és információgazdák kívánalmainak megfelelően biztonságban juthassanak el az arra jogosult felhasználók közé. Jelen kutatás elsőként az ember-ember közvetlen kommunikációs interakció során megjelenő fizikai jelenségeket tekinti át és az esetlegesen szükséges megjelenítő interfészek hordozta információszivárgási csatornákat vázolja fel. Ezt követően alapmodellt vázol fel egy védett helyiség, tárgyaló kialakítására, majd egy elképzelt kialakítást mutat be áttekintve a felhasználható biztonságtechnikai eszközök struktúráját. Problémát jelent, hogy Magyarországon információbiztonsági szempontból védett tárgyalók kialakítására, tervezési irányelveire, valamint a védelmi hatékonyságának ellenőrzésére egységesített előírás nem fellelhető, amely pontos meghatározásokat adhatna egy ilyen helyiség kialakítására és üzemeltetésére. Itt kell megjegyezni, hogy a fizikai adathordozók védelme, a rendszereken történő tárolás és továbbítás, mint alapvető védeni kívánt információbiztonsági elemek, törvényi szabályozással, kialakult védelmi megoldásokkal és folyamatos fejlesztéssekkel jól ellátott területnek bizonyulnak [2], [3]. Azonban az adat és információbiztonság nem csak műszaki tartalmak implementálásából álló folyamat, mivel a biztonság megteremtésének másik összetevő eleme maga az ember. Jelen sorok terjedelmi lehetőségei nem engedik meg az emberi tényező információbiztonsági vonulatainak kifejtését, azonban mint potenciális információbiztonsági kockázat, mégis megemlítem mivel az információbiztonság az ember biztonságtudatos viselkedése nélkül nehezen megvalósítható védelmi folyamat [4],[5].

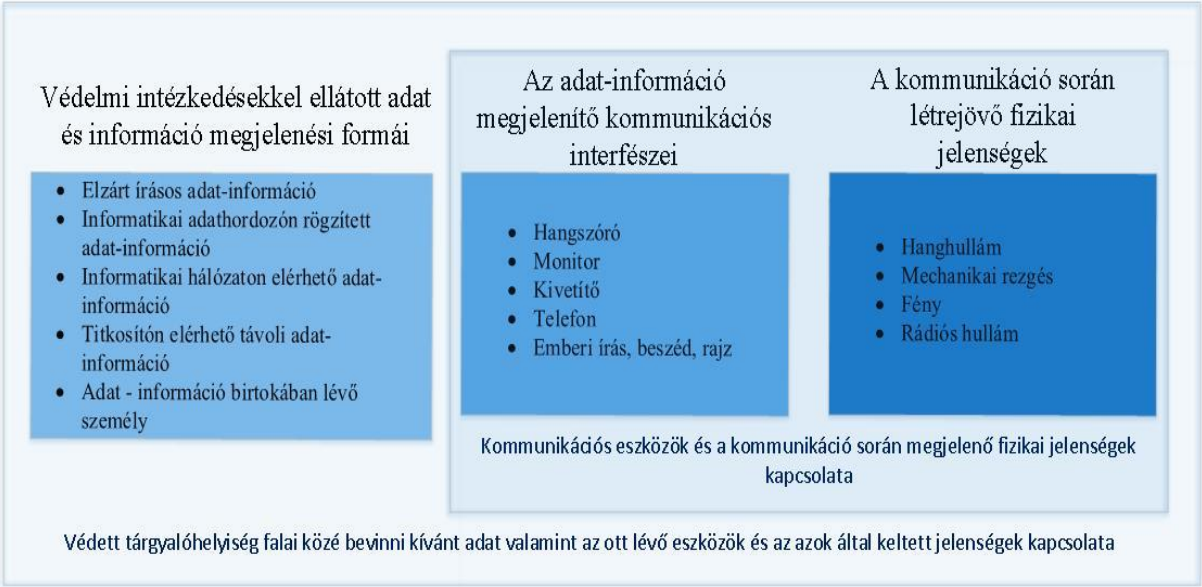
A MEGJELENŐ INFORMÁCIÓBIZTONSÁGI RÉS

Ahhoz, hogy az ember számára értelmezhető legyen egy adathordozón rögzített információ, és annak logikai kapcsolatából tudást szerezhessen, valamilyen kommunikációra van szüksége, vagyis meg kell, hogy ismerje azt [1]. A megismerésnek fő érzékszerveink adhatnak lehetőséget, a hallás és a látás. A hordozón lévő információnak az ember számára értelmezhető formában történő megjelenítése a megjelenés kezdeti pillanatától a végéig az átviteli láncban olyan újabb elemeket hoz létre, amelyeknek az illetéktelenek előli védelme megoldandó feladat. A rögzített információk megismeréséhez interfészek kellenek, az átvitelhez alkalmas minőségben. Hang alapú átvitel esetén az emberi kommunikáció hangja vagy a médiatartalmat lejátszó berendezés hangszórója által keltett hang rezgése.

Vizuális átvitel alkalmával, az írásjelekkel ellátott papír vagy a különböző monitorok, kivetítők információ tartalmú fénye. A láncban megjelenik több olyan fizikai jelenség, amelyeknek a hatását információbiztonsági szempontból meg kell vizsgálni és elvi információbiztonsági rés fennállása esetén a lehetséges csatorna elzárása érdekében védelmi megoldásokat kell kialakítani.

A védelmi egyenszilárdság elvét szem előtt tartva, ha egy, az adathordozók és informatikai rendszerek magas szintű védelmével felszerelt környezetben mindent megteszünk az

információbiztonság megvalósítása érdekében, akkor az objektumvédelem a fizikai védelem és az informatikai elemek védelme mellett, nem hagyható figyelmen kívül annak a speciális környezetnek az információbiztonságilag megfelelő kialakítása sem, ahol azok kikerülnek a védett rendszerből és tisztán emberközeli formában jelenek meg. Osztályozhatjuk a megjelenő és védeni kívánt fizikai jelenségeket direkt és indirekt módon megjelenőnek. Direkt módon a hang a levegő által szerte terjed egy helyiség falai közt és a beszéd erősségétől függően megrezgeti a bent lévők dobhártyáját és az összes közeli tárgy felületét. A vizuális megismerés esetén a fény fotonjai az írott adathordozóról visszaverődés útján, monitor, kivetítő esetén fény emittáció útján kerülnek a helyiség falai közé, majd a levegőn áthaladva a résztvevők szemébe, valamint a megjelenítő eszköz teljes betekintési szögének terébe. Indirekt módon előálló jelenségek az alkalmazott berendezések működéséből fakadó információ tartalmú mágneses kisugárzások, a hang által megrezgetett tárgyakban terjedő további rezgések, valamint a fény tükröződése során létrejövő szórt nyalábok. Miután az emberhez eljutnak az említett fizikai jelenségek, és ha hallják és értik az adott nyelvet, valamint látják és értelmezik az írásjeleket és ábrákat, részesei-tudói lesznek az eddig szigorú műszaki követelményekkel és megoldásokkal védett adathordozókon lévő információknak. A megjelenő probléma elemeit összegezve az 1. ábrán láthatjuk.



1. ábra A kommunikáció védett és megjelenő elemei [saját ábra]]

Az információbiztonsági probléma ott jelentkezik, hogy az emberi találékonyság és a műszaki kereskedelem adta kínálat segítségével lehetőség adódott olyan érzékelő, rögzítő célberendezések elterjedésére, amellyel autonóm módon megfelelő minőségben lehet akusztikus rezgést, valamint vizuális eseményeket érzékelni és rögzíteni. A legegyszerűbb példát véve, a legtöbb mobiltelefon készülék az alapfunkcióit tekintve a telefonálás mellett az akusztikus és vizuális rögzítés megvalósítására lett kifejlesztve, amelyen a rögzített médiatartalom gombnyomásra, vagy távoli hozzáférés engedélyezésével a világ bármely táján elérhetővé válik egy másik fogadó berendezés számára a telekommunikációs hálózatot, mint átviteli utat használva.

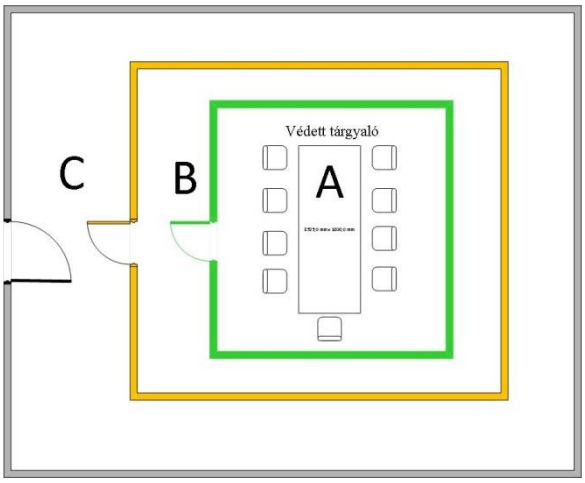
Továbbá a rádiótechnika és a számítástechnika rohamos fejlődésének köszönhetően távolról detektálhatóvá és értelmezhetővé váltak az elektromos kommunikációs berendezések működéséből fakadó jelek is [6], [11]. Az előbbi tények kívánják meg azt a megközelítést, amely szerint az érzékeny adatokból nyert szenzitív információkat olyan helyiségben kell feldolgozni, olyan tárgyalóban kell megosztani az arra jogosultakkal, amelyben biztosított az emberi kommunikációs formák során megjelenő direkt és indirekt információ védelme. A

kommunikáció különböző formáiból eredő és a járulékosan megjelenő információt hordozó fizikai jelenségek a védett tér körülhatároló falainak síkjában meg kell, hogy álljanak. A védelmet és annak fenntartását arányos határok között, a ma használatban lévő vagyonvédelmi és a villamos méréstechnikai, elektrotechnikai eszközökkel biztosítható formában szavatolhatóan kell kialakítani. A szóban forgó helyiség kialakítása során elsőként az alkalmas helyszín kijelölésének elvi megközelítését kell körüljárnunk, mivel a későbbi védelmi megoldások alkalmazhatóságát nagymértékben befolyásolja a jó helyszín kiválasztása [6], [12].

AZ OBJEKTUMVÉDELEM ÉS A VÉDETT HELYISÉG KIALAKÍTÁSA

Egy védett helyiség, esetünkben egy védett tárgyaló kialakításának a biztonságszervezése védelmi erőforrások igénybevétele nélkül aligha elképzelhető [7]. Az erőforrások növelésével a védelmi szint mértéke természetesen növelhető. A védelmi szint eléréséhez, meg kell határozni azt az arányt, ami a védeni kívánt információ értékét, és a védelem kialakításával és fenntartásával járó költségeket szembeállítja. Abban az esetben ha megállapítást nyer a védelem kialakításának relevanciája, akkor a következő elgondolások támpontot nyújthatnak egy a szóban forgó helyiség kialakításához. Az erőforrások, típusuk alapján lehetnek technikai védelmi eszközök és élőerős megoldások. A technikai úton megvalósított védelem egyik alapeleme a mechanikai védelem. Mechanikai védelemnek tekinthető, minden olyan eszköz és technológia, valamint gépészeti és építészeti megoldás, amely a vagyon létezését vagy működését veszéllyel fenyegető szándékos ellenérdekű, jogellenes cselekményt késleltet vagy megakadályoz [7], [8]. A mechanikai védelem első lépcsője a kültéri védelem kialakítása, amely egy épület, vagy épületkomplexum elhelyezéséül szolgáló terület határát jelöli ki, pontosan meghatározva azt a vonalat, amely idegen által megközelítve még nem von maga után védelmi intézkedés, illetve a védelem kialakításának szempontjából az a határterület, ahonnan kezdve az arányosság mértékével ki kell alakítani olyan megoldásokat, amelyek a védeni kívánt objektum, épület biztonságát szolgálják. A kültéri védelem elemei általában kerítések, kapuk, ritkábban árkok és sáncok, azonban nagyvárosi környezetben gyakran előfordul, hogy az épülethatároló homlokzati falazat a kültéri mechanikus védelem elsődleges eleme és egyúttal a védeni kívánt objektum maga. Egy folyamatos üzemű objektum védelme napjainkban elképzelhetetlen élőerős őrszolgálat működése nélkül. A külső határt kijelölő eszközrendszer megteremtésével fel kell állítani egy őrszolgálati egységet, aminek alapfeladata a kijelölt terület rendjének a szemmel tartása, valamint az incidensek észlelése és kezelése. Az őrszolgálatnak több főből kell, hogy álljon, és ez a védeni kívánt objektum méreteivel, a védeni kívánt értékek nagyságával és a belépési pontjainak számával arányosan kell, hogy növekedjen. Az őrszolgálatok munkáját gyakran segítik videó kamerás megfigyelő rendszerek, amelyek megfelelő telepítés esetén a teljes objektum területe átláthatóvá válik [7], [8], [9], [10].

A kültéri objektumvédelem megalkotása során, használatosak különböző elektronikus vagyonvédelmi rendszerek is, amelyek kimondottan külső mozgás és átlépés távérzékelése megvalósítására lettek kifejlesztve. A megfigyelő és jelző eszközök kombinációja révén fokozható a külső tér behatolókkal szembeni védelmi hatékonysága. Egy a védett helyiség kialakítása szempontjából fontos intézkedés, hogy a védeni kívánt helyiség elhelyezését körülvevő épületet, ellenőrizetlen formában ne közelíthesse meg senki. Az élőerős objektumvédelem feladata, összetett módon nem csak a külső részek ellenőrzése lehet, hanem a belső épületrészek folyamatos felügyelete is, mivel komplexen módon át kell látni a teljes védeni kívánt területet. A téma szempontjából véleményem szerint itt egy speciális elhelyezési és vagyonvédelmi szemlélet követelményét kell kialakítani. A védett tárgyaló héjmodellben kell, hogy kialakítva legyen. Az objektumvédelmi erőknek teljes körüljárhatóságot kell biztosítani a védeni kívánt helyiség külső határoló falai körül, mind horizontális, mind vertikális irányban, meg kell akadályozni a védett szoba közvetlen falazata mellé jutást. Zónákat kell kialakítani, amely a 2. számú ábrán "A, B, C" betűkkel lett jelölve.



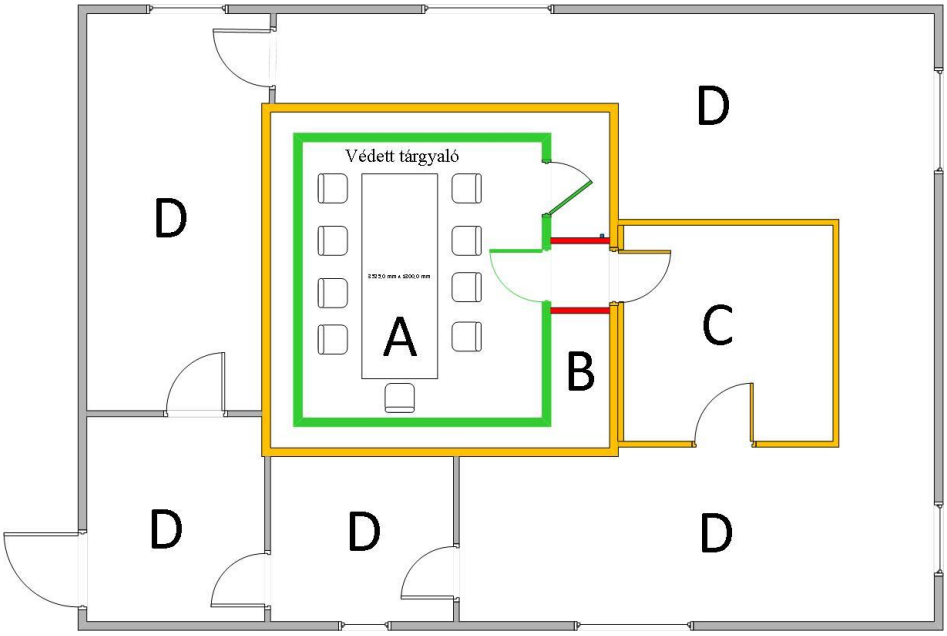
2. ábra A védett tárgyaló elvi kialakításának alapmodellje [saját ábra]

Az "A" zóna a védett tárgyaló, a "B" zóna egy köztes védett tér valamint a "C" zóna a védett tárgyalót körülvevő befoglaló épületrész. A speciális környezet az elképzelésem szerint az "A" és "B" zónák határoló falazata. Az általános objektum őrség csak a külső "C" jelű zónát közelítheti meg, léphet be oda, amelynek a területén a teljes területet lefedő videó rögzítővel ellátott és elektronikus vagyonvédelmi eszközökkel biztosítható külön riasztási zónaként kezelhető védelmi réteget kell kialakítani. Az átlépési pontokat a jogosultságok meghatározása mellett beléptető rendszerrel kell biztosítani. Az egyik különleges intézkedés az, hogy az összes az "A, B, C" részekre csak olyan, a védett tárgyaló üzemeltetését ellátó személyek léphetnek be, akik munkájuk során a védett tárgyaló sértetlenségét biztosítják. A "C" és "A" részekre a "B" szakaszon átvezető nyílászárókon keresztül a tárgyalásra érkező személyek léphetnek be, különleges beléptetési protokoll elvégzését követően. Objektumvédelmi szempontból a védett helyiségnek olyan ellenőrzött objektumrésznek kell lennie, amely folyamatos üzemű védelemmel rendelkezik és a karbantartási időszakon kívül bármikor használható szenzitív megbeszélések lefolytatására. [3], [10]

A téma tárgyául választott speciális helyiség kivitelezését, mint minden különleges építmény megvalósítását, az elhelyezés pontos megjelölésével kell kezdeni a különleges későbbi igények szem előtt tartásával. A tárgyaló kiviteli helyszínének elvi és fizikai megvalósítási kritériumoknak kell, hogy megfeleljen. Elvi igény, hogy olyan épületrészt kell keresnünk, ahol a felhasználni kívánt terület teljes tulajdonjogi joggal bír a birtokos irányába, és ott a teljes rendelkezésre állás, a körüljárhatóság, a szemrevételezés, a műszeres vizsgálat lehetősége bármely időpillanatban szavatolt formában megvalósítható legyen, például a 2. ábra "C" területének külső határoló falazata is. Az olyan terület, amely csak részben körüljárható, esetleg közterülettel, idegen tulajdonú szomszéd épülettel közös fallal rendelkezik, nem megoldható a teljes fizikai körüljárás valamint az ellenőrizhetőség követelménye, idegen személy által bármikor elérhetővé válik a körülhatároló falazat egy része, az a terület, helyiség véleményem szerint nem alkalmas a tárgybeli létesítmény megvalósítására. Fizikai igény az olyan méret és kiterjedés, amely lehetővé teszi a kialakítani kívánt helyiség megfelelő számú befogadóképességét valamint a járulékos védelmi infrastruktúra kialakítási igényeinek is megfelel.

Végeredményben, olyan héjmodell szerkezetű helyiség megvalósítása a cél, amely mind a védelmi infrastruktúráját tekintve, mind építészeti kialakítását megteremtve (doboz a dobozban) többlépcsős védelmi modellt alkot. Ez fizikailag és építészetileg azt jelentheti, hogy a befogadó helyiségnek a külső határoló falai, valamint födémje és padozata jóval nagyobb kiterjedést igényel, mint a megvalósítani kívánt védett szoba mérete. Olyan környezetet kell keresnünk vagy tervezzünk, ahol belső, épületrészekkel körülhatárolva tudjuk elhelyezni a

védeni kívánt helyiségünket, vagy föld alatt elhelyezett szobát tudunk kiépíteni a kívánalmaknak megfelelően.
Elképzelésem szerint az ilyen elhelyezésű térrészben lehet a téma szempontjából megfelelő biztonságos terület kialakítani. Egy megvalósítási elképzelést szemléltet a 3. ábra.



3. ábra Egy védett tárgyaló lehetséges gyakorlati kialakítása [saját ábra]

A VÉDETT HELYISÉG VAGYONVÉDELEMI RENDSZEREI

Eddig a pontig a védett helyiségünk külső védelmének és elhelyezésének a főbb szempontjait tekinthettük át. A következőekben áttekintem az alkalmazható elektronikus vagyonvédelmi eszközök rendszerét. Egy ellentmondás vetődik fel, mivel egyfelől egy védett tárgyalót mindenképpen el kell látni elektronikus vagyonvédelmi rendszerrel azonban másfelől véleményem szerint egy védett tárgyaló helyiségben korlátozni kell az alkalmazott elektronikus berendezések számát. Ha ha mód van rá, el kell kerülni azok helyiségen belüli alkalmazását.
Amennyiben a fent említett dupla körülhatároló szerkezettel rendelkező védett terünk külső körülhatároló falainak határáig az objektumvédelmi rendszer behatolás elleni védelme kialakítottnak tekinthető, akkor eljutunk addig a szintig, hogy biztosítanunk kell a különleges az ábrákon köztes "B" és belső "A" a tárgyalás lebonyolítására létrehozott területek állandó felügyeletét és érintetlenségét. Amennyiben a védett helyiségünk önállóan, egy épület középső falakkal határolt részén helyezkedik el a fent részletezett módon, úgy biztosíthatóvá válik a befoglaló falak, a padozat és a mennyezet épségének felügyelete. Véleményem szerint a belső védeni kívánt területek védelmi rendszereit a védett helyiségünk környezetében, az átfogó objektumvédelemtől elszeparáltan, csak a tárgyaló kezelőszemélyzete által elérhető zónába javasolt telepíteni, átjelző lehetőséggel az átfogó teljes objektumvédelem irányába.
A 3. ábra "A, B, C" részeit el kell látnunk elektronikus vagyonvédelmi jelzőrendszer elemekkel úgy, hogy a "C" és "B" részek körülhatároló szerkezeti elemei "D" irányból érkező megbontás ellen védve legyenek. A vagyonvédelmi eszközök csak a külső "D" épületrészek felé néző falakon lehetnek elhelyezve. Az "A" jelű tárgyaló falazata a falazó anyagon kívül semmilyen más anyagot ne tartalmazzon, se rászerelve, se átfúrva, se beleépítve. Ez meglehetősen szigorú kompromisszumnak látszik, azonban így szavatolható a tárgyaló külső irányból való sérthetetlenségének biztosítása.

A külső 3. ábra "B" és "C" részek közötti falainak megbontás, megfúrás tényének detektálása céljából, érdemes jelző rendszert kiépíteni. Megoldás lehet a vezető szálakkal szőtt háló, amely megbontást detektáló elem. A fal szerkezetébe integrálva a vezető szál szakadása révén biztosíthatja a fal megbontása estén a jelzés generálását. Másik érzékelő megoldás az akusztikus fúrás érzékelő, amely a falban a fúró által keltett hang hatására indít riasztást.

Azon túl, hogy a védett helyiség üzemeltetésével foglakozó személyek bármely időpillanatban fizikailag ellenőrizhetik a védett helyiség teljes körülhatároló falazatát, a köztes "B" jelölésű fal külső és belső oldalán, 24 órás rögzítővel ellátott videó megfigyelőrendszerrel javasolt biztosítani az állandó felügyeletet a teljes objektumvédelmi rendszeréhez hasonlóan. A videokamerás megfigyelőrendszer oly módon kell, hogy kialakítva legyen, hogy a védett helyiség és a külső részek köztes falazatának terét is figyeli, és ott esemény hatására riasztást generál. Továbbá a biztonság fokozása érdekében, egy az előzőektől független elektronikus riasztórendszert kell kialakítani a vagyonvédelemben szokásos érzékelő elemek felhasználásával, önálló védett zónát, zónákat létrehozva.

A fizikai védelem kialakításának további speciális eleme a nyílászáró, amely a védett tárgyaló előterébe, és a tárgyalóba enged bebocsájtást. Az ajtóknak mechanikailag és információbiztonságilag is egységes egyenszilárdságú felületet kell, hogy alkossanak a határoló falakkal. Mind fizikai behatolás ellen kell, hogy védjenek, mind akusztikusan kell, hogy csillapítsanak. A riasztórendszer számára jelet kell, hogy szolgáltassanak az állapotukat illetően. A 3. ábra "C" helyiségébe "D" irányából történő belépésre olyan nyílászáró beépítése lehet a követelmény, amely viszonylag nagy átjutási idővel rendelkezik és megtalálható rajta minden olyan elem, amely jelzi az átjutás kísérletét és tényét. Továbbá mint egyetlen belépési pont a védett tér irányába, követelmény egy beléptető rendszer kialakítása is, amely rendszer a belépési jogosultságok pontos meghatározása mellett regisztrálja az áthaladó forgalmat. Itt elképzelhető a kialakítástól függően bármilyen elvű beléptető megoldás, a tudás alapú rendszerektől kezdve a birtok alapú rendszereken át a korszerű biometrikus rendszerek felhasználásáig. A 3. ábra "C" helyiségéből "A" helyiségébe vezető nyílászárója úgy képzelhető el, hogy két olyan ajtó kerül egymás mögé beépítésre, amelyek egymást nem akadályozzák a működésben és a funkciókat elosztva teljesítik az előírt fizikai és információbiztonsági kívánalmakat [7], [8], [10], [11].

A leírt megközelítések alapján a védeni kívánt helyiség közvetlen külső környezete csak regisztrált és rögzített módon közelíthető meg, és a határoló felületeit érő behatások naplózást generáló eseményt idéznek elő.

KÖVETKEZTETÉSEK

Jelen cikk soraiban, megahatározásra került az alapprobléma, amely a védett tárgyalók információbiztonsági kihívását jelenti. A technológia oly mértékben fejlődött, hogy az információ az emberi érzékszervek számára értelmezhető formában történő megjelenítése során, nem csupán a megjelenés helyszínén, de távolabbi térrészekben is érzékelhető és rögzíthető formában elérhetővé vált. A vezeték nélküli telekommunikáció és annak eszközei, fokozzák az információszivárgási rés megjelenésének kockázatát. Egy védett tárgyaló kialakítása során, minden olyan információszivárgási kockázati tényezőt ki kell zárni, amelynek a megvalósítása az információk védelmi értékével arányos módon megtehető. A legkézenfekvőbb módja egy ilyen helyiség kialakításának a körbezárás valamint a szeparált elhelyezés. Amennyiben a külvilág felől ellenőrzötten megközelíthető, biztosított helyszínen alakítunk ki védett tárgyalót, úgy jó eséllyel csökkenthetjük az információszivárgás kockázatát. Az elhelyezést követően a védett helyiség többlépcsős védelmét kialakítva a biztonság technika és a vagyonvédelem elemeivel biztosíthatjuk egy védett tárgyaló kialakításának alapfeltételeit.

Az objektumbiztonság megteremtését követően kiépíthetőek azok az elvi és műszaki intézkedések, amelyek szavatolhatják a létre hozni kívánt védett tárgyaló információbiztonsági szempontból való megfelelőségét.

FELHASZNÁLT IRODALOM

[1] ACKOFF, R. L., (1989): "From Data to Wisdom", Journal of Applies Systems Analysis, Volume 16, pp. 3-9.

[2] KURIS Z.: A komplex információvédelem új irányai a nemzeti minősített adatok védelmével összefüggésben, Hadmérnök, 2010 december ; V. évfolyam 4. szám. http://hadmernok.hu/2010_4_kuris.pdf (2017.január 06)

[3] HAIG ZS.: Az információbiztonság komplex értelmezése, ZMNE http://hadmernok.hu/kulonszamok/robothadviseles6/haig_rw6.pdf (letöltve: 2017.01.06)

[4] LAZÁNYI K., (2015): A biztonsági kultúra; TAYLOR Gazdálkodás- és szervezéstudományi folyóirat 2015. 1-2 szám;Szeged 2015, p.398-405 http://vikek.hu/wpcontent/uploads/2015/10/TAYLOR_2015-nyomdai.pdf (2017.január 06)

[5] LAZÁNYI K., (2016): A biztonsági kultúra szerepe a vezetői döntések támogatásában; TAYLOR Gazdálkodás- és szervezéstudományi folyóirat 2016. 1. szám; Szeged 2016, p. 143-150 http://vikek.hu/wpcontent/uploads/2016/05/Taylor2016.1.sz%C3%A1mNo22.pdf (2017. január 06)

[6] VÁNYA L.; Zrínyi Miklós Nemzetvédelmi Egyetem, Az elektronikai hadviselés eszközeinek,rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre, Doktori (PhD) értekezés, 2001. http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2003/vanya_laszlo.pdf (letöltve: 2017.01.06)

[7] BEREK L.: Biztonságtechnika, NKE, Budapest, 2014. http://real.mtak.hu/19709/1/biztonsagtechnika.original.pdf (letöltve: 2017.01.06)

[8] BEREK L., BEREK T., BEREK L.: Személy és vagyonbiztonság, ÓE, Budapest, 2016. ISBN 978-615-5460-94-4 http://asp01.ex-lh.hu:80/R/-?func=dbin-jump-full&object_id=23873&silo_library=GEN01 (letöltve: 2017.01.06)

[9] BOROS B., Et. al.: Rendészet, vagyonvédelem; BME Mérnöktovábbképző Intézet 1997; ISSN 08653313,ISBN963-431-797-9ö,801-0 TANENBAUM, A.S.: *Számítógép hálózatok*; Panem 1998.

[10] BEREK T.: ABV (CBRN) analitikai laboratórium beléptető rendszere a biztonságos üzemeltetés szolgálatában, Hadmérnök, VI. Évfolyam 2. szám, 2011/2, ISSN1788-1919, http://www.hadmernok.hu/2011_2_berek.pdf (letöltve: 2017.01.06)

[11] *A Nemzeti Biztonsági Felügyelet feladatairól és az elektromágneses kisugárzás elleni védettség minősítéséről elérhető információ az interneten*:
http://www.nbf.hu/tempestmer.html
(letöltve: 2017.01.06)

[12] *MIL-STD-461E; Department of Defense Interface Standard*
http://www.chassis-plans.com/PDF/MIL-STD-461E.pdf
(letöltve: 2018.01.06)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

TŰZVÉDELMI ESZKÖZÖK OPTIMÁLIS ELHELYEZÉSÉNEK ANTROPOMETRIAI MEGHATÁROZÁSA

ANTHROPOMETRIC DETERMINATION OF THE OPTIMAL LOCATION OF THE FIRE PROTECTION EQUIPMENT

HERCZEG Gergely

(ORCID 0000-0001-9633-5152)

herczeggergely@gmail.com

Absztrakt

A tűzvédelmi eszközök (pl. tűzoltó készülékek, tűzcsapok, kézi jelzésadók stb.) könnyű, gyors és hatékony használatának feltétele a hozzáférhetőség. A tűzvédelmi eszközök hozzáférhetősége a kialakult tüzek korai eloltását, a késedelem nélküli riasztást és ezáltal az emberi élet védelmét szolgálja. Az optimális hozzáférhetőséghez az eszköz elhelyezését célszerű a felhasználó populáció antropometriai adataihoz igazítani. Bemutatom és elemzem a tűzvédelmi eszközök elhelyezésekor releváns antropometriai adatokat, valamint ezek felhasználásával meghatározom egyes tűzvédelmi eszközök optimális elhelyezési paramétereit.

Kulcsszavak: *antropometriai illesztés, tűzvédelmi eszközök, tűzmegelőzés; használati szabályok*

Abstract

The accessibility is the criterion of the easy, quick and effective use of the fire protection equipment (e.g. fire extinguishers, fire hydrants, manual call points, etc.). The accessibility of the fire protection equipment allows to extinguish fires in their early stage, alarm without delay and thereby protecting people's life. For the optimal accessibility it is expedient to adjust the location of the equipment to the user's population's anthropometric data. I present and analyse the anthropometric data relevant for placement of the fire protection equipment, I define using them the optimal parameters of the location of the fire protection equipment.

Keywords: *anthropometric accommodation, fire protection equipment, fire prevention, rules of use in fire protection*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.11.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.24.

BEVEZETÉS

A hazai és nemzetközi szakirodalom nem bővelkedik a tűzvédelmi eszközök hozzáférhetőségére és azok antropometriai illesztésére vonatkozó közleményekben. Antropometriai és ergonómiai témában több mű is született mind hazai, mind nemzetközi viszonylatban, azonban azok vagy csupán szűk szakterületükkel foglalkoznak, vagy vizsgálják a tágabban értelmezett szakterületet is, azonban nem terjednek ki kifejezetten tűzvédelmi eszközök és az ember közötti kapcsolatra, a tűzvédelmi eszközök könnyű hozzáférhetőségére és gyors használata feltételeinek megteremtésére. Szabványok és szabványszerű dokumentumok foglalkoznak e témával [1] [2].

Fentiek miatt ezen cikk hiánypótló lehet abban a tekintetben, hogy igyekszik feltárni azon antropometriai adatokat, melyek a tűzvédelmi eszközök könnyű és gyors hozzáférhetőségéhez járulhatnak hozzá. Törekedtem arra, hogy a hazai és nemzetközi szakirodalomban fellelhető adatok, módszerek és elvek alapján olyan javaslatokat dolgozzak ki, melyek segítenek megállapítani a tűzoltó készülékek vagy egyéb tűzvédelmi eszközök hozzáférhetőségéhez szükséges paramétereket.

Kutatásom módszere a szakirodalom feldolgozása és elemzése, mely kiterjed a meglévő szabványokra és szabványszerű dokumentumokra is.

Az általam fellelt vonatkozó hazai és nemzetközi szakirodalom egyrészt általánosságban tartalmazza az emberi test méreteivel kapcsolatos adatokat [3], másrészt olyan konkrét javaslatokat tartalmaznak, melyek a műszaki élet más területein hasznosíthatóak [4].

Eddigi kutatások az antropometriai adatokat felhasználták, és azokból kiindulva ergonómiai eredmények születtek, de azok elsősorban az ember, a gép és környezete közötti kölcsönhatásokat vizsgálták, azokat igyekeztek optimalizálni. Ezen kutatások nem térnek ki olyan ritkán előforduló, esetleges, alkalomszerű tevékenységekre, mint például a tűzoltó készülékek használata, tűzjelző kézi jelzésadók működtetése, fali tűzcsapok, vagy egyéb tűzvédelmi eszközök használata.

Az ergonómia egyik főbb területe a fizikai ergonómia, mely a fizikai tevékenység és az emberi test felépítésével, annak méreteivel, biomechanikai és fizikai jellemzőivel foglalkozik [5].

Az antropometria az emberi test méreteivel foglalkozó tudomány, mely a test méreteit, formáját, az általa kifejthető erőt és amunkavégző képességet vizsgálja. Az antropometria az ergonómia egy ága [6].

A tűzvédelmi eszközök nagyban hozzájárulnak a tüzek korai eloltásához, a késedelem nélküli riasztáshoz, ezáltal a tűz által veszélyeztetettek életének védelmét szolgálják. Hozzáférhetőségük több módon is biztosítható. Az optimális elhelyezés lehetővé teszi, hogy azok gyorsan elérhetők legyenek és a felhasználók könnyen tudják azokat alkalmazni. A tűzvédelmi eszközök magassági elhelyezése lehetővé kell tegye alacsonyabb és magasabb személyek részére is a hozzáférhetőséget éppen úgy, mint erősebb vagy gyengébb személyek részére is. Minden olyan személy részére biztosítani kell a tűzvédelmi eszközök hozzáférhetőségét, akik képesek lehetnek azokat használni és ezáltal a tűz korai jelzése, a riasztás és a tűz eloltása gyorsan és hatékonyan megvalósítható.

Rendkívüli esemény, tűzeset során az emberi viselkedésformák eltérnek a szokványostól [7], így ilyen helyzetben különösen fontos, hogy a tűzvédelmi eszközök a lehető legjobban észrevehető, legkönnyebben hozzáférhető módon kerüljenek elhelyezésre. Kutatásommal célom az ilyen helyzetben nehézzé váló döntéshoztalt és ezáltal a hatékony korai tűzoltást elősegíteni.

Kutatási eredményeim alátámasztják, hogy a jelenleg kialakult gyakorlaton változtatni szükséges a tűzvédelmi eszközök elhelyezése vonatkozásában és célszerű egy ennek részleteire vonatkozó irányelv kidolgozása.

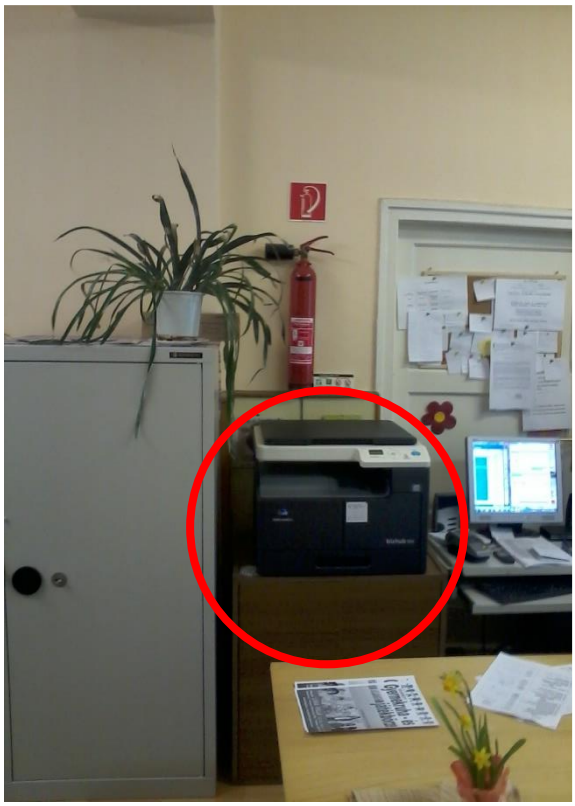
AZ ANTROPOMETRIAI ILLESZTÉS JELENTŐSÉGE

A tűzvédelmi eszközök optimális hozzáférhetőségének meghatározásakor figyelembe kell venni az azokat használó személyek adottságait. Nem ad a felhasználók széles körének lehetőséget az olyan tűzvédelmi eszköz, mely olyan magasra van elhelyezve, hogy annak fali tartóról való levétele nem minden személy által végrehajtható (**1. kép**; **2. kép**).

1. kép Magasan elhelyezett tűzoltó készülék (saját felvétel)

2. kép Falnyílás mellett 2 m magasságban elhelyezett tűzoltó készülék, alatta megközelítést korlátozó tárolás (saját felvétel)

A tűzvédelmi eszközök könnyű hozzáférését korlátozza az olyan elhelyezés, mely nem teszi lehetővé a tűzoltó készülék kellő megközelíthetőségét (**3. kép**, **4. kép**)



3. kép Tárgyak akadályozzák a tűzoltó készülék kellő megközelíthetőségét (saját felvétel)

4. kép Csak nyújtott karokkal elérhető tűzoltó készülék (saját felvétel)

Fentiekből látszik, hogy nem minden esetben biztosítható a tűzvédelmi eszközök, tűzoltó készülékek szabad hozzáférhetősége. Felmerül a kérdés, hogy milyen feltételek esetén nevezhető biztosítottnak a hozzáférhetőség. A használathoz a tűzvédelmi eszközhöz hozzá kell férni, azt meg kell közelíteni, majd üzembe kell tudni helyezni. A hozzáférés a szabad terek biztosításával megoldható, de az üzembe helyezéshez a tűzvédelmi eszközt el kell távolítani rögzítőjéről. Ehhez testi erőkifejtésre van szükség. Az ember különböző testhelyzetekben különböző erő kifejtésére lehet képes [5], így a megfelelő elhelyezéshez az emberi erőkifejtést is figyelembe kell venni.

A VdS 2001 (Vertrauen durch Sicherheit; VdS Schadenverhütung GmbH) szerint a hordozható tűzoltó készülékeket olyan magasságba kell a falra rögzíteni, hogy fogantyúja 80–120 cm közé essen és az egyes tűzoltó készülékek ne legyen egymástól 30 m-nél nagyobb távolságra [1]. Ugyanezen érték alkalmazását javasolja a BGI560 (Berufsgenossenschaft Information) is [8].

Sportcsarnokokban gyakran nem csak sportesemények, hanem egyéb rendezvények is megtartásra kerülnek. Minden esetben külön figyelmet kell fordítani a különféle tűzvédelmi berendezések, vészkijáratok, tűzoltó készülékek szabad hozzáférhetőségének biztosítására [9]. Kórházakban, felújítások során, de egyébként is, a szabadon tartandó területeket gyakran eltorlaszolják (pl. tűzcsap, tűzoltási felvonulási terület) [10]. Célszerű munkahelyen kijelölni olyan személyeket, akiknek tűz esetén a menekülés előtt beavatkozás, a tűz oltása is feladata és erre fel vannak készülve [11]. Az NFPA 10 (National Fire Protection Association, USA) szerint a 18,14 kg-nál nem nehezebb tűzoltó készülékeket úgy kell elhelyezni, hogy legmagasabb pontjuk ne haladja meg az 1,53 m magasságot. A 18,14 kg-nál nehezebb tűzoltó készülékek esetén az utóbbi magasság maximum 1,07 m. A tűzoltó készülék legalacsonyabb pontja és a padló között legalább 102 mm szabad távolságot kell tartani. A tűzoltó készüléket erre a célra jóváhagyott fali függesztőn, polcon vagy szekrényben kell elhelyezni [2].

A tűzoltó készülékek könnyű és gyors hozzáférhetősége azért is fontos, mert a kezdődő tüzek gyors eloltása így a tűzoltóság beavatkozás nélkül megvalósulhat. Jelenleg Magyarország területének 97,9 %-ában biztosított, hogy 25 percen belül kiér az első beavatkozó tűzoltó egység [12]. A tűz kialakulása és a beavatkozás megkezdése között eltelt idő alatt a tűz fejlődhet és nagyobb károkat okozhat. Célszerű tehát, ha az állampolgárok meg tudják kezdeni a még kialakulóban lévő tüzek oltását a rendelkezésükre álló tűzvédelmi eszközökkel, tűzoltó készülékekkel.

A hatályos magyar jogi szabályozás csupán a tűzvédelmi eszközök hozzáférhetőségének követelményét fogalmazza meg, de nem rendelkezik a megvalósítás konkrét módjáról [13].

A német ASR (Arbeitsstättenregel; Technische Regeln für Arbeitsstätten) A2.2 irányelv sem ad iránymutatást a tűzoltó készülékek hozzáférhetőségének konkrét adataira, csupán általánosságban írja elő a hozzáférhetőség biztosítását [14].

Előfordul, hogy a tűzoltó készüléket nem csak a tűz oltásában kevésbé jártas állampolgárok, hanem a tűzoltóság is használja, amennyiben azok könnyen hozzáférhetőek [15].

A mielőbbi, hatékony beavatkozás a tűzkárt és ezáltal a kárértéket csökkenti, a megmentett értéket növeli [16] [17].

A klímaváltozás hatásai gyakoribbá tehetik a szabadtéri tüzeket [18], így a létesítményen belüli szabadterek tűzveszélyessége is növekedhet. A kialakuló tüzek gyors és hatékony eloltását lehetővé tevő, hozzáférhető tűzoltó készülékekre fokozott igény jelentkezhet.

ANTROPOMETRIAI ADATOK

A tűzvédelmi eszközök optimális elhelyezésének meghatározásához ismerni kell a lehetséges felhasználók antropometriai adatait. Az európai populáció reprezentatív antropometriai adatait szabvány [19] tartalmazza. Ez a szabvány az antropometriai adatokat gépeken alkalmazott hozzáférési nyílások tervezéséhez szükséges mértékben tartalmazza, azonban adatai felhasználhatók a tűzvédelmi eszközök hozzáférhetőségének meghatározásához is.

Az adatok statikus mérésből származnak és figyelmen kívül hagyják a ruházatot, felszerelést és a környezeti körülményeket [19].

A szabványban megadott adatok percentiliseket határoznak meg. *„Egy eloszlás x%-os percentilisének nevezzük azt a számot, amelynél kisebb vagy egyenlő az elemek x%-a.”* [20]

Az átlagos európai populáció azon antropometriai adatait, melyeket a tűzvédelmi eszközök elhelyezése során figyelembe célszerű venni, az 1. táblázat tartalmazza. A zárójelben szereplő indexelt betűk az értékek szabványos jelölését tartalmazzák.

	5 %-os	95 %-os	99 %-os
	percentilis		
testmagasság (h_1)		1881 mm	1944 mm
könyök-könyök széleség (a_1)		545 mm	576 mm
fogástávolság (előre) (b_2)	615 mm	820 mm	845 mm
működési karhosszúság (t_1)	340 mm		
alkar elérési távolsága (t_2)	170 mm		
kézfejvastagság a hüvelykujjnál (b_4)		35 mm	
kézfejszélesség hüvelykujjal (a_3)		120 mm	
kézfejhosszúság (t_4)	152 mm		

1. táblázat Figyelembe veendő antropometriai adatok [19]

A testmagasság (h_1) meghatározását az álló személy talpának síkja és a fej legmagasabb pontját tartalmazó vízszintes sík közötti távolság adja [3]. A könyök-könyök távolság (a_1) mérését ülő személyen végzik, ahol a karok a törzs mellett helyezkednek el. A könyök-könyök távolság a két könyök legkülsőbb pontjai közt mért vízszintes távolság. A fogástávolság (b_2) azt a távolságot jelöli, mely az álló ember hátához támaszkodó függőleges sík és az ember kinyújtott kezének fogástengelye között mérhető. A könyök-elérési távolság az ülő személy függőleges karja és 90°-ban behajlított alkarja esetén mérendő. Ebben az esetben a könyök leghátsó pontja és a kéz fogástengelye közötti vízszintes távolság adja a könyök-elérési távolságot. [21] A kézfejszélesség a kézközépnél elnevezésű érték a kéz ujjtőízületeinél mért szélessége a hüvelykujj nélkül [22]. A kézfejhosszúság (t_4) az alkar csontjainak távolabbi végétől a III. ujj hegyéig mért hosszúság. [23]

A működési karhosszúság értékét (t_1) a 275 mm-rel csökkentett fogástávolság értéke jelenti. Az alkar elérési távolsága (t_2) a könyök-elérési távolság 121 mm-rel csökkentett értéke. A kézfejvastagság a hüvelykujjnál (b_4) rögzített érték: 35 mm. A kézfejszélesség hüvelykujjal (a_3) érték a kézfejszélesség a kézközépnél érték 1,25-szorosa. [19]

A testméreteken felül célszerű figyelembe venni a ruházat és egyéb hatások miatt szükséges tényezőket. Ezeket pótlékok formájában lehet megállapítani. A testmagassághoz figyelembe veendő pótlékok: 50 mm testmozgási alappótlék, 40 mm lábbeli miatti pótlék, 60 mm fejfedő (pl. sisak, sapka vagy kalap) miatti pótlék. Ezekkel a pótlékokkal megnövelt testmagasság 99 %-os percentilise 2094 mm. A könyök-könyök szélességen felül figyelembe veendő pótlékok: 50 mm testmozgási alappótlék, 100 mm nehéz téli ruházati pótlék. Ezen pótlékokkal a könyök-könyök szélesség 99 %-os percentilise 726 mm. [24]

A kéz beféréséhez figyelembe veendő pótlékok: 10 mm mozgási alappótlék és 20 mm kézvédelem (pl. kesztyű) miatti pótlék, azaz összesen 30 mm pótlék szükséges. [4] A pótlékokkal növelt kézfejszélesség 150 mm, a kézfejvastagság 65 mm.

A méreteken felül az optimális illesztéshez ismerni kell a felhasználók által kifejthető erő mértékét is. Az egy kézzel végzett erőzáró fogás határa 250 N üzemi előfordulás esetén. Az egy karral végzett munka (pl. tűzoltó készülék fali tartóról történő leakasztásakor) üzemi előfordulás esetén is legfeljebb 50 N. Az üzemi körülmények között kifejthető erő az értékek

15 %-os percentilisét jelentik. Háztartási előfordulás esetén az 1 %-os percentilist vették figyelembe. Az értékeket a **2. táblázat** mutatja be. [25]

	5 %-os	1 %-os
	percentilis	
kézzel végzett erőzáró fogás	250 N	184 N
egy karral végzett munka felfelé	50 N	31 N
egész testtel végzett nyomás	200 N	119 N

2. táblázat A figyelembe vett ajánlott erőhatárok [25]

A kutatásom során nemzetközi szinten egyetlen forrást találtam a fejtető és a szemtengely közötti távolságra, mely indiai hallgatók adatain alapul [26]. Ez jó közelítést ad más adatok hiányában az európai populáció antropometriai adataira, jelen kutatáshoz elegendően pontos. Indiai hallgatóknál a fejtető és a szem tengelye közötti távolságot a **3. táblázat** A fejtető és a szemtengely közötti távolság [26]**3. táblázat** mutatja be.

	indiai nők		indiai férfiak	
	5 %-os	95 %-os	5 %-os	95 %-os
	percentilis			
testmagasság ülve	730 mm	820 mm	730 mm	880 mm
szemmagasság ülve	630 mm	720 mm	630 mm	780 mm
fejtető és szemtengely közötti távolság	100 mm	100 mm	100 mm	100 mm

3. táblázat A fejtető és a szemtengely közötti távolság [26]

AZ OPTIMÁLIS ELHELYEZÉS MEGHATÁROZÁSA

A fali tartóról leemelendő tűzvédelmi eszközök (pl. tűzoltó készülék) hozzáféréshez elegendő méretű terek szabadon tartása szükséges. A tűzvédelmi eszköz leemeléséhez erőkifejtésre van szükség. A kifejthető erő nagyobb, ha a személy a tűzoltó készülékhez olyan közel áll, hogy karja függőleges, alkarja vízszintes helyzetű lehet. Ehhez a tűzvédelmi eszközt kellően meg kell közelíteni. A tűzoltó készüléket így legalább az alkar elérési távolságának megfelelő mértékben meg kell tudja közelíteni a személy. A megközelítési űrszelvénynek tehát legalább a tűzvédelmi eszköz függőleges tengelyétől visszamért 170 mm-ig biztosítottnak kell lennie. Ekkor az alkar elérési távolságával számolhatunk.

A megközelítés során olyan űrszelvény szükséges, melyben a személy elfér. Az oda vezető űrszelvény magassága legalább a testmozgási alappótlék, lábbeli miatti pótlék és fejfedő (pl. sisak, sapka vagy kalap) miatti pótlék értékével növelt testmagasság legyen: 2094 mm. Az űrszelvény szélessége a pótlékokkal növelt könyök-könyök szélesség, mely 726 mm.

A tűzvédelmi eszköz leemeléséhez azt meg kell fogni. Ehhez a tűzvédelmi eszköz körül célszerű a kéz beférésének biztosítása. A tűzvédelmi eszköz mellett akkor fér be a kéz, ha ott legalább a pótlékokkal növelt kézfejvastagság biztosított, ez 65 mm.

A tűzvédelmi eszközök magassági elhelyezésekor figyelembe vehető a gépek kiszolgálása során nehéz tárgyak emelésekor megengedett megfogási magasság. Ez az érték 867 mm és 1105 mm közé kell essen. [27]

Amennyiben a tűzvédelmi eszköz fogantyúval rendelkezik, melynél fogva mozgatható, vagy tartójáról leemelhető, akkor célszerű a fogantyút 867–1105 mm közé helyezni.

Más források szerint a könyökmagasságban történő (és így a legnagyobb erő kifejtését lehetővé tevő) hozzáférés 920–1230 mm között biztosított. A biztonságos leemeléshez szükséges lehet a tűzvédelmi eszköz alsó felszínét is megfogni, esetleg megemelni. Ez a legalsó megfogási pont 600 mm-nél ne legyen alacsonyabb. Amennyiben a tűzvédelmi eszköz hasznlatához annak legfelső pontját is meg kell fogni (ha itt jelentősebb erőt nem kell kifejteni), akkor ez a magasság legfeljebb 1520 mm legyen. [4]

A fenti értékek figyelembevételével biztosítható a legszélesebb körben a tűzvédelmi eszköz hozzáférhetősége.

A tűzvédelmi eszköz legfelső megfogási pontja és az álló személy szeme között nem lehet takaró tárgy, hiszen az akadályozná a megfogás vizuális kontrollját. Ezt a tűzvédelmi eszköz felett szabadon hagyott megfelelő térrel lehet biztosítani. Szemmagasságként a testmagasság 100 mm-rel csökkentett értékét célszerű figyelembe venni. Ennek 99 %-os percentilise 1844 mm. A tűzvédelmi eszköz előtt 170 mm-re 1844 mm magasságtól a szabad látótér biztosított kell legyen a tűzvédelmi eszközig.

Olyan tűzvédelmi eszköznél, melynek működtetéséhez legfeljebb a teljes test általi nyomóerő kifejtésére van szükség, elegendő lehet kisebb tér biztosítása is, például egy kézzel vagy oldalról történő működtetés esetén.

KÖVETKEZTETÉSEK

Vizsgáltam és bemutattam a tűzvédelmi eszközök antropometriai illesztésének gyakorlati jelentőségét az épületek megelőző tűzvédelmében, melyek nem csupán épületek esetén alkalmazhatók, de alkalmasak lehetnek járművek (szárazföldi, vízi és légijárművek), szabadterek tűzvédelmének tervezése és szervezése során is.

Feltártam a tűzvédelmi eszközök hozzáférésének biztosítása során figyelembe veendő antropometriai értékeket, melyeket táblázatba foglaltam. Bemutattam ezen értékek meghatározásának módját.

A feltárt antropometriai adatok alapján meghatároztam a tűzvédelmi eszközök hozzáférhetőségének optimális paramétereit, elsősorban a tűzvédelmi eszközök vertikális elhelyezését illetően. Ezen értékek alapján meghatározható a szabad űrszelvény, melyet a tűzvédelmi eszköz megközelítésére szolgáló útvonalon biztosítani kell. Meghatároztam továbbá a tűzvédelmi eszköz legalacsonyabb pontjának minimális és legmagasabb pontjának maximális magasságát, mely az optimális hozzáférhetőséget biztosítja. Megállapítottam a tűzvédelmi eszközök megfogásra szolgáló részeinek (pl. fogantyúinak) a könnyű, gyors, hatékony és biztonságos alkalmazáshoz szükséges optimális elhelyezési magasságát. Definiáltam a tűzvédelmi eszköz közvetlen közelről (170 mm-ről) történő láthatóságához szükséges szabadon tartandó teret, mely nem a tűzvédelmi eszköz felfedezhetőségét (megtalálhatóságát) hivatott biztosítani, hanem annak rögzítési helyéről a használatba vételhez szükséges elmozdításához elengedhetetlen látóteret biztosítja a tűzvédelmi eszközt használni kívánó személy részére.

Iránymutatást kívántam adni az általánosan megfogalmazott előírások konkrét megvalósítási formáira, azok számszerűsítésével.

A tűzvédelmi eszközök optimális hozzáférhetőségének biztosításához általam meghatározott adatok a következők:

- a tűzvédelmi eszközig 726×2094 mm űrszelvény biztosítása szükséges, egészen a tűzvédelmi eszköz megfogási pontjától visszafelé mért 170 mm távolságig;
- a tűzvédelmi eszköz legalacsonyabb pontja el kell érje a padlótól számított 600 mm-t, de legmagasabb pontja nem lehet 1520 mm-nél magasabban;
- a tűzvédelmi eszköz megfogásra vagy kezelésre szolgáló pontja célszerűen 920 mm és 1105 mm közé essen;

– a tűzvédelmi eszközre való rálátást a tűzvédelmi eszköz előtt 170 mm-rel legalább 1844 mm magasságból biztosítani szükséges.

Fenti értékek biztosításával a tűzvédelmi eszközöket használni kényszerülő populáció széles körének biztosítható a megfelelő hozzáférés ritkán előforduló használathoz.

A cikkben szereplő értékek csupán irodalmi adatokon alapulnak, melyek az emberi test méreteit, az ember által kifejthető erőt veszik figyelembe. Az alapul vett források elsősorban gépek, termelőeszközök rendszeres és ismétlődő emberi kiszolgálásának ergonomikus kialakításához szolgáltatnak adatokat. A tűzvédelmi eszközök használata a gyakorlatban, egy adott személy élete során csupán alkalomszerűen, ritkán történik meg, így a kiindulási adatok fenntartással kezelendők. Ezek a forrásadatok mégis kiindulási alapot jelenthetnek a tűzvédelmi eszközök optimális hozzáférhetőségének megállapításához is.

Ahhoz, hogy a tűzvédelmi eszközöket használni akaró és azokat használni képes személyek a tűzvédelmi eszközöket többlet időráfordítás nélkül és hatékonyan tudják használni, további vizsgálatok szükségesek.

FELHASZNÁLT IRODALOM

[1] VdS 2001 *Regeln für die Ausrüstung von Arbeitsstätten mit Feuerlöschern*. Köln. VdS Schadenverhütung GmbH, 1998.

[2] NFPA 1852 *Standard for portable fire extinguishers*; 2013 Edition. In: *NFPA National Fire Codes Online*. http://codesonline.nfpa.org (letöltve 2018.05.01.)

[3] MSZ EN ISO 7250-1:2018 *Az emberi test alapvető méretei műszaki tervezéshez. 1. rész: Testméret-meghatározások és mérési pontok* (ISO 7250-1:2017)

[4] MSZ EN 547-2:1996+A1:2009 *Gépek biztonsága. Az emberi test méretei. 2. rész: A hozzáférési nyílások méretezésének alapelvei*

[5] SZABÓ, Gy.: *A katonai szolgálatból származó fizikai terhelés értékelésének módszerei;* doktori (PhD) értekezés; NKE KMDI, Budapest, 2013.

[6] PHEASANT, S.: *Bodyspace Anthropometry, Ergonomics and the Design of Work;* Taylor & Francis, 2003. p. 6.

[7] RESTÁS Á.: *Tűzoltók szemtől szemben az érintettekkel: Viselkedésformák tűz- és káreseteknél;* Bolyai Szemle XIII. 3. (2014) 25–35. o.

[8] BGI 560 *Arbeitssicherheit durch vorbeugenden Brandschutz;* Berufsgenossenschaft Holz und Metall 2013.

[9] HERPERGER S.: *A használat tűzvédelmi tapasztalatai a Debreceni Főnix Csarnokban;* Védelem Katasztrófavédelmi Szemle, XIII. 4. (2006), 15. o.

[10] TISZOLCZI B. G.: *Tűzvédelmi követelmények érvényesítése kórházak rekonstrukciójánál I.;* Védelem Katasztrófavédelmi Szemle, XVIII. 3. (2011), 17–19. o.

[11] HAGEBÖLLING, D. (szerk.): *Taschenbuch betrieblicher Brandschutz*; Essen: Vulkan Verlag 1999.

[12] BÉRCZI L., PAPP CS. L.: *A mentő tűzvédelem diszlokációja a valóságos fehér foltok függvényében;* Védelem Katasztrófavédelmi Szemle XX. 2. (2013) 9–11. o.

[13] 54/2014. (XII. 5.) *BM rendelet az Országos Tűzvédelmi Szabályzatról*

[14] ASR A2.2 *Technische Regeln für Arbeitsstätten, Maßnahmen gegen Brände;* Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, 2014.

[15] BEDA L.: *Épületek tűzbiztonságának műszaki értékelése;* Doktori (PhD) értekezés, ZMNE 2004.

[16] RESTÁS Á.: *Az erdőtűzoltás hatékonyságának közgazdasági megközelítése*; Védelem - Katasztrófa- Tűz- és Polgári Védelmi Szemle XVIII. 5. (2011) p. 50.

[17] BLESZITY J., ZELENÁK M.: *A tűzoltás taktikája;* BM Könyvkiadó, Budapest, 1989.

[18] SOLYMOSI J.: *A klímaváltozás várható nemkívánatos hatásai, kritikusszektorok és a katasztrófavédelmet érintő indikátorok vizsgálata kidolgozása;* Védelem Online: Tűz- és Katasztrófavédelmi Szakkönyvtár, 2008. http://www.vedelem.hu/letoltes/anyagok/166-a-klimavaltozas-varhato-nemkivanatos-hatasai-kritikus-szektorok-es-a-katasztrofavedelmet-erinto-indikatorok-vizsgalata-kidolgozasa.pdf (letöltve 2018.05.10.)

[19] MSZ EN 547-3:1996+A1:2009 *Gépek biztonsága. Az emberi test méretei. 3. rész: Testméretek*

[20] FIDY J., MAKARA G.: *Biostatisztika*; InforMed 2002 Kft. 2005. p. 22.

[21] HOTZMAN, J.: *Measurer's Handbook: US Army and Marine Corps Anthropometric Survey 2010–2012. Technical Report NATICK/TR-11/-017*; US Army Natick Soldier Research, Development and Engineering Center, Natick, 2011.

[22] KNUSSMANN, R. eds.: *Anthropologie, Handbuch der vergleichenden Biologie des Menschen;* Vol. I/1. Fischer, Stuttgart, 1988.

[23] WEINER, J. S., LOURIE, J. A. eds.: *Human biology: A guide to field methods;* Blackwell Scientific Press, Oxford, 1969.

[24] MSZ EN 547-1:1996+A1:2009 *Gépek biztonsága. Az emberi test méretei. 1. rész: Alapelvek a nyílások szükséges méreteinek meghatározásához gépeken az egész testtel való bejutás céljából*

[25] MSZ EN 1005-3:2002+A1:2009 *Gépek biztonsága. Az ember fizikai teljesítménye. 3. rész: A gépkezeléshez ajánlott erőhatárok*

[26] TAIFA, I. W.; DESAI, D. A.: *Anthropometric measurements for ergonomic design of students' furniture in India*; Engineering Science and Technology, an International Journal XX. 1. (2017) pp. 232–239.

[27] MSZ EN ISO 14738:2009 *Gépek biztonsága. A gépkezelési munkahelyek tervezésének antropometriai követelményei*

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

HÁLÓZATI HIBA ESETÉN A VÉGFELHASZNÁLÓI KIESÉSEK SZÁMÁNAK GRÁFELMÉLETI MEGHATÁROZÁSA

DETERMINATION OF CUSTOMER NUMBER BY MATRIX OPERATIONS IN CASE OF NETWORK FAILURE

HOLCSIK Péter; POKORÁDI László; PÁLFI Judith

(ORCID: 0000-0002-8877-8620); (ORCID: 0000-0003-2857-1887);
(ORCID: 0000-0001-5313-6794)

peter.holcsik@elmu.hu; pokoradi.laszlo@bgk.uni-obuda.hu; palfi.judith@kvk.uni-obuda.hu

Absztrakt

Cikkünkben a fa struktúrával modellezhető rendszerek gráfelméleti elemzését mutatjuk be. A vizsgált modellekben a gráf csomópontjai a lehetséges meghibásodott eszközök, a fa gráf legalacsonyabb szintjein elhelyezkedő csomópontok, azaz a levelek pedig az ügyfelek vagy más fogyasztók, végfelhasználók. Az ismertetett új módszerrel elérhetőségi mátrix és gráfelméleti módszerek alkalmazásával alacsony lépésszámú matematikai művelet végrehajtásával meghatározható e modellekben az egyes csomópontok meghibásodása következtében szolgáltatás kieséssel érintett végfelhasználói darabszám. Azaz, hogy egy meghibásodott eszköz, hány végfelhasználó üzemszünetével jár.

A kidolgozott új módszer a villamos energia szolgáltatás megbízhatóságának – a nemzetközi szakirodalomban SAIFI és SAIDI-ként ismert – mutatói és az AD&TE kutatócsoport által létrehozott villamosenergia-rendszer modell alkalmazásával mutatjuk be.

Kulcsszavak: *gráfelmélet, elérhetőségi mátrix, kisfeszültségű elosztóhálózat*

Abstract

Systems that can be modelled with a tree-structured graph described in the current Article. In these models the nodes of the graph are the possible defective devices. The nodes at the lowest levels of the tree graph (also known as letters nodes) are the customers or consumers or end users.

The number of the end users affected by the service outage due to the failure of certain nodes can be determined by a new low step new mathematical operation using matrices and graph theories as described in the paper.

The developed new method is described by applying the indicators of reliability of electricity service – known as SAIFI and SAIDI indicator in the international literature – and also the electricity system model created by AD&TE research group.

Keywords: *graph theory, attainability matrix, low-voltage distribution network*

A kézirat benyújtásának dátuma (Date of the submission): 2018.07.02.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.27.

BEVEZETÉS

Villamos energiaellátási hálózatok biztonsága értékelésének egyik fontos mérőszáma az, hogy az egy berendezés meghibásodása hatására hány fogyasztónál keletkezik áramszünet.

Az Óbudai Egyetem AD&TE (az angol nyelvű Research Group of Applied Disciplines and Technologies in Energetics rövidítése, magyarul: Alkalmazott Tudományok és Technológiák az Energetikában) kutatócsoportja lehetőséget kapott az ELMŰ és ÉMÁSZ áramszolgáltató GIS alapú térképe (Elmű Émász Geographic Information System, EÉGIS, magyarul: Elmű Émász Geográfiai Információs Rendszer) mögött álló adatbázis kutatási célú felhasználására.

A kutatócsoport 2016-ban minden idők talán legnagyobb villamoshálózati modelljét hozta létre. Az egyik magyarországi áramszolgáltató vállalat két ellátási területének (ELMŰ és ÉMÁSZ) teljes hálózati adatait gyűjtötte ki és építette újra egy egységes átviteli és elosztóhálózati modell (Transmission and Distribution Network Model – TDNm) formájában. Az így létrejövő modell 2,4 millió fogyasztási hely kis-, közép-, és részben nagyfeszültségű hálózati kapcsolatait írja le.

A kapott kutatási engedély lehetőséget adott arra, hogy az AD&TE kutatócsoport részére az ELMŰ és ÉMÁSZ Hálózat dokumentációs osztály (HDO) munkatársai berendezés típusonként kiexportálták az EÉGIS rendszerből a kutatáshoz nélkülözhetetlen adatokat. A modell felépítése során a kutatócsoport számos problémába ütközött, amelyeket külön cikkben részletez [1].

A hálózati rendszerek matematikai modellezésének és vizsgálatának kiterjedt szakirodalma van. Barabási részletesen leírja a hálózatok tudományának alapjait [2]. Fazekas [3] jegyzetéből a gráfelméleti alapok ismerhetőek meg.

Jocic és szerzőtársai egy új algoritmust javasoltak a kiterjedt irányított gráfok hasonló csomópontjainak bejárására. Az általuk publikált algoritmus a fuzzy halmazelméleten alapul és gyakorlati alkalmazása többek között a befolyásos vagy kritikus pontok megtalálása egy adott hálózatban [4].

A villamos energia rendszerek gráfelméleti elemzése Novothny [5] könyvében megfogalmazott módszer alapján lehetséges. Az általa alkalmazott módszer egyes hálózati elemek egy-egy csomópontként, az őket összekötő vezetékek élekként való értelmezése megvalósítható.

Pokorádi [6] és [7] publikációiban részletesen ismerteti a jelen cikkben is alkalmazott, a gráfokat leíró mátrixokkal végzett műveleteket és az elérhetőségi mátrix fogalmát. Az általa alkalmazott matematikai módszerek azonban nem terjednek ki a fentiekben említett energiaellátási probléma megoldására.

Jelen tanulmány az áramszolgáltatók egy gyakorlati problémájának megoldásával foglalkozik. A Szerzők arra adnak választ, hogy ha a hálózaton meghibásodik egy berendezés annak hatására hány fogyasztónál keletkezik áramszünet. E vizsgálati módszer kidolgozása nagy jelentőséggel bír a villamos hálózat minőségét jellemző minőségi mutatók értékeinek meghatározásakor. A végfelhasználói kiesések determinálásának új módszerét a Szerzők az angol COnsumer Numbers with Attainability Matrices – Fogyasztói szám meghatározás elérhetőségi mátrixszal – kifejezés kezdőbetűiből alkotott betűszóval, CONAM módszer néven vezetik be.

Tanulmányunk az alábbi módon épül fel: A következő fejezet bemutatja a villamos energetikai hálózatok minőségi mutatóinak rendszerét. A harmadik fejezet ismerteti az átviteli és elosztó hálózat a kutatócsoport által készített modelljét. A negyedik és ötödik fejezet leírja az alkalmazott és bevezetett matematikai módszereket. Az ezeket követő fejezet a bevezetett új módszerekkel esettanulmányt mutat be. Végül a Szerzők összefoglalják munkájukat.

MINŐSÉGI MUTATÓK RENDSZERE

A villamos energetikai hálózatok minőségi mutató egy nemzetközileg elfogadott mutató rendszert alkotnak, amellyel azok biztonsága mérhetővé, összehasonlíthatóvá válik. Segítségükkel nem csak az egyes hálózatok ellátás-biztonsági összehasonlíthatósága valósul meg, de – a megfelelő adattisztítás után – az egyes hálózati beavatkozások (például: karbantartások, rekonstrukciók, innovatív távjelző, távbeavatkozó eszközök telepítése) hatása is mérhető. A nemzetközi szakirodalom több mint tíz különböző minőségi mutatót különböztet meg.

Azonban a magyarországi áramszolgáltatók kiemelten csak két mutatót követnek nyomon. Ezek a MEH 1 (nemzetközi környezetben: System Average Interruption Frequency Index, rövidítve SAIFI, magyarul: átlagos zavartatási gyakoriság) és a MEH 2 (nemzetközi környezetben: System Average Interruption Duration Index, rövidítve SAIDI, magyarul: átlagos zavartatási idő) mutatót. Ennek oka, hogy a Magyar Energetikai és Közműszabályozási Hivatal e két mutató alapján ítéli meg az áramszolgáltatók tevékenységét. A hivatal minden évben az elmúlt három év átlagához képest adja meg, hogy mekkora az általa elvárt szint a következő évre. Az ettől való negatív irányú eltérés szankcionálható.

Az összehasonlíthatóság és az egyes beavatkozások hatásosságának vizsgálata mellett a minőségi mutatók – ugyan csak közvetve –, de a hálózatfejlesztési ösztönzők rendszerében is fontos szerepet töltenek be.

SAIFI mutató

SAIFI – egy mértékegység nélküli (pontosabban 1 dimenziójú) mérőszám, amely azt mutatja meg, hogy egy fogyasztási helyre hány darab nem tervezett áramszünet jut átlagosan az adott időintervallumban (jellemzően adott évben). Másképpen fogalmazva: „az ellátás nem tervezett megszakadásának gyakorisága egy fogyasztóra vetítve” [8]:

$$SAIFI = \frac{\sum_{i=1}^{n} N_i}{N_T} \quad , \tag{1}$$

ahol:

N_i – az i-edik üzemzavarban érintett fogyasztók száma;

N_T – a T ellátási területen a fogyasztók összesített darabszáma.

SAIDI mutató

SAIDI – egy fogyasztóra hány perc üzemzavari kiesés jut átlagosan. Más megfogalmazásban: „az ellátás nem tervezett megszakadásának átlagos időtartama” [8]:

$$SAIDI = \frac{\sum_{i=1}^{n} (U_i N_i)}{N_T} \text{ [perc]} \tag{2}$$

ahol:

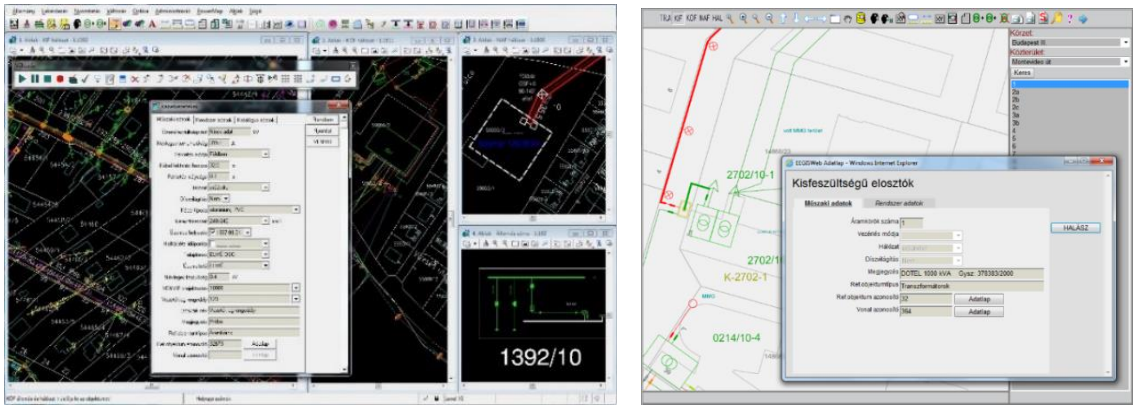
U_i – az i-edik meghibásodás okozta szolgáltatás kimaradás összegzett ideje [perc];

A SAIDI és SAIFI hálózatminőségi mutatók egyik meghatározó tényezője tehát az *i-dik* üzemzavarban érintett fogyasztók N_i darabszáma. Arról, hogy egy adott berendezés meghibásodása hány fogyasztót érint a villamos energiaszolgáltató vállalatok nyilvántartást vezetnek. Azonban e nyilvántartás folyamatos karbantartása, frissítése nagy informatikai

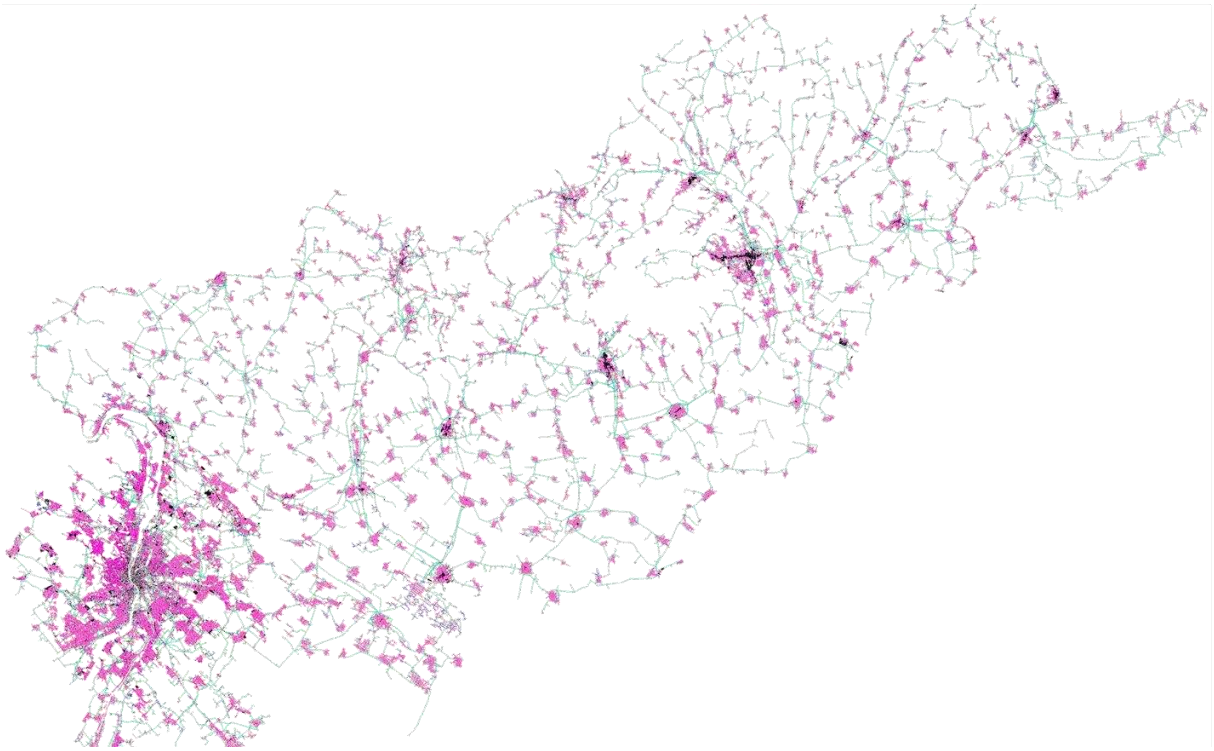
erőforrásokkal jár. Éppen ez az egyik oka az AD&TE kutatócsoport által kidolgozott, mátrix műveletekkel megvalósítható, érintett fogyasztói szám meghatározás.
A másik ok, – ahogy az a Bevezetésben említésre került – a kutatócsoport által létrehozott TDNm tulajdonságainak feltárása.

AZ ÁTVITELI- ÉS ELOSZTÓHÁLÓZATI MODELL

Az ELMŰ és ÉMÁSZ áramszolgáltató GIS alapú térképe (ELMŰ-ÉMÁSZ Geographic Information System, rövidítve: EÉGIS, magyarul ELMŰ-ÉMÁSZ földrajzi információs rendszer) az áramszolgáltató vállalatok villamos hálózatainak teljes műszaki hálózat-nyilvántartását valósítja meg (1. ábra).



1. ábra Az EÉGIS rendszer megjelenítési felületei [9]



2. ábra A TDNm vizuális megjelenítése, ELMŰ-ÉMÁSZ [10]

Az EÉGIS magában foglalja az ELMŰ és az ÉMÁSZ kezelésében lévő nagy-, közép- és kisfeszültségű villamos hálózat nyilvántartását az áramszolgáltatók teljes szolgáltatási területén. Az EÉGIS rendszer Oracle 10/11g Spatial technológiára épülő hálózat-

nyilvántartást megvalósító műszaki információs rendszer, amely együttműködik a vállalat további informatikai rendszereivel (SAP, munkairányítási, SCADA/DMS stb.) [9].

A kapott kutatási engedély lehetőséget adott arra, hogy az AD&TE kutatócsoport részére az ELMŰ és ÉMÁSZ Hálózat dokumentációs osztály (HDO) munkatársai berendezés típusonként kiexportálták az EÉGIS rendszerből a kutatáshoz nélkülözhetetlen adatokat. A modell felépítése során a kutatócsoport számos problémába ütközött, amelyeket korábban már külön cikkben részletezte [1].

Az elkészült diszkrét TDNm gráf vizuálisan is megjelenítésre került (2. és 3. ábra).

3. ábra A TDNm vizuális megjelenítése, Budapest [10]

A TDNm gráf (2. és 3. ábra) tulajdonságai szoftveres úton igen könnyen kinyerhetőek, melyekhez a kutatócsoport a nyílt forráskódú R szoftvert alkalmazta.

Fogyasztók száma	2 572 147
Maximum fokszám	1 254
Átmérő	36
Átlagos legrövidebb távolság	5,01
Klaszterezettségi együttható	0,00001
Átlag fokszám	2,017

1. táblázat A TDNm tulajdonságai

Az I. táblázatban a hálózat mérete 2 572 147, amely a hálózatba bekapcsolt fogyasztó számát jelenti. A fogyasztószám meghatározása az 1 fokszámú, azaz az úgynevezett levél csomópontok száma alapján történt. A modell maximum fokszámát mutatja. Ez azt jelenti, hogy egy adott leágazó csomóponthoz (ami egy transzformátor vagy elosztószekrény a modellben) maximálisan 1254 hálózati elem csatlakozik. A modell átmérője 36-os értéket mutat, ami a két legtávolabbi csomópont közötti legrövidebb úthossz maximuma. A modell átlagos legrövidebb távolsága 5,01, a csomópontok közötti legrövidebb távolságok átlagát mutatja. Klaszterezettségi együttható vagy más szóval csoportosulási együttható 0,00001, azt mutatja meg, hogy mekkora valószínűséggel van egy adott csomópont összekötve a

szomszédos csomóponttal. Az átlag fokszám 2,017, ami azt jelenti, hogy egy csomópontnak átlagosan valamivel több, mint 2 másik csomóponttal van kapcsolata [4].

Az 1. táblázat adatai teljes áttekintést adnak a TDNm tulajdonságairól, azonban az egyes csomópontok meghibásodásáról csak igen kevés információnk van. Ezért vezette be a kutatócsoport az elérhetőségi mátrixok adatain alapuló CONAM módszert.

AZ ELÉRHETŐSÉGI MÁTRIX

Az elérhetőségi mátrix azt mutatja meg, hogy két, csomópont között van-e elérhetőség: azaz az egyik csomópont állapotváltozása hatással van-e a másik csomópont állapotára. A villamosenergia-rendszer modellek esetében ez az állapot az adott csomópont ellátottsága.

A példaként leírt kisméretű, fa struktúrájú villamosenergia-rendszerek irányított gráfként modellezhetőek, mivel – értelemszerűen – a kapcsolat nem irány-független. Hiszen egy fogyasztó kiesése (alsóbb rendű csomópont) jellemzően nem fogja befolyásolni egy egész transzformátor körzet (magasabb szintű csomópont) ellátottságát.

Egy rendszer egyes elemei közötti összetett kapcsolatot, egymásra hatásokat a rendszer vizsgálati gráfjának úgynevezett elérhetőségi mátrixa jellemzi. Egy *m* csúcsból álló gráf elérhetőségi mátrixán azt az *m* sorból és oszlopból álló

$$\mathbf{Z}_{mxm} = \left[z_{ij} \right] \tag{3}$$

kvadratikus mátrixot értjük, ahol:

$$z_{ij} = \begin{cases} 1, & \text{ha a } p_i \text{ csúcsból a } p_j \text{ szögpont elérhető} \\ 0, & \text{ha nem} \end{cases} \tag{4}$$

Ez a mátrix például egy rendszer esetén azt mutatja meg, hogy az egyik (az *i*-edik) elem anomáliája, meghibásodása hatással van-e a másik (*j*-edik) elem működésére. Valamely folyamat vizsgálata esetén pedig megadja azt, hogy mely állapotokból lehet mely állapotokba eljutni. [6]

Egy *m* csomópontból álló gráf A_{mxm} szomszédossági mátrixának ismeretében a Z_{mxm} elérhetőségi mátrixa az

$$\mathbf{Z} = sign \sum_{n=1}^{m} \mathbf{A}^n \tag{5}$$

egyenlettel meghatározható [7].

A szomszédossági, vagy más néven csúcs, idegen szóval adjacencia-mátrix a gráf csúcsai (szögpontjai) közti kapcsolatokat leíró mátrix. Irányított gráf esetén az **A** szomszédossági mátrix a_{ij} eleme [1]:

$$z_{ij} = \begin{cases} 1, & \text{ha a } p_i\text{-ből kiinduló és a } p_j\text{-be vezető él} \\ 0, & \text{ha nem} \end{cases} \tag{6}$$

A CONAM MÁTRIX

Az elérhetőségi mátrix a fogyasztószám meghatározásra átalakítás nélkül nem alkalmas. Az elérhetőségi mátrixszal ugyanis csak azt tudjuk meghatározni, hogy hány hálózati elemet "érünk el", hány hálózati elemet befolyásol az adott csomópont kiesése. Ezen csomópontok azonban nem feltétlenül fogyasztók, lehetnek bármilyen hálózati elemek.

A villamosenergia-rendszer célja, hogy a végfelhasználóknak villamos energiát juttasson el. Ebből következik, hogy a rendszert leíró gráf minden egyes rész gráfjának legalsó szintjén a fogyasztók lesznek. Ebből következik, hogy a fogyasztók és csakis a fogyasztók fokszáma lehetséges, hogy egy legyen.

Ha **Z** elérhetőségi mátrixot felhasználva létrehozásra kerül a **C** (CONAM) mátrix úgy, hogy

$$z_{ij} = \begin{cases} [1,\infty], & \text{ha a } p_i \text{ csúcsból a } p_j \text{ szögpont elérhető} \\ 0, & \text{ha nem} \end{cases}, \tag{7}$$

ahol:

$[1,\infty]$ Z_{ij} – fokszáma,

akkor tetszőleges F csomópont (modellezett berendezés) alatt lévő fogyasztók száma az alábbi módon határozható meg:

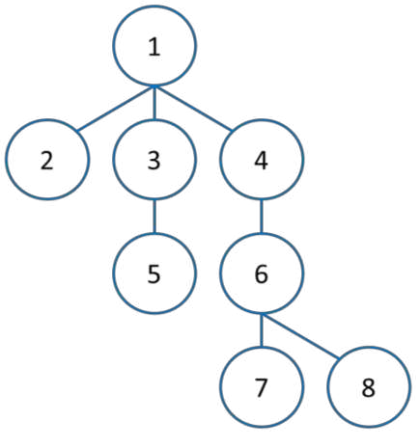
$$F = \sum_{i=1}^{n} C_{ij}^{(c_{ij}=1)}\Big|_{i=F} \tag{8}$$

Azaz, a mátrix oszlopai értékeinek összegzéséből csak azok az értékek kerülnek összegzésre melynek értéke fokszáma alapján 1.

Az elvégzésre kerülő műveletek száma, a számítás informatikai igénye könnyen belátható, hogy az 1. táblázatban ismertetett tulajdonságoktól függ.

ESETTANULMÁNY

A CONAM módszer bemutatható az alábbi, igen leegyszerűsített kisfeszültségű hálózatot leíró gráfon keresztül:



4. ábra A CONAM módszer bemutatását szolgáló példa gráf (Szerzők szerkesztése)

A példa gráfban (4. ábra) az 1. csomópont reprezentálhatja például a transzformátor állomást, a 2. csomópont egy nagyobb fogyasztót, amelyik közvetlenül a transzformátorról vételez, a 3. és 4. csomópontok az elosztószekrény két kivezetését. A 6. csomópont egy elosztó szekrényt jelenthet, míg az 5., 7., 8. csomópontok pedig a fogyasztókat.

A példa gráfot leíró **A** szomszédossági mátrix:

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{9}$$

Az **A** mátrix fő átlójába 0 értékek kerültek. A gráf, melyet az **A** mátrix leír irányított, és a számkiosztása fentről lefelé növekvő volt, így a fő átló feletti értékek nem lehettek nullától különbözőek.

Az **A** mátrixból a **Z** szomszédossági mátrix, az (5) egyenlet alapján:

$$\mathbf{Z} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{10}$$

A mátrix értékei az (5) egyenlet alapján akkor lesznek egyenlők 1-el, ha adott csomópontból egy másik csomópont elérhető. Például a $z_{1;6}$ értéke 1, mivel az 1. csomópontról elindulva irányítottan fentről lefelé haladva van olyan út, mellyel a 6. csomópont elérhető. Ezen irányítottság miatt lett a $z_{6;1}$ értéke 0, ahogyan a $z_{2;4}$ is.

A (7) egyenletnek megfelelően a **Z** mátrixból a **C** mátrix az alábbi módon származtatható, a jobb átláthatóság érdekében pirossal kiemelve az 1 fokszámú fogyasztókat:

$$\mathbf{C} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{11}$$

A **Z** és **C** mátrix felépítése alapvetően megegyezik. Azon helyeken, ahol nincs – az ismertetett módon – elérhetőség, ott az érték 0, ahol van elérhetőség, ott nem nulla. A **Z** mátrix esetében 1, míg a **C** mátrix esetében a elért csomópont fokszáma.

E definícióból következik, hogy a **C** mátrix minden sorában csak egy adott természetes szám vagy nulla szerepelhet. Például a (11) egyenletben a 4. ábra példa gráfot leíró **C** mátrix 6. sora csak 3 vagy 0 értéket tartalmaz. Hiszen ha az adott csomópontból elérik a 6. sort, akkor az ő fokszáma, azaz a 3 lesz az érték, vagy ha nem érik el, ekkor pedig 0.

A (8) egyenletei alapján a **C** mátrixból tetszőleges csomópontra megadható az, hogy annak meghibásodása esetén mekkora a végfelhasználói kiesés:

$$F_i = \begin{cases} F_1 = 4 \\ F_2 = 0 \\ F_3 = 1 \\ F_4 = 2 \\ F_5 = 0 \\ F_6 = 2 \\ F_7 = 0 \\ F_8 = 0 \end{cases} \tag{12}$$

Tehát F_i megmutatja, hogy ha az i-edik elem meghibásodik akkor az hány darab fogyasztó szolgáltatásból való kiesésével fog járni.

A (12) egyenlet eredményiben F_i értéke minden fogyasztó esetében 0. Ez megegyezik a várt eredménnyel, hiszen ha egy fogyasztónál meghibásodás történik az nincs hatással további fogyasztókra. A kisfeszültségű villamosenergia-rendszert leíró fa struktúrájú gráfból következik, hogy 0 érték csak és kizárólag fogyasztók esetében lesz.

Azonban például ha

$$F_i = 4\,, \tag{13}$$

azaz a 4. csomópont által érintett fogyasztókat keressük, már más a helyzet. A 4. ábra alapján megállapítható, hogy 2 végfelhasználó: a 7. és 8. csomóponttal modellezett fogyasztók fognak kiesni, azaz végeredményben 2 várható.

A (10) egyenletben megjelenített **Z** mátrixból leolvasható, hogy a 4. csomópontot leíró 4. oszlop értékei közül a [4;6], a [4;7] és [4;8] értékek egyesek, míg a többi érték a 4. oszlopban 0. Ez azt jelenti, hogy – ahogy az a 4. ábra ábráról is leolvasható – a 4. csomópontból kiindulva, fentről lefelé haladva a három csomópont érhető el, a 6., a 7. és a 8. számmal jelöltek.

A (11) egyenletben megjelenített **C** mátrixból leolvasható, hogy a 6. a 7. és a 8. csomópont közül csak kettő, a 7. és a 8. csomópont fokszáma 1, ami a 4. ábra leolvasásából várt érték.

KÖVETKEZTETÉSEK

Tanulmányunkban bemutattuk a CONAM módszert, mely az irányított fa struktúrájú gráfokként modellezhető rendszerek elemzéséhez, megbízhatóságuk minősítéséhez alkalmazható. A javasolt gráfelméleti eljárás elméleti és gyakorlati problémákra egyaránt megoldást nyújt. Ilyen probléma lehet például az áramszolgáltatói SAIDI és SAIFI mutatók értékeinek számításához a kiesett fogyasztók számának meghatározása vagy a nagy adatbázisok kutatói részére kapcsolati problémák megoldása. A Szerzők jövőbeni kutatásainak célja a kidolgozott módszer továbbfejlesztése más hálózati struktúrájú rendszerek, mint például a járművek közti kommunikációs rendszerek, hálózatok, járműipari szenzorhálózatok megbízhatóságának, ellenálló-képességének vizsgálatára.

KÖSZÖNETNYÍLVÁNÍTÁS

Jelen cikk az Óbudai Egyetem Alkalmazott Tudományágak és Technológiák kutatócsoport által jött létre. A kutatócsoport kiemelt támogatója az ELMŰ Hálózati kft. és ÉMÁSZ Hálózati kft.

A kutatást a Magyar Állam és az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával megvalósuló EFOP-3.6.2-16-2017- 00016: „Autonóm járművek dinamikája és irányítása az automatizált közlekedési rendszerek követelményeinek szinergiájában” projekt támogatta.

FELHASZNÁLT IRODALOM

[1] PÁLFI J., TOMPA M., HOLCSIK P., Analysis of the Efficiency of the Recloser Function of LV Smart Switchboards, Acta Polytechnica Hungarica Vol. 14, No. 2 (2017), ISSN: 1785-8860

[2] BARABÁSI A.-L., A hálózatok tudománya, Libri Kiadó 2016, ISBN: 9789633107874

[3] FAZEKAS F., Alkalmazott matematika II., Jegyzet, Óbudai Egyetem (1979), 347 o.

[4] JOCIC, M., PAP E., SZAKÁL A., OBRADOVIC D., KONJOVIC Z., Managing Big Data Using Fuzzy Sets by Directed Graph Node Similarity, Acta Polytechnica Hungarica Vol. 14, No. 2 (2017) 183-200 o., ISSN: 1785-8860

[5] NOVOTHNY F., Villamosenergia-ellátás I., Jegyzet, 2022, Óbudai Egyetem 2010

[6] POKORÁDI L., Rendszerek és folyamatok modellezése, Campus Kiadó (2008)

[7] POKORÁDI L., SOMOSI V., A Koszovói magaslégtéri irányítási rendszer gráfmodellezése HADMÉRNÖK XII. 4 (2017) 239-251. o.

[8] AVORNICULUI M-C., Considerations On Objective Methods For Developing Applied Event Extraction Systems, SEA-Practical Application of Science, Volume II, Issue 2 (2014), 447-456 o.

[9] Elmű és Émász GIS rendszere, http://www.geometria.hu/?p=1357 (letöltve: 2018.05.05.)

[10] PÁLFI J., HOLCSIK P., TOMPA M., New Database and Theoretical Model for Power Distribution Networks, 9th International Scientific Symposium on Electrical Power Engineering, Stará Lesná, Szlovákia (2017), 539-544 o.

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

KISFORMÁTUMÚ KÉPBONTÓK HATÁRFELBONTÁS KORLÁTAI

LIMITATIONS OF CAPTURE RESOLUTION IN SMALL-FORMAT IMAGE RECEIVERS

TÓTH Levente

(ORCID ID: 0000-0003-2979-5911)

toth.levente@uni-nke.hu

Absztrakt

A biztonságtechnikai területen alkalmazott videó megfigyelő rendszer a kezdetektől fogva több ponton is támaszkodik a konzumer piac technológiai vívmányaira, fejlesztéseire. Nincs ez másképp az Ultra HD (4K) tekintetében. Bár az ultra nagyfelbontású Broadcast technológia térhódítása jóval lassabb, mint azt korábban prognosztizálták, ennek ellenére a 4K felbontás szép lassan beszivárog a videó megfigyelő rendszerek területére. Egyre több gyártó portfóliójában tűnik fel az Ultra HD felbontású kamera. A kérdés csupán csak annyi: Valóban felkészült ez a terület ennek a technológiának az implementációjára? Ténylegesen több információt szolgáltat a nagyobb felbontás? Kiaknáztuk a full HD adta lehetőségeket, vagy lenne mit javítani még ezen a területen?

Kulcsszavak: *UHD, 4K, felbontás, diffrakció, határfelbontás*

Abstract

Safety video surveillance systems have been relying on the technological achievements and developments of the consumer market in a number of respects from the very beginning. It is no different in the case of Ultra HD (4K). Although in spite of the fact that the market penetration of the ultra-high definition Broadcast technology is considerably slower than previously predicted, 4K-resolution slowly but surely infiltrates into the domain of video surveillance systems. More and more manufacturers include Ultra HD cameras in their portfolios. The question, however, is rather simple: is this sector really prepared to implement this technology? Does higher resolution actually provide more information? Have all the opportunities provided by full HD been fully exploited, or is there still room for improvement in this area?.

Keywords: keywords1, keywords2, keywords3

A kézirat benyújtásának dátuma (Date of the submission): 2018.04.22.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.05.02.

BEVEZETÉS

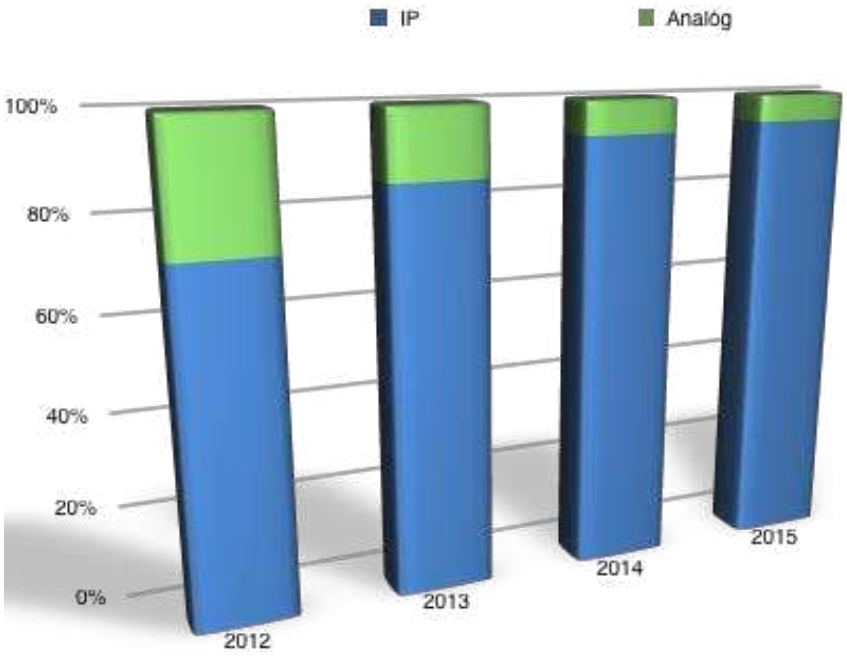
A technológiai versenyfutás az élet számos területén tapasztalható. Legyen ez például az autóipar, vagy a mobil telefonok piaca, napról napra jelennek meg az adott terület újabbnál újabb technikai fejlesztései. A gyártók egymást túllicitálva próbálják a lehető legnagyobb piaci részesedést megszerezni. Ehhez számos marketing eszközt bevetnek. A mobiltelefonok piacán dúl a pixelháború, míg a televíziós technológiánál még igazán bevezetésre sem került a 4K-s felbontás, a kiállításokon már találkozhatunk a 8K-s tovább fejlesztett változatával is.

Ez az irány nem kerülte el a videó megfigyelő rendszerek területét sem. Egyre több gyártó portfoliójában található már meg a Full HD-nál nagyobb felbontású kamera. Sokan gondolják azt, hogy a nagyobb képelem szám, jobb képminőséget és ezzel párhuzamosan részletgazdagabb megjelenítést tesz lehetővé.

Ennek a cikknek az a nem titkolt célja, hogy rávilágítson arra, hogy a kapott képünk minősége nem csak a képérzékelő felbontásától függ. Elérkeztünk egy olyan szintre, amikor már számolni kell olyan fizikai korlátokkal is, mely pontosan ellene hat a részletgazdag képmegjelenítésnek.

A PIACI TREND VÁLTOZÁSA AZ ELMÚLT NÉHÁNY ÉVBEN

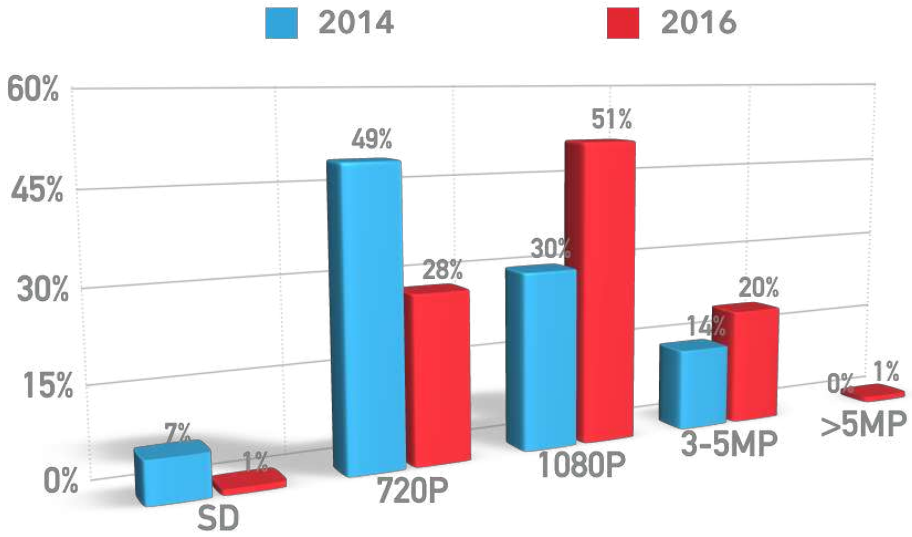
A videó megfigyelő rendszerek piacán vezető szerepet játszó Bosch cég magyarországi kamera eladási statisztikája is jól mutatja ennek a területnek a technológiai fejlődését.



1. grafikon: Bosch magyarországi kamera eladási statisztikája 2012 és 2015 között (saját szerkesztés)

Az analóg kamerák eladása folyamatosan csökken, míg az IP kameráké ugyan ilyen mértékben növekszik[1]. Tovább bontva a HD és az a feletti felbontású kamerák eladási statisztikáját, jól látható, hogy az értékesítés egyre inkább a nagyobb felbontású képalkotók irányába tolódik el [1]. Minél nagyobb felbontású kamerát választunk, annál nagyobb az esélye, hogy bizonyos körülmények között a felbontás határokba ütközik.

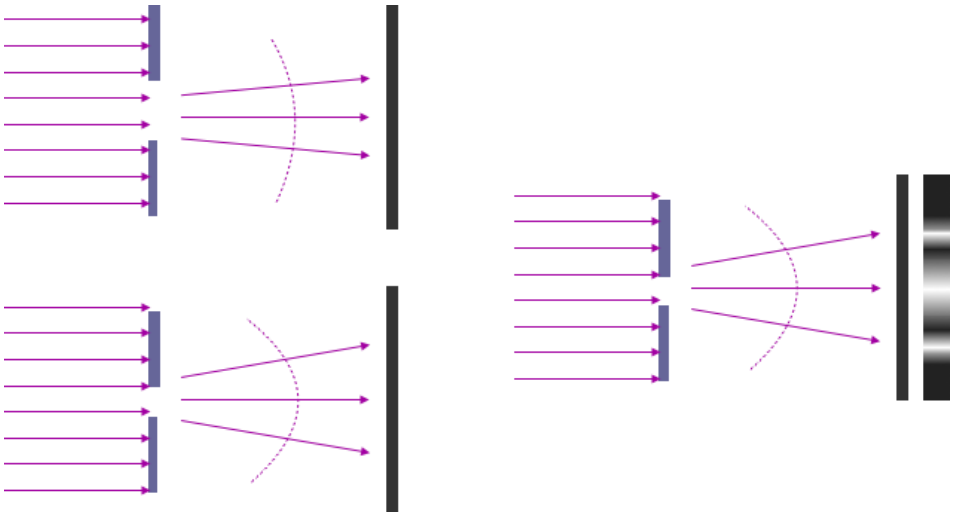
[1] Bárány Attila, Bosch értékesítési üzletág vezető adatai alapján



2. grafikon: Felbontás szerinti kameraeladás 2014 és 2016 között (saját szerkesztés)

DIFFRAKCIÓS LIMIT

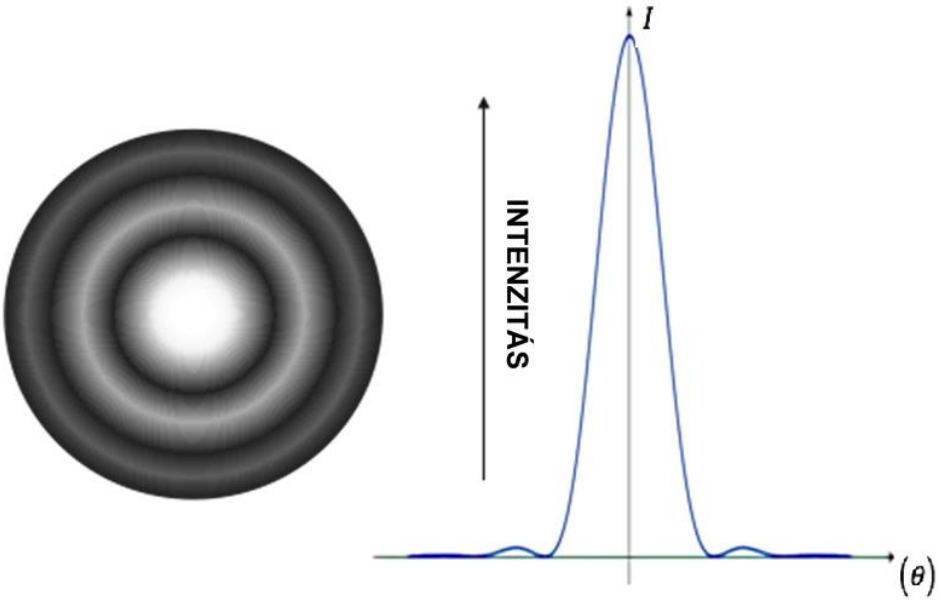
A diffrakcióval, mint fizikai jelenséggel legfőképp a hullámoptikában találkozhatunk. A fény hullámhosszával összemérhető nagyságú résen átengedve a merőlegesen érkező párhuzamos fénynyalábokat azt tapasztalhatjuk, hogy a felfogó ernyő olyan területeire is jutnak fényhullámok, ami az egyenes vonalú terjedést feltételezve optikailag takart.



1. ábra: Fényelhajlás és a rés kapcsolata (saját szerkesztés)

A Huygens-Fresnel elv szerint [2, pp. 413-414] az elemi hullámok a hullámtér különböző tartományaiban interferálnak, azaz gyengítik vagy erősítik egymást. Ez az intenzitásváltozás a felfogó ernyőn jól látszódik. A rés közepével egy vonalban található a legnagyobb intenzitású fénycsík mely jobbra és balra egyre halványodik egészen a teljes kioltás helyig. Abban az esetben, ha a rést egydimenziósnak tekintjük, akkor legnagyobb intenzitású fénypont a felfogó ernyőn a rés középpontján átmenő, az ernyőre merőleges egyenes és az ernyő metszéspontjában van, ettől pozitív és negatív irányban haladva az intenzitás a kioltásig csökken. Innen megint egyre világosodó sávokat láthatunk, mely a maximumát követően ismét halványul a második kioltási pontig (1. ábra jobb oldal).

Az elhajlás mértéke egyenes arányban van a fény hullámhosszával és fordított arányban a rés nagyságával. (1. ábra bal oldal).

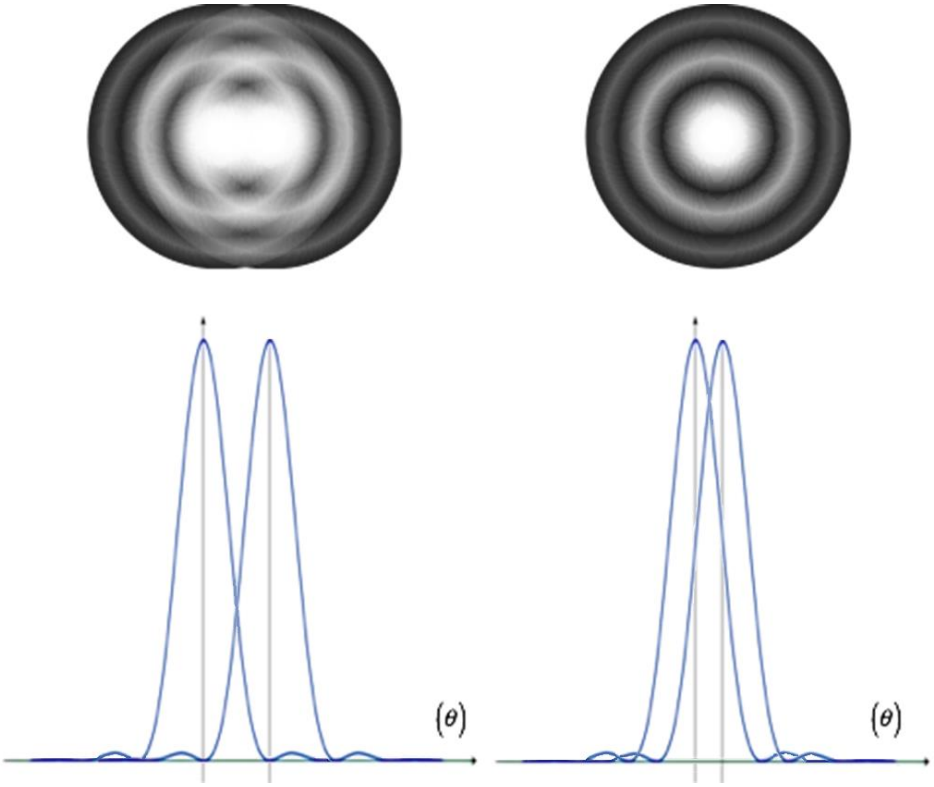


2. ábra: Az Airy korong és intenzitás függvénye (forrás: saját szerkesztés)

Körlakú résen az egy pontból kiinduló fénysugarak koncentrikusan elhelyezkedő, egyre halványodó, váltakozva világos és sötét körgyűrűket vetítenek a felfogó ernyőre. Az így kapott képet Airy[2] korongnak nevezzük (2. ábra). A korong mellett lévő intenzitás függvényen jól látszódik, hogy az első, fő minimumot követő második maximum érték csak töredéke (1,75 %-a) a fő maximumnak. Az ezt követő maximumok értékei tovább csökkenek. A harmadik maximum érték már csak 0,42 %-a a fő maximumnak (így ezek a körök csak igen erős fényforrás esetén látszódnak).

A képalkotó eszköz határfelbontásának vizsgálatakor fontos fogalom a Rayleigh[3] féle feloldási küszöb. Vizsgáljuk két, az átmérőjükhöz képest egymástól távol eső inkoherens pontszerű fénykorong képét kis átmérőjű kör alakú résre! A diffrakció következtében a két pontszerű fényforrás vetített képe már Airy korong lesz. Abban az esetben, ha a két pontszerű fényforrás távolsága összemérhető a rés nagyságával, akkor a képük összemosódik, azaz nem tudjuk egymástól megkülönböztetni őket [3, p. 149]. A Rayleigh kritérium értelmében a két közel azonos fényerősségű pontszerű folt még éppen megkülönböztethető, ha a vetített képen az egyik Airy folt maximuma a másik Airy folt első minimumára esik (3. ábra baloldali kép). Ennél kisebb távolságoknál a két pontszerű korong összeolvad (3. ábra jobboldali kép).

[2] Sir George Biddell Airy (1801 – 1892) Matematikus és csillagász
[3] Lord Rayleigh (1842-1919) angol fizikus



3. ábra: Rayleigh kritérium (saját szerkesztés)

Ahhoz, hogy az Airy korong intenzitás függvényének első minimumát számolni tudjuk, fel kell tudni írni magát a függvényt. Optikai rendszernél vizsgálva a határfelbontást [4, p. 117], a teljes matematikai levezetést mellőzve a függvény első minimum helyéhez tartozó irányra:

$$\theta_0 = \arcsin\left(1{,}22\frac{\lambda}{D}\right) \tag{1}$$

összefüggés áll fent, ahol D a kör alakú apertúra átmérője, míg λ a fény hullámhossza. Ebből következik, hogy két α szögtávolságban lévő pont akkor különböztethető meg egymástól, ha:

$$\alpha \geq \theta_0 = 1{,}22\frac{\lambda}{D} \tag{2}$$

Mivel ilyen közeli ponttávolságok esetén igen kis szögekről beszélünk, ezért nem tévedünk nagyot, ha azt mondjuk, hogy:

$$\sin\theta_0 = \tan\theta_0 = \frac{r}{f} \tag{3}$$

Ahol r az első minimum kör sugara, míg f az optikai rendszer (objektív) fókusztávolsága.

Mivel egy objektív rekeszértéke (*N*),

$$N = \frac{f}{D} \tag{4}$$

ahol *D* jelen esetben az optika belépő pupilla nyílása, így ezt valamint az (1) és (3) egyenleteket felhasználva, meghatározhatjuk a különböző rekeszértékekhez tartozó Airy korong első minimumának a sugarát:

$$r = 1{,}22 \cdot \lambda \cdot N \tag{5}$$

Az (5) egyenlet alapján tehát az Airy korong nagysága egyenes arányban van a hullámhosszal és a rekesz nagyságával. F8.0 rekeszértéknél, zöld fény hullámhosszával (520 nm) számolva az Airy korong átmérője

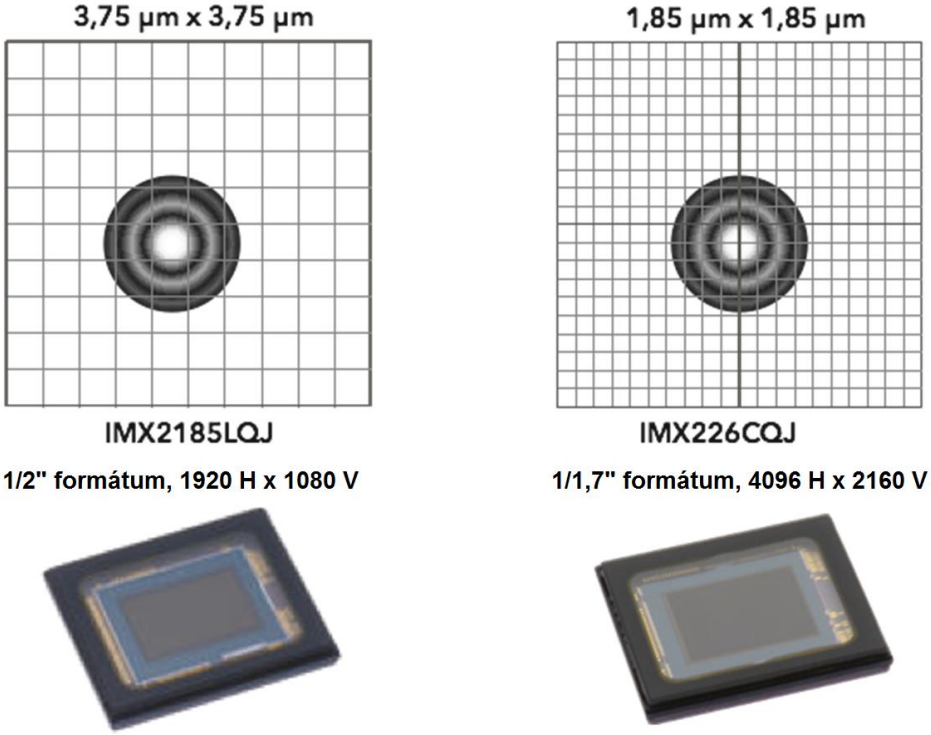
$$2r = 2{,}44 \cdot 5{,}2 \cdot 10^{-7} \cdot 8 = 10{,}15\ [\mu m] \tag{6}$$

Egyes autóiriszes optikáknál a maximális rekeszérték akár F64 is lehet, ami a (6) egyenlet eredményéhez képest 8-szor nagyobb Airy korong átmérőt jelent.

A DIFFRAKCIÓS LIMIT ÉS A PIXELMÉRET ÖSSZEFÜGGÉSE

A gyártási technológia fejlődésével a CCD[4] és CMOS[5] képbontók elemi pixel méretei egyre kisebbé válnak. Az elmúlt közel húsz évben az elemi pixel mérete több mint 100-ad részére csökkent, miközben az egységnyi felületi érzékenységet (mV/µm^2) ugyanilyen arányban sikerült növelni. Ezt olyan technológiai újításoknak köszönhetjük, mint az OCML[6], OCCF[7] és a wolfram árnyékolás, mely 20-40 %-kal alacsonyabb reflexióval rendelkezik, mint a korábban használt alumínium réteg [5, pp. 27-30]. Míg a mobiltelefonok látványos zsugorodása egyfajta elvárást támaszt a kamera és optika gyártók felé, ugyanez nem lenne igény a videó megfigyelő rendszerek területén. Ennek ellenére a képbontó elem és az objektív formátumának csökkenése folyamatos. Manapság használt 5MP, vagy ennél nagyobb felbontású képérzékelők többnyire 1/1,8” (7,17 mm · 5,32 mm), vagy jobb esetben esetleg 1/1,7” (7,6 mm · 5,7 mm) méretűek. Ezzel szemben a DSLR[8] fényképezőgépek formátuma a felbontással párhuzamosan folyamatosan növekszik. Egy Canon PowerShot G1 X Mark II típusú DSLR fényképezőgép közel 13 megapixeles (MP) képbontója 1,5”-os (18.7 mm · 14 mm) [6]. Ez 6,8-szor nagyobb felületű, mint az 1/1,8” formátumé.

Ha összehasonlítjuk a Sony IMX185LQJ típusú Full HD [7] és a IMX226CQJ típusú 4K [8] felbontásra képes CMOS érzékelőit, akkor láthatjuk, hogy az elemi pixel mérete a kisebb felbontású eszköznél 3.75 µm · 3.75 µm, míg ugyanez 4K esetében 1.85 µm · 1.85 µm. Mivel kis méretekről beszélünk, ezért nem tűnik nagynak a különbség. Kiszámolva azonban az elemi pixel felületének a nagyságát, az előbbi esetben 14,06(25) µm^2-t, míg a nagy felbontású eszköznél csak közel negyedét, azaz 3,42(25) µm^2-t kapunk.



4. ábra: Diffrakció hatása nagy és kis felbontás esetén (saját szerkesztés)

[4] Charged Couple Device – Töltés csatolt elem
[5] Complementary Metal-Oxide Semiconductor - komplementer fém-oxid félvezető
[6] On-chip microlenses – Elemi pixelre felvitt mikrolencse
[7] On-chip color filters – Elemi pixelre felvitt színszűrő
[8] Digital Single Lens Reflex - Tükörreflexes

Eltekintve a színes kameránál használt Bayer színszűrőtől[9], valamint attól a ténytől, hogy ezen képbontó eszközök szín információját 3 db elemi pixel adja és ezek nem szorosan csatlakoznak egymáshoz, vizsgáljuk meg a diffrakció okozta Airy korong hatását a képalkotásra.

A 4. ábra jól szemlélteti, hogy kis felbontás esetén az Airy korong pontosan egy teljes pixelt fed le. Ugyanakkora rekeszértéket feltételezve a nagyfelbontású szenzornál már több pixelre esik az egy pontból kiinduló fénysugár. Ez pedig azt jelenti, hogy az egymás közelében lévő pixelek azonos információt fognak megjeleníteni. Különböző méretű képbontó elemeknél különböző lesz az a rekeszérték, amely limitálja a maximális felbontást. Általánosságban elmondható, hogy ugyanakkora képérzékelő formátum mellett a nagyobb felbontású elemnél nagyobb rekeszértéknél következik be a felbontás romlása. Ez a jelenség a régebbi 1/4”-os, vagy 1/3”-os full HD, vagy esetleg 3 megapixeles biztonságtechnikában alkalmazott kameráknál ismeretlen volt. Ez alól kivétel a hosszú hullámhosszú infravörös sugárzás (LWIR[10]) tartományban működő hőkamerák, ahol az 1 megapixelnél nagyobb felbontásnál már jelentős korlátozó tényező, így polgári felhasználás esetén meg kell elégednünk az 1024 x 768-as felbontással [9, p. 21].

ÉRZÉKENYSÉG ÉS PIXELMÉRET ÖSSZEFÜGGÉSE

A képbontó eszközök felbontásának növelése egy másik problémával is együtt jár. Ez pedig az érzékenység csökkenése. Könnyű belátni, hogy a kisebb elemi pixel felületre adott állandó megvilágítás mellett egységnyi idő alatt kevesebb foton fog becsapódni, mint a nagyobbra. Ennek köszönhetően romlik az eszköz érzékenysége és dinamikatartománya. A kevesebb foton becsapódás ugyanakkora kvantum hatásfokot (QE)[11] feltételezve kevesebb elektront eredményez. Ez a kevesebb töltés pedig már összemérhető lesz a képbontó által termelt kiolvasó-, és sötétáram-zajjal. Ezek összességében szintén negatív hatással vannak a felbontásra. [9, pp. 35-36]

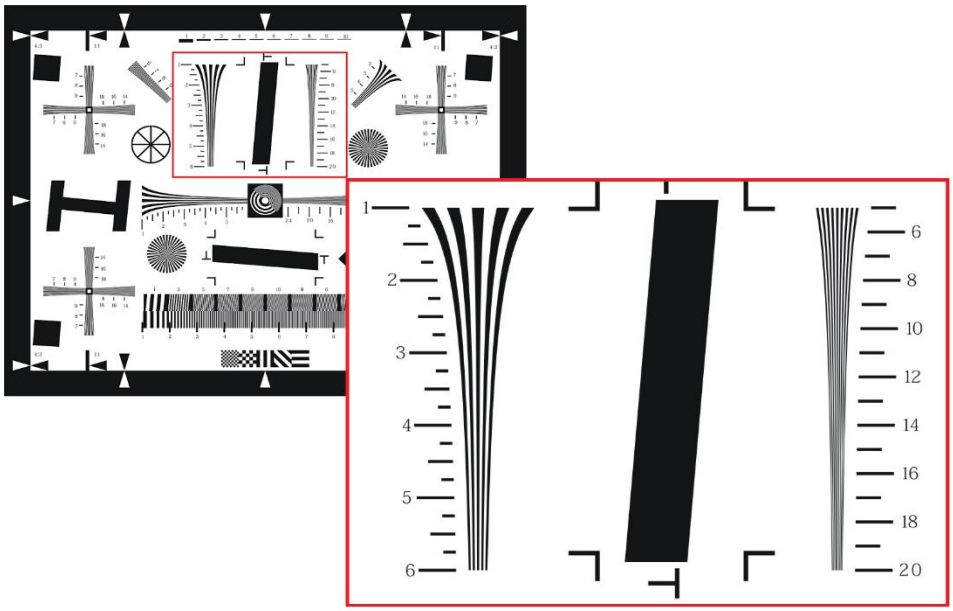
A megnövekedett jel-zaj viszony további problémát okozhat a képfeldolgozás, átvitel és tárolás terén is. A zajos kép szoftveres analitikával történő feldolgozása nehezebb, például mozgásérzékelés esetén megnövekedhet a téves riasztások száma, vagy ellenkezőleg: a küszöbszint megemelése miatt a valós mozgások felismerése csökkenhet. A nagyobb zaj rosszabb képtömörítési hatásfokot eredményez. Ez nagyobb átviteli sávszélességhez és a tárterület igény megnövekedéséhez vezet.

TESZT EREDMÉNYEK

Az eddigiekben leírtak azt sugallják, hogy az említett fizikai korlátok jelentősen rontják a kép minőségét.

Az elméleti számítások helytállóságát mérésekkel igazoltam. A megfelelő tesztkörnyezet kialakításánál figyelembe vettem a készülő IEC 62676-5 szabvány 5.3 pontját, amely részletesen meghatározza a tesztábra típusát, valamint a kamerának a megvilágításnak és a fénymérőnek az egymáshoz képest történő elhelyezkedését. A méréshez használt tesztábra a szabványban is ajánlott ISO 12233.

[9] A képbontó felületén mozaik szerűen elhelyezett RGB színszűrő
[10] Long Wave Infrared
[11] A kvantumhatásfok (Quantum Efficiency, QE) megmutatja, hogy egységnyi becsapódó fotonból hány elektron (töltéshordozó) keletkezik



5. ábra: ISO 12233 tesztábra és a kinagyított seprűék alakzat (saját szerkesztés)

A tesztábra középső-felső részen található seprűék alakzat szolgál a vízszintes felbontás megállapítására. Azt a pontot ahol az egyre sűrűsödő fekete és fehér vonalak már nem különböztethetők meg (egybeolvadnak), nevezzük a kamera határfelbontásának. Ehhez a ponthoz tartozó vonalpár/milliméter (lp/mm) érték a skáláról leolvasható. Azért, hogy leolvasásból adódó pontatlanságot elkerüljem, a felbontást az Olympus HYRes 3.1 szoftverrel állapítottam meg.

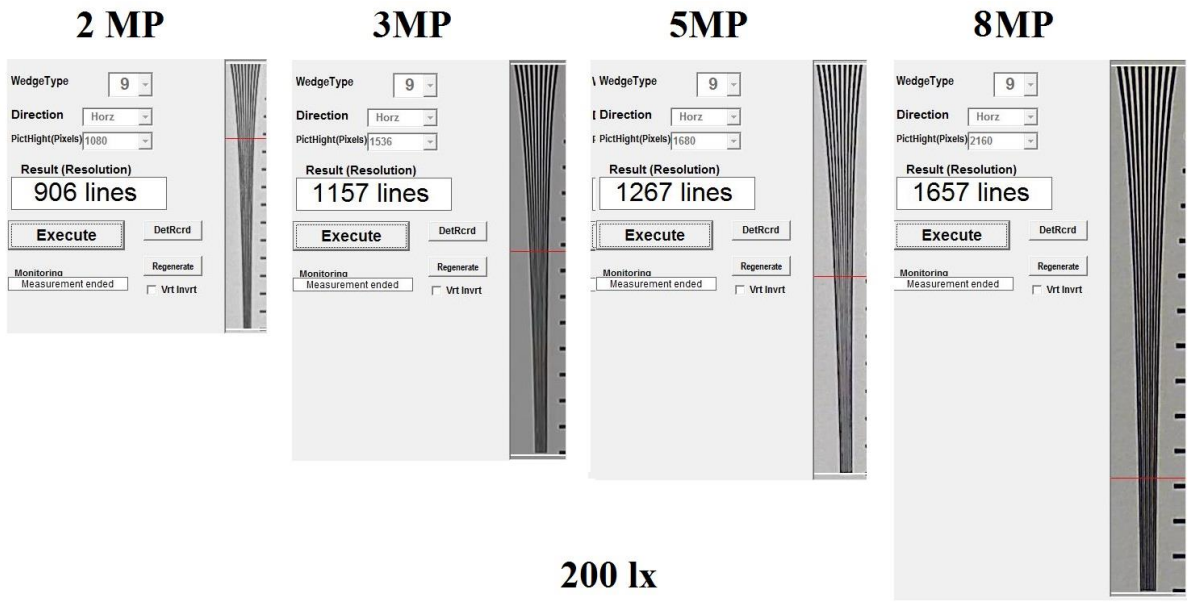
A különböző felbontású kamerák kiválasztásánál figyelembe vettem, hogy vezető gyártók közel azonos (prémium kategóriás) eszközeit válasszam. Felbontás szerint a vizsgált típusok: 2 MP (Full HD), 3 MP, 5 MP (3K) és 8 MP (4K). A tesztben résztvevő kamerák gyártói: Axis, Bosch, Hikvision és Samsung[12].

Fontos megjegyezni, hogy a felbontást nagymértékben befolyásolja az objektív határfelbontása is. Ezért a teszteszközök összeválogatásánál figyelembe vettem a gyártói ajánlást, illetve a 2 MP-es és 3 MP-es kameráknál ugyanazt a 3 MP-es objektívet használtam.

A mérés célja az volt, hogy megállapítsam: a változó környezeti megvilágítás értékek, miként befolyásolják a kép részletgazdagságát a különböző felbontású kameráknál.

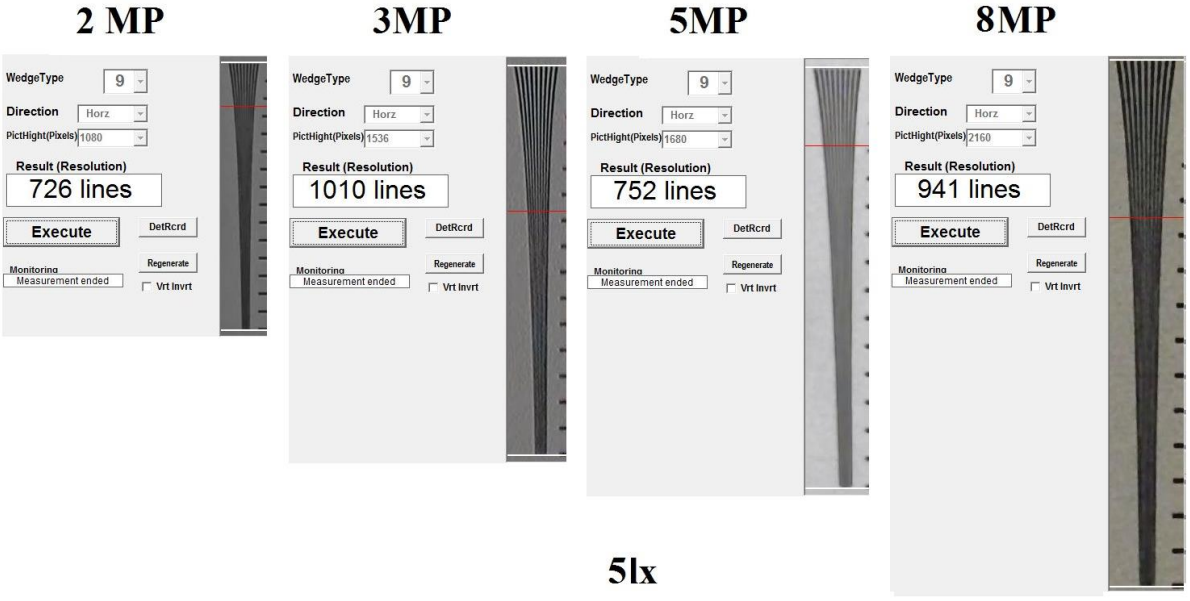
A 6. ábra az átlagos 200 lx környezeti megvilágítási értéknél kapott eredményeket mutatja. Ennél a megvilágításnál a kamerák képminősége a felbontásuknak megfelelő.

[12] Mivel a tesztnek nem volt célja, hogy rangsorolja a kamerákat, ezért a mérések eredményei szándékosan nem tartalmaznak típust és gyártót, a felsorolás alfabetikus sorrendben történt és semmilyen kapcsolatban nincs a tesztábrák sorrendjével.



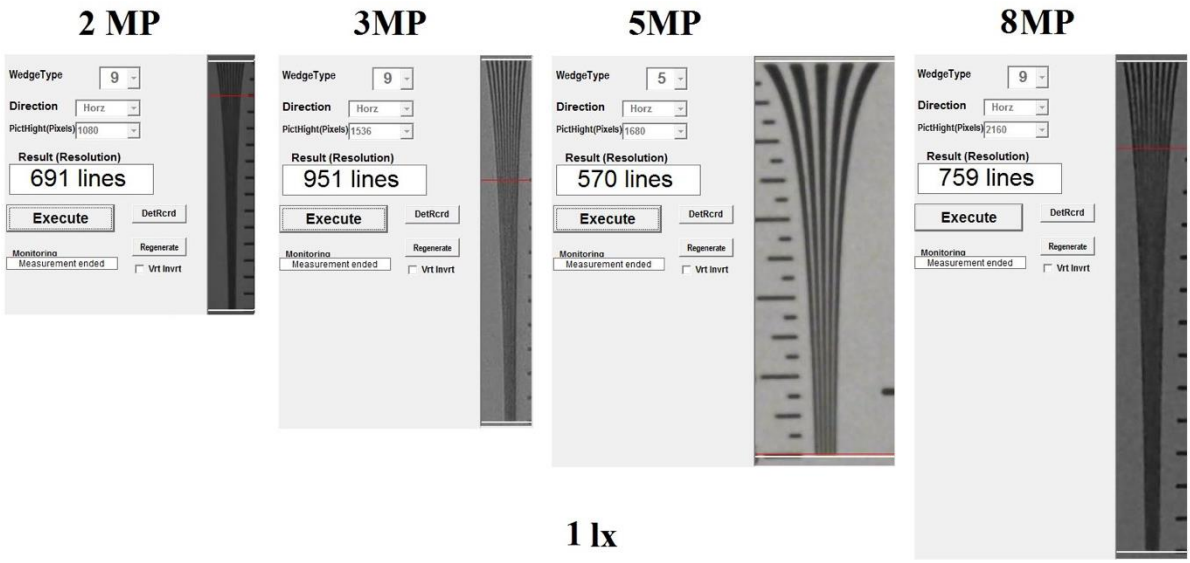
6. ábra Felbontás összehasonlítás 200 lx környezeti megvilágításnál (saját szerkesztés)

A környezeti megvilágítási értéket 5 luxra csökkentve az 8 MP-es és 5 MP-es kamerák felbontása drasztikusan romlik. Az előbbinél a csökkenés 43 %-os, míg az utóbbinál 41 %-os. Az alacsonyabb pixelszámú eszközöknél ez a felbontás-romlás csupán 13 %-os és 20 %-os (7. ábra).



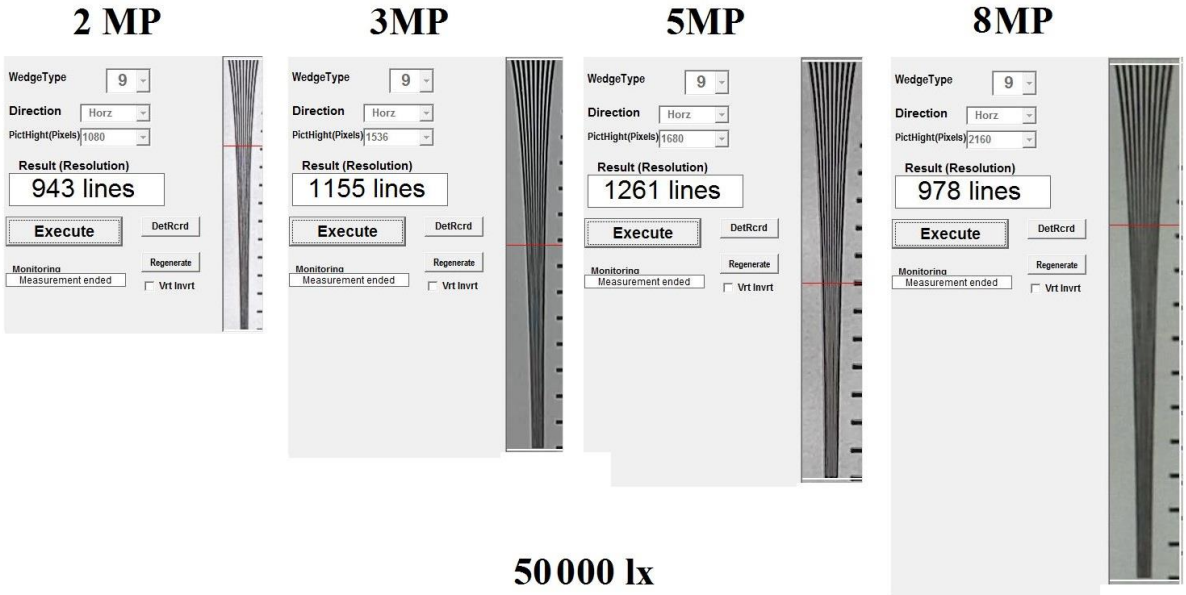
7. ábra Felbontás összehasonlítás 5 lx környezeti megvilágításnál (saját szerkesztés)

A megvilágítási értéket tovább csökkentve a felbontás tovább romlik. Az 5 MP-es és 8 MP-es kamerák egyaránt 54 %-os felbontás-csökkenést szenvedtek. A 3 MP-es eszköznél ez az érték mindössze 18 %. Az 5 MP-es kamera felbontása ennél a megvilágítási értéknél szinte a Full HD-s eszköz értékével egyezik meg, míg a legnagyobb felbontású 4K-s kamera alulmúlja a 3 MP-es képalkotót.



8. ábra Felbontás összehasonlítás 1 lx környezeti megvilágításnál (saját szerkesztés)

Az eddigiekben ismertetett méréseket beltéri környezetben, mesterséges (2700 K színhőmérsékletű) fényforrással végeztem. Azonban a diffrakciós limit hatásának vizsgálatához szükség volt több tízezer lux környezeti megvilágítási értékre, ezért a további mérések kültéren, késő tavaszi délelőtt (május 20.-án) 11 órakor, napos időben történtek. Az eredmények a 4K-s kameránál igazolták a várakozásomat: az eszköz felbontása 41 %-kal romlott, a mért érték közel van a Full HD-s kamera felbontásához. Az 5 MP-es és a 3 MP-es, valamint a 2 MP-es kameránál a diffrakció nem okoz felbontás csökkenést (9. ábra). A két utóbbi eszköznél ez elfogadható, azonban az 5 MP-es kameránál ez némi magyarázatra szorul. Ennél az eszköznél használt optika rekeszértéke F1.8 és F8 között változik. F8-as rekesznél pedig ennél az 1/1.8”-os formátumú képbontónál nem mérhető számottevő diffrakciós hatás.



9. ábra: Felbontás-összehasonlítás 50.000 lx környezeti megvilágításnál (saját szerkesztés)

KÖVETKEZTETÉSEK

A gyártástechnológia fejlődésének köszönhetően folyamatosan csökken a videó megfigyelő rendszerek kameráinak CCD és CMOS képérzékelő mérete. Ezzel párhuzamosan egyfajta verseny indult meg a gyártók között a minél nagyobb felbontású kamerák gyártása terén és mint azt a statisztikai mérés is igazolja már az eladások is elmozdultak ebbe az irányba.

A formátumcsökkenés és a felbontás-növekedés következménye az elemi pixelméret zsugorodása. Ez viszont olyan nem kívánt hatásokkal jár, amelyek ellene hatnak a részlet-gazdag, nagyfelbontású képnek. A 1/1,7”-os formátumba zsugorított 4K, vagy e feletti pixelszámú kamerák felbontása környezeti megvilágítás szempontjából alulról és felülről is korlátos lesz. Alacsony megvilágítás esetén romlik a jel-zaj viszony és ezzel együtt a felbontás. A zajos kép tömörítési hatásfoka rosszabb, így a kép átvitelekor nagyobb sávszélességet, rögzítésekor több tárhelyet igényel. Kültéri alkalmazás esetén, ahol nyáron számolni kell az akár 100.000 lx környezeti megvilágítási értékkel, az autóíriszes objektív összehúzódó rekeszének köszönhető diffrakciós elhajlás okoz felbontás-romlást. A két szélső esetben a minőségromlás olyan mértékű is lehet, hogy egy jó minőségű Full HD felbontású kamera akár kisebb zajú, részletgazdagabb képet is produkálhat.

Az eddig leírtak nem azt jelentik, hogy az ilyen kis formátumú 4K feletti felbontású kamerák nem használhatók. Állandó és elégséges (néhány száztól pár ezer lux) megvilágítás mellett a kamera auto shutter (elektronikus írisz) funkciójára célszerű rábízni a fényerő szabályzást és inkább kézi rekeszű objektívet kell alkalmazni. A rekeszt javasolt maximálisra kinyitni, bár ekkor számolni kell a mélységélesség csökkenésével. Szélsőségesebb környezeti megvilágítás esetén a kamera elektronikus írisz funkciója nem képes ~~le~~kezelni a nagy fényátfogást. Ekkor olyan optikát kell választani, amelynek a maximális rekeszértéke nem haladja meg F8-as értéket, míg sötétedéskor kiegészítő világítást kell alkalmazni. Végső esetben megfontolandó több, kisebb felbontású kamera alkalmazása is.

FELHASZNÁLT IRODALOM

[1] HONOVICH, J. IPVM, http://ipvm.com/reports/resolution-stats-2016, (letöltve: 2018.05.26.)

[2] WOLF, E. és BORN, M.: *Priciples of Optics*, Cambridge, Cambridge University Press, 1999.

[3] WAGH, S.M és DESHPANDE, D.A.: *Essentials of Physics*, Delhi, PHI Learning Private Limited, 2013.

[4] RAGHUVANSHI, G.: *Engineering Physics*, New-Delhi, PHI Learning Private Limmited, 2010.

[5] SUZUKI, T.: *Challenges of image-sensor development*, San Francisco, IEEE, 2010.

[6] Canon PowerShot G1 X Mark II http://www.canon-europe.com/for_home/product_finder/cameras/digital_camera/powershot/powershot_g1x_mark_ii/ - specification, (letöltve: 2018.05.26.)

[7] http://www.sony.net/Products/SC-HP/new_pro/september_2013/imx185lqj_e.html, (letöltve: 2018.05.26)

[8] http://www.sony.net/Products/SC-HP/new_pro/february_2014/imx226_e.html, (letöltve: 2018.05.26)

[9] HORVÁTH T. és KOVÁCS T.: *Possible application of thermal cameras with regard to security engineering;* Hírvillám IV. 1. (2013) 17-31. o.

[10] JANESICK, J. R. in *Scientific Charge-coupled Devices*, Bellingham, Washington: Press, SPIE, 2001.

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

A LÖVÉSZKATONA, MINT ELEMI ESZKÖZRENDSZER VIZSGÁLATA A HARCBAN A „LÖVÉSZKATONA" HARCÁNAK ESZKÖZRENDSZERE A MŰSZAKI FEJLESZTŐ SZEMSZÖGÉBŐL

TESTING OF INFANTRY WARRIOR IN COMBAT AS A BASIC TOOLKIT (THE TOOLKIT OF COMBAT OF „INFANTRY WARRIOR" FROM A TECHNIKAL DEVELOPER PERSPECTIVE)

FÖLDI Ferenc

(ORCID: 0000-0002-0513-8493)

foldifdr@t-online.hu

Absztrakt

A cikk a kézifegyveres harc alapelemét, a lövészkatona szerepét vizsgálja, ezúttal műszaki szempontú elemzéssel.
Az elemzés során megalkotja a lövészkatona által képviselt legkisebb alkotóelemet, a lövész, fegyvere és a fegyveréből indított lövedék alkotta elemi eszközrendszert, amely még vizsgálható a funkcióanalízis szolgáltatásaival.
Meghatározza ennek az eszközrendszernek a képesség követelményeit és alapelemeit.
Következtetéseket von le az alapelemek képesség követelményeinek egymásra hatásából és ebből számszerűsíti az eszközrendszer eredő képességeit.

Kulcsszavak: *funkció analízis, elemi eszközrendszer, lövész, rohampuska, lövedék*

Abstract

The purpose of this article to examine the role of infantry rifleman with method of technical analysis, as a basic element of infantry weapon fighting.
During analysis creates the smallest element is represented by infantry rifleman: the toolkit that consist of infantry rifleman, his weapon and the shot projectile, and can still be tested with the function analysis method.
Describes the capability requirements and basic elements.
Draws conclusions from the interaction of the basic elements of requirements capability and quantify the toolkit resulting ability.

Keywords*: Function Analysis, Elementary toolkit, infantry warrior, assault rifle, bullet*

A kézirat benyújtásának dátuma (Date of the submission): 2018.02.28.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.07.26.

BEVEZETÉS

A lövészfegyver vizsgálatban és fejlesztésben eltöltött másfél évtizedes katonai feladatvégzésem alatt meggyőződésemmé vált, hogy a lövészkatona kézifegyverével vívott harc (hadi)technikai oldalról való megközelítésének és elemzésének legcélravezetőbb módszere a rendszerszemléletű vizsgálat, mert ezzel a módszerrel olyan mérnöki értékű eredményekhez juthatok, amelyek alkalmasak lesznek a műszaki fejlesztés valóban előremutató irányainak meghatározására, a jelenlegi helyben járásból való kilépésre.

Módszerem a tanulmányom megírásához alapvetően a személyes, közvetlen megtapasztalás[1], a szubjektív élményeim gyűjtése és rendszerezése és az azokból levonható, a gyakorlatban bizonyítható tanulságok felhasználása, másrészt a rendelkezésemre álló bőséges szakirodalmi forrás[2] és nem utolsó sorban tanulmányaim során szerzett ismereteim[3] szintetizálása volt, annak a célnak az érdekében, hogy az eddigi katonai elméleti alapoktól eltérő, műszaki megközelítési szemléletet dolgozzak ki.

A műszaki megközelítés miatt gondolataimat főleg a fegyvertervezők, továbbá a lő-, és harcfeladatokat tervező parancsnokok, valamint a lőfegyvereket használók okítására is szánom, kinek-kinek a szüksége szerint, mert a lőfegyveres harc jobb megértését várom ettől.

A HARCRÓL ÁLTALÁBAN – SAJÁT MEGKÖZELÍTÉSEMBEN

Két embercsoport számtalan konfliktusba keveredhet egymással és e konfliktusoknak ugyancsak számtalan megoldása lehetséges, de elemzésemben csupán a harccal, mint a tárgyalandó témámmal egyetlen összefüggő megoldással kívánok foglalkozni.

Értekezésem tárgyának szemszögéből nézve a kérdést, a harcról nagy általánosságban kijelentem, hogy:

1. „a harc két embercsoport közötti konfliktus egyfajta speciális, de szokványos[4] megoldása”.

Amire igaz, hogy:

- a harc célja az, hogy az egyik embercsoport a másikra erőltesse az akaratát (az itt és most nem részletezett és elemzésem szempontjából nem is lényeges okokból és várható előnyök miatt);
- a megcélzott embercsoport az előző csoport céljának megvalósulását megakadályozni igyekszik[5];
- mindkét embercsoport a céljai elérésére eszközrendszert használ;

[1] Többek között kézifegyverek összehasonlító és kézifegyverek haditechnikai ellenőrző vizsgálatai (nagylőpróbák) során, illetve fegyverfejlesztéseim haditechnikai vizsgálatai (deszkamodell → kísérleti minta → „0”-sorozat → sorozatgyártási) során személyesen leadott, legalább másfél évtized alatt százezret is jóval meghaladó lövés megtapasztalása (legalább) és a 12,7 mm-es GEPÁRD M1 mesterlövész puska saját tervezésének tanulságai (összesen mintegy tucatnyi nagylőpróba). Számtalan üzleti célú kézilőfegyver megrendelésre való lővizsgálata.

[2] A Haditechnikai Intézet tudományos könyv és folyóirat tárában, valamint a fejlesztéseket tartalmazó rajz és irattárban található TU-k, fejlesztési dokumentációk, lőfegyverek fejlesztési és sorozatgyártási rajzai, stb.

[3] A Budapesti Műszaki Egyetem Gépészmérnöki karán szereztem hőerőgépész mérnöki oklevelet.

[4] Clausewitz szerint a politikai tevékenység folytatása más eszközök igénybevételével is (lásd: [1]-ben), de ez a megállapítás inkább Clausewitz korlátait jellemzi, legalább is J. Keagan szerint [2; 13.-34. old.], mert szerinte a háború inkább az adott csoport kultúrájának egy fajta megnyilvánulása [2; u.o.].

[5] Ellenállás hiányában viszont semmiképp nem használnám a harc kifejezést, mert az ilyen tevékenység nem katonai kategória.

- ennek az eszközrendszernek a számos elemén belül vannak olyan kitüntetett elemei, amelyeknek fizikai megtestesülése van.

Értekezésemben, a továbbiakban csak a fizikai jellemzőkkel bíró eszközök rendszerét kívánom elemezni.

A HARC ESZKÖZRENDSZERÉNEK RÉSZEIRŐL – UGYANÚGY

A harctevékenység során, az eszközrendszerrel vívott harcnak kell lennie egy olyan szegmensének is, amire igaz az a (szűkítéssel kapott) megállapítás, hogy:

2. „a harcban az egyik embercsoport arra alkalmas6 része, a másik embercsoport meghatározott részét – az arra a célra szolgáló saját eszközeit alkalmazva – úgy befolyásolja, hogy ne akadályozhassák meg (meghatározott ideig, vagy véglegesen) őt a célja elérésében."

Ez a megállapításom a harc *általános* megközelítéséhez képest két kitüntetett megkötést tartalmaz:

- harcra alkalmas embercsoport, és;
- ennek az embercsoportnak a harcra alkalmas saját eszközei meglétét követeli meg.

Nyilvánvaló, hogy ez a két feltétel szoros összefüggésben (egymásra hatásban) áll, mert az embercsoport a célorientált eszközei nélkül nem képes elérni a kitűzött célt, ugyanakkor az eszközök önmagukban, az emberi elem (kitüntetetten az emberi akarat) nélkül viszont csak holt tárgyaknak tekinthetők. Az embercsoport célorientált része az ugyancsak célorientált eszközeivel alkotja az embercsoportnak a «2» szerint orientált eszközrendszerét, amelyet a további vizsgálat tárgyává kívánok tenni.

Fenntartva a megállapításomat, hogy az embercsoport céljai elérésére eszközrendszert használ, az előző fejtegetésemből következik, hogy ennek az eszközrendszernek tehát van:

- humán összetevője;
- tárgyi (technikai) összetevője.

A humán összetevőt – a közhasználatú kifejezéssel – harcosoknak, a technikai összetevőt egyelőre **e**szköznek fogom megnevezni.

A harcosok az eszközeikkel lesznek képesek tevékenységüket a cél elérése érdekében kifejteni. Ezek az eszközök, mint önálló alrendszerek számos példányban (általában ahány harcos) lelhetők fel a harcszíntéren.

Vizsgálatom szempontjából – hogy a vizsgálati minta nagyságát folyamatosan szűkíteni tudjam – meg kell kötnöm, hogy:

3. A harc eredménye természetesen a harcosok eredő tevékenységén múlik, de a harcmezőn a harcot ott és akkor minden harcos egyedül és önmagának vívja meg, végső soron a saját túléléséért[7].

Ezzel a fejtegetéssel jutottam el a vizsgálatom célobjektumához, mert kijelentem, hogy az eszközrendszerrel vívott harctevékenység – elemzésem szemszögéből – lebontható az egyedi

---

[6] A megkülönböztetés kulcsszavai: válogatott, felkészített, adott célra kiképzett.

[7] Ugyanakkor az eredmény szempontjából (a győzelem) minden egyéni teljesítmény egyaránt fontos, sőt sok esetben akár egyetlen egyéni teljesítmény is döntő befolyású lehet! Ezt az első pillanatra sajátosnak tűnő megállapításomat más, a csata emberi oldalával foglalkozó szakíró is megerősíteni látszik, lásd: a [3] és [4] irodalmi forrásokban. Lásd még: Keagan véleménye a párviadalok szerepéről a harcban → kézitusa [3; 119 old.]

harcos saját eszközeivel vívott elemi harcára. Ebből következik, hogy az eszközrendszerrel vívott harc célja az elemi harcok összességének az eredőjeként valósul meg, tehát ennek az elemi harcnak elemi eszközrendszere alkalmas a külön elemzésre, további megállapítások levonására. Az ilyen eszközrendszernek az elemi szinten is humán és technikai összetevői vannak.

Megállapítom tehát, hogy:

4. „egyes célorientált embercsoportok azt a magasabb csoportérdeket jelentő célkitűzést, hogy egy másik meghatározott embercsoportra az akaratukat rákényszerítsék, a rendelkezésükre álló elemi eszközrendszerek hatása eredőjeként érik el. A végeredmény szempontjából ezért minden elemi eszközrendszer hatása döntő fontosságú lehet."

Az elemi eszközrendszer első elemének a humán tényezőt választottam, akit ezután – általánosítva – harcosnak fogok nevezni.

A harcost

- fizikai;
- mentális;
- szellemi állapotával;
- kiképzettségi szintjével;
- ismeretei szinten tartásának minőségével, mint alapvető jellemzőivel kívánom a későbbiekben leírni.

A harcos elemi harcához nélkülönözhetetlen eszközök – mint azt a következőkben bebizonyítom – eszköz-alrendszert alkotnak[8] és a harcoshoz, mint individuumhoz elválaszthatatlanul kapcsolódnak

Annak érdekében, hogy az eszköz alrendszert értekezésem szempontjából könnyen elemezhetővé tegyem, tovább szűkítem a vizsgált kört, ha kikötöm, hogy:

5. *„a harc közben az akarat érvényesítésére alkalmazott befolyásolás az érintettek fizikai állapotának olyan mértékű romlásához vezessen, hogy azok ne akadályozhassák a cél elérését."*

Az általános megfogalmazás tartalmát még tovább szűkítve, a fizikai állapotromláshoz vezető tevékenységek közül csupán azok a területek érdekesek elemzésem szempontjából, ahol valamely ismert és mérhető energiát (továbbiakban: *károsító energia*) közölnek az emberi szervezettel[9]. A sokféle számba jöhető energia közül általában a mozgási, a kémiai és a hőenergia a fontos a vizsgálódáshoz, amire később még részletesen szintén visszatérek.

A folyamatos szűkítésekkel jutottam el ahhoz a megállapításomhoz, hogy:

6. „az egyik embercsoport kitüntetett egyedei olyan módon befolyásolják a másik embercsoport kiválasztott egyedeit – ismert és mérhető energiák (károsító energia) egy részének közlésével -, hogy akaratukat a másik embercsoportra rákényszeríthessék és ehhez konkrét eszközt (természeteset, vagy megalkotottat) alkalmaznak"

[8] Az alrendszer természetesen több elemből állhat, hacsak nem puszta kézzel folyik a küzdelem (ez a harc legősibb megnyilvánulása, ma viszont már úgy minősítik az eseményt, hogy verekednek).

[9] Károsítani lehet elvileg az ellenséget azzal, hogy megijesztik, vagy megátkozzák, de ezek eredményességét a hadtörténelem nem tudja kellőképp igazolni, illetve tudományosan nehezen kimutatható az ok-okozati összefüggés.

Ezt az eszközt nevezem fegyvernek.

A harcban csak az egy harcos által kezelt fegyverek összességét vizsgáltam (egyéni fegyver), valamint peremfeltételként megszabtam, hogy a fegyver a károsító energiát legyen képes annak keletkezési helyétől távolabbra eljuttatni és ez a távolság a szokásos dobótávolságokat[10] sokszorosan meghaladja, ezzel megkaptam az egyéni lőfegyverek (a továbbiakban lőfegyverek) csoportját.

További megkötésként – a modern harc alapvető jellegzetességének megfelelően –kizártam az emberi izomerőt felhasználó fegyvereket. Értelemszerűen adódott tehát, hogy az így vizsgált eszközcsoportba csak olyan fegyverek tartoznak, amelyek a károsító energia transzportálását valamely (ismert) természeti energia felhasználásával:

- mechanikai energiából nyert mozgási energiával (hajítógépek, légfegyverek, stb.);
- kémiai energiából nyert mozgási energiával (tűzfegyverek);
- hősugárzással;
- elektromos energiával (elektromágneses hajítás);
- nukleáris és részecske sugárzással végzik el.

A károsító energia mértékének vizsgálatával tovább csökkentettem a lőfegyverek csoportjának a méretét. Ennek érdekében meg kellett határoznom a károsító energia „szükséges értékének*"* alsó és felső határát egyaránt [5]. Az alsó határ (energiaminimum) mértékének azt az energiamennyiséget kell tekinteni, mely hatására az ellenség legalább egy egyede biztosan kiválik a harcból, függetlenül attól, hogy az energia testének melyik pontján (felületén) érte!

A szakirodalom, különösen a katonaorvosi szakirodalom tanulmányozása során arra a megállapításra jutottam, hogy ebben a kérdésben semmilyen egységes álláspont nem létezik. Az egyes országok ilyen irányú publikációinak adatait összefoglaló egyik szakmunka [6; 303. o.] szerint a harcképtelenné tévő energiamennyiség saját katonáikat illetően: a francia 40 J, a svájci 63 J, a német 80 J, az amerikai 80 J, a szovjet 240 J (erről jegyzi meg *epésen* a svájci Stutz ezredes – a svájci Védelmi Minisztérium Védelmi Technológiai és Beszerzési 2. Csoport későbbi feje –, hogy: „Did that mean that a Russian soldier was six times more resilient than a French soldier?"[11]). Ezek tükrében, teljesen önkényesen, de a realitás talaján maradva a vastagcsont-törő képesség határenergiáját 85 J-nak vettem (át)[12], a valószínűsíthetően halált okozóét viszont 200 J-ban, ebből a biztosan harcképtelenné tévőt[13] legalább 150 J értékben határoztam meg. Ezek a mennyiségek azonban a károsító energia hatáskifejtésének pontjában (tehát a célban) értendők[14], mert mindenképpen figyelembe kell venni azt is, hogy a kívánt energia mennyiséget teljes mértékben közölni kell a céltesttel. Amennyiben az energiának csak egy része marad a testben és a többi távozik, mert a lövedék áthatol a céltesten, akkor az előbb közölt értékek csak a bennmaradó energiára vonatkoznak[15].

---

[10] A fegyverek azon halmaza, amelyekre nem alkalmazom a szokásos dobótávolságon túli (nem több mint 50 m) megkötést, tartalmazza a kézi hajítófegyvereket is, amelyek nem képezik a dolgozat tárgyát. A lőfegyver a károsító energiát a célba ellövi.

[11] Magyarul: "ez azt jelentette, hogy egy orosz katona hatszor *ellenállóbb*, mint egy francia katona?" (ami akár lehet igaz is – legalább is a II. Világháborús teljesítményük tükrében). Kiemelés tőlem.

[12] Az 1"-os fenyődeszka átütéséhez szükséges energia 100 m lőtávolságon. A Haditechnikai Intézetben Egerszegi János munkássága és mérései nyomán használtuk ezeket az energia mennyiséget.

[13] Mert a néhány minősített esetet kivéve az ellenség biztos harcképtelenné tétele a cél nem a megölése.

[14] Földi körülmények között a transzportált energia a művelet során mindig veszít valamilyen mértékben kiinduló értékéből. Ez a veszteség az adott esetekben jól leírható matematikai összefüggésben van a transzportáció távolságával, valamint annak a közegnek az állapotjelzőivel, amelyen keresztül az átvitel történik (alapesetben ez a közeg a légkör). Lásd még a [8]-ban kifejtett gondolatokat is, egy másik megközelítésében.

[15] Számszerűsítve: $E_{károsító} = m_{lövedék} * (v_{be}^2 - v_{ki}^2) / 2$; ahol v_{be} a lövedék becsapódási a v_{ki} a kilépési sebessége.

Az energiamennyiség felső korlátját az a megfontolás határozza meg, hogy az energia átvitel a lehető legnagyobb távolságra megtörténhessen, ugyanakkor ennek jelentős megvalósíthatósági korlátjai vannak. A számba jöhető megfontolások közül a leglényegesebb az a feltétel, hogy a károsító energia azt a célobjektumot (célszemélyt, céltárgyat[16], célkörzetet) érje, akinek (aminek) a károsítását a harcos célul tűzte ki[17] maga elé. Ez átvezet a később tárgyalandó pontosság[18] követelményéhez. Szem előtt kell tartani – többek között technikai és gazdasági okokból is[19] –, hogy felesleges a mindenképpen szükségesnél lényegesen nagyobb energiát közölni a céllal a maximális energia átvitel távolságán (maximális lőtávolságon), hiszen adott esetben az energia transzportáció vesztesége akár a távolság négyzetével arányosan nőhet és ezt a veszteséget a kiindulási ponton (a fegyverben) kell dotálni. Változatlanul fenntartva a 150 J értéket, továbbá figyelembe véve a transzportálás miatti energia veszteségeket belátható, hogy a károsító energia felső határértéke általánosan nem számszerűsíthető, mert több, esetenként csak az adott energiafajtára és átviteli módszerre jellemző tényezőtől is függ. Miután egyértelmű, hogy a károsító energia mértékét az energiaátvitel kiinduló pontján lehet csak befolyásolni, valamint léteznek szükséges és elégséges korlátok is, úgy döntöttem, hogy értekezésemben csak azokat a lőfegyvereket veszem figyelembe, ahol a károsító energia a keletkezés helyén (a lőfegyverben[20]) meghaladja a 300 J-t és nem nagyobb, mint egy önkényesen megadott (pl. a cél felismerhetőségét biztosító) távolságban mérhető szintén 300[21] J becsapódási energia létrehozásához szükséges[22] energia. A torkolati energia emiatt akár 3000 J is lehet, tehát a felső korlát mértéke esetenként akár nagyságrenddel is meghaladhatja az alsó korlát mértékét.

A fenti gondolatmenetet lezárva kijelentem, hogy elemzésem szempontjából a továbbiakban katonai célú lőfegyvernek a legalább 300 J induló (torkolati) károsító energiát előállító lőfegyvert tekintem, nem megadva az energia felső korlátját, amit a későbbiekben kívánok megmagyarázni.

Ezt a lőfegyvert választottam az eszközrendszer következő elemének.

Tovább elemezve az energiakérdést felismertem, hogy nem csak azt szükséges vizsgálni, hogy a károsító energia milyen transzportáló energiával jut el a fegyvertől a célig, hanem azt

---

[16] Sok esetben az élőerő harcképtelenné tételéhez bizonyos tárgyak (főleg a fegyver és a célszemély között lévők) rombolása elengedhetetlen. Azonban minden esetben az élőerő harcból való kiiktatása a végső cél!

[17] Az új katonai feladatkörökben (béketeremtés, békefenntartás) egyenesen megengedhetetlen, hogy vétlen áldozatok sérüljenek meg

[18] A pontos célzás követelményeiben a humán elem oldaláról hosszú időn keresztül az átlagos teljesítményű emberi szem azon látótávolsága volt a meghatározó, amin belül az emberalak méretű cél még elkülöníthető volt a környezetétől (kb. 1000 m). A célzást segítő optikai eszközök térnyerésével, valamint az új katonai eljárások bevezetésével mindinkább a cél(személy) felismerhetőségének távolsága szabja meg a felső határt. A fegyver-lövedék alrendszer pontosság képessége a másik tényező, amely a lőtávolságot a pontosság kritériumának oldaláról behatárolja, ez viszont a történelem során egészen az utóbbi időkig rövidebb távolságot jelentett, mint a humán tényező adta lehetőség.

[19] Könnyen belátható, hogy egy fegyver által transzportálható energia mennyisége és a fegyver bonyolultsága és ára között összefüggés van

[20] A továbbiakban - jó közelítéssel – a torkolati energia kifejezést célszerű használni, tudomásul véve, hogy adott esetben csak látszólagos torkolatról lehet szó, illetve, hogy sok esetben a torkolati energia hagyományos módon nem is mérhető. A torkolati energiát mérhető tömeggel rendelkező lövedék esetében a torkolati sebesség meghatározása után, a mozgási energia képlettel lehet kiszámítani ($E_0=1/2mv^2$).

[21] Abból a megfontolásból, hogy a biztos harcképtelenné tétel érdekében (figyelembe véve, hogy az energiaátadás a célpont számára szintén veszteséggel járhat, pl.: áthatoló lövedék miatt) 100%-kal több károsító energiát célszerű számításba venni.

[22] Legalább 50%-os energia-átadási hatásfokot feltételezve

is, hogy mi a transzportáló energia hordozója. A könnyebb érthetőség és a megvalósított szerkezetek ismeretében csupán két részre osztom a lehetséges megoldásokat, miszerint:

- külön erre a célra alkotott, tömeggel és kiterjedéssel, többnyire adott elvek alapján szerkesztett alakkal rendelkező tárgy segítségével,
- a (szub)atomi méretű világ természetét felhasználva (ezzel a megfogalmazással kerülve el a kvantumfizikai és filozófiai fejtegetéseket egyaránt[23]) végzi a károsító energia eljuttatását a célba.

Az egyszerűség kedvéért mindkét esetben az energiaátvitelt szolgáló megoldást lövedéknek fogom nevezni, még akkor is, ha tudom, hogy a β változat esetében ez kissé túlzó általánosítás[24], de a továbbiak könnyebb megértése szempontjából kell ragaszkodnom hozzá, főleg, hogy elemzésem tárgyában (a megvalósult mesterlövész alrendszerek műszaki megoldásai miatt) csak az α változatú lövedék kap további szerepet.

Ezt a lövedéket választottam az eszközrendszer utolsó elemének.

A lövéssel kapcsolatos alapfogalmakat – fejtegetéseim szempontjából némi önkénnyel – a következők szerint ismertetem:

- az űrméret a nemzetközi gyakorlatban általánosan a fegyvercső furatának a legkisebb (az oromzatok között mérhető átmérő) méretét jelenti. Egyes angolszász fegyvereknél az űrméretet a kilőtt lövedék fontokban mért tömegével azonosítják, míg a sörétes fegyverek űrméret-jelzése azt mutatja, hogy a cső furatának átmérőjével egyező átmérőjű ólomgömbből hány darab készíthető el 1 font tömegű ólomból, de ezek az esetek elemzésem szempontjából érdektelenek;
- az energia transzportáció folyamatának megindítását (amikor az előbb meghatározott *lövedék* megindul) összefoglaló néven (az egyszerűség kedvéért nem téve különbséget az egészen finom részletekben) nevezem lövésnek;
- az energia transzportáció befejező pillanatát, amikor a károsító energia eléri a célt[25] és elkezdi kifejteni hatását, nevezem – szintén az egyszerűség kedvéért – találatnak;
- azt a háromdimenziós térben és az időben pontosan meghatározható helyet, ahonnan az energia transzportációt (a lövedéket) megindítjuk, nevezem – általánosított kifejezéssel – lőállásnak[26];
- azt a háromdimenziós térben és az időben pontosan meghatározható helyet, ahová a károsító energiát el akarjuk juttatni**,** nevezem célzási pontnak (célpontnak). A célpont térbeli kiterjedése lényegesen kisebb is lehet, mint a célobjektum térbeli kiterjedése, bizonyos fajtájú károsító energia alkalmazása esetén viszont lehet a célnál nagyobb is[27];
- azt a háromdimenziós térben és az időben pontosan meghatározható helyet, ahol a lövedék az energia transzportáció végén tartózkodik („becsapódik”), illetve ahol a

[23] Például a fény kettős természetéről, vagy a hősugárzásról, a részecskesugárzásról, stb.

[24] Impulzuslézer esetében a foton-csomag például könnyen felfogható lövedéknek, mint ahogy minden részecskeáramlás is, amelynek a térben kiterjedése van.

[25] Vagy valamit annak környezetében.

[26] A lőállásnak az eszközrendszer által kitöltött azt a térrészt kell tekinteni, amelyet a lövés pillanatában foglal el. Értelemszerűen a lőállás nem lehet pontszerű, azonban esetenként a csőtorkolatnak a háromdimenziós térben és az időben pontosan meghatározható helyével fogom helyettesíteni.

[27] Ha a károsító energia (a lövedékből kiszabadulva) távolabb is hat (lásd a 7. oldalon a másodlagosan ható energiák).

károsító energia ténylegesen elkezdi kifejteni hatását[28], nevezem találati pontnak[29], függetlenül attól, hogy ez a pont a cél által elfoglalt térrészben van-e, vagy sem!
- végül azt az utat, amelyet, a károsító energiát hordozó lövedék az energia transzportáció során bejár, nevezem röppályának;
- a harcos azon elhatározását és cselekvését, amikor a lövedék röppályáját úgy irányítja a fegyvere segítségével, hogy az messe a cél által kitöltött térrészt, nevezem (a hagyományos kifejezéssel élve) célzásnak;
- azt az időpillanatot, amikor a harcos, a lövést kiváltó akaratát átviszi a fegyverre, (szintén hagyományos kifejezéssel) nevezem elsütésnek;
- azt az időben pontosan meghatározható terjedelmű cselekvés és történés sort, amely a harcos által kiváltott lövéstől a lövedék által transzportált károsító energia hatásának a célra történő kifejtéséig tart, nevezem lövésfolyamatnak[30].

Könnyen belátható, hogy ezek az elnevezések függetlenek attól, hogy milyen jellegű transzportáló energiával, milyen fajta lövedéket lőnek, mert mindenkor azonos folyamatokat jelölnek.

A lövésfolyamatnak azt a részét, amely a lövés akaratlagos kiváltásától a lövedék becsapódásáig tart, a ballisztika tudománya (a tűzfegyverek esetében) négy szakaszra bontja (ezek alapfogalmak, magyarázatukat önkényesen egyszerűsítettem a lényeget megtartva):

1. *belballisztika* (azon folyamatok összessége, amelyek azalatt játszódnak le, amíg a lövedék a fegyver csövében tartózkodik);
2. *átmeneti ballisztika* (azon folyamatok összessége, amíg a lövedék a fegyvercső torkolatának közvetlen közelében tartózkodik; pl.: amikor a lőporgázok elégéséből keletkező gázok feszítőereje által mozgatott lövedéket a csőtorkolat elhagyása után még befolyásolják a hajtógázok);
3. *külballisztika* (azon folyamatok összessége, amelyek azalatt játszódnak le, ameddig a lövedék a röppályán tartózkodik);
4. *célballisztika* (azon folyamatok összessége, amelyek a lövedék becsapódásakor játszódnak le).

AZ ESZKÖZRENDSZERBEN HATÓ ENERGIÁK ELEMZÉSE

Elemzésem e szakaszában felismertem, hogy a lövedék által transzportált károsító energia fajtája a következő lehet:

- mozgási energia (alapvetően azonos a lövedék mozgási energiájával a találati pontban, kivéve, ha a „becsapódás” újabb energiát szabadít fel);
- irányított hőenergia (pl.: lángszóró);
- irányított részecske energia (pl. koherens, párhuzamos fénynyaláb → lézer; irányított nukleáris sugárzás → mézer; stb.);

[28] Nem szükségszerű, hogy a lövedék a cél által elfoglalt térrészt elérje, vagy abba behatoljon, bizonyos esetekben elegendő, hogy a cél közelében szabaduljon fel a károsító energia (pl. az időzítő, vagy közelségi gyújtóval rendelkező robbanó lövedékek)

[29] Mind a célzási pont, mind a találati pont valóban pontszerű kiterjedésnek tekinthető, amennyiben a károsító energia nem másodlagosan ható energia felszabadításból származik (pl.: robbanó lövedék robbanása)

[30] Egyes felfogások szerint a lövésfolyamat kezdetének nem a lövés kiváltását, hanem a célnak a lövész által való megirányzását kell tekinteni, mert az ettől az időponttól kezdődő történések mind befolyásolják a lövésfolyamatot. Amennyiben a célzást lövés követi ez a gondolatmenet maradéktalanul elfogadható. A probléma akkor keletkezik, ha a célzást nem követi lövés, mint ahogy az a gyakorlatban sokszor előfordul. Természetesen, ha nem így történik valóban célszerű a lövésfolyamatot a célzástól vizsgálni.

- speciális energia (pl.: hullám energia, az alacsonyfrekvenciás hanghullámok által keltett 3-7 Hz-s test-önrezgés → infrahang), ezeket az energiákat elsődlegesen hatónak neveztem el (és E jellel jelölöm), mert már a lövéskor felszabadulnak.
- kémiai energia felszabadulásából származó energiák (mozgási-, hő-, nyomás) alapvetően a robbanó lövedékek és ezek repeszhatása;
- nem irányított nukleáris energia, amelyeket a lövedék találati pontba érkezése szabadít fel, és ezért másodlagosan hatónak neveztem el (és M jellel jelölöm) azokat (pl. a robbanó lövedékek, stb.).

Természetesen ezek az energia fajták egyenként, vagy tetszőleges kombinációkban is alkalmazhatók, de a károsító képesség megítélése szempontjából csak az az energiafajta veendő figyelembe, amely a harcképtelenséget ténylegesen okozza.

Megvizsgáltam végül, hogy ha a lőfegyver nem a hagyományos lőpor-energiát hasznosító fegyver, akkor a ballisztika klasszikus négyes felosztása (bel-, átmeneti-, kül-, és célballisztika) mennyire tartható fenn.

Megállapítottam, hogy:

- az átmeneti ballisztika kivételével a bel-, kül-, és célballisztika[31] (ha némi áttétellel is) a transzportáló energia fajtájától és a lövedék jellegétől függetlenül használható fogalmak;
- a fegyverben, mint transzportáló energia (és esetenként károsító energia) előállító gépben történő folyamatok leírására alkalmas a belballisztika, függetlenül attól, hogy ez a folyamat csőben, vagy más (de ugyanazt a célt szolgáló) szerkezetben megy végbe, ugyanígy lényegtelen, hogy a transzportáló energia az a. – e. keletkezési mód melyikéből származik;
- a lövedék, függetlenül attól, hogy α, vagy β csoportba tartozik, röppályát leírva kerül a célba, és ezen a röppályán a környezettől függő hatások érik, tehát leírása a külballisztika feladata;
- a lövedék, bármelyik típusú is, a célban hatást fejt ki, mely hatás a lövedék károsító energia átadási képességétől függ. Tehát leírására alkalmas a célballisztika fogalma.

A felsoroltakkal bizonyítottam – függetlenül attól, hogy az elemzésem szoros tárgyába tartozik-e vagy sem –, hogy minden lőfegyverre (ha nem is azonos mértékben és részleteiben is azonos eszközrendszert alkalmazva) igaz, hogy lövésfolyamata során a jelenségek leírására a ballisztika klasszikus négyes felosztását alkalmazni lehet.

Az eszközrendszer felállításához végül az «1» – «6» megállapításokat összevetettem az előbbi meggondolásokkal és azokat úgy összegeztem, hogy az általam felállított eszközrendszerre igaz:

7. „az egyik embercsoport harcosai a csoport akaratának egy másik embercsoportra való rákényszerítése érdekében olyan módon befolyásolják a másik csoport általuk veszélyesnek ítélt egyedeit, hogy ellenállás képtelenné váljanak, és ehhez lőfegyvert használnak, mely a harcképtelenséget olyan energiaátviteli módszerrel éri el, amely erre a célra lövedéket alkalmaz és ez a lövedék a célszemélynek fizikai/lelki traumát okoz”.

Az eszközrendszer elemei tehát:

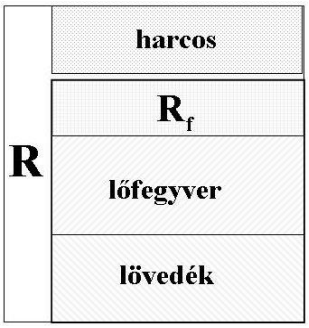
[31] Nem lehet kétséges, hogy amikor a lövedék elhagyja a fegyvert (és a röppályán való útját épp megkezdi) olyan hatások érik, melyek egyrészt a fegyvertől való elszakadásából, másrészt az új környezeti közegbe való belépésétől függenek és nem teljesen azonosak a külballisztika által figyelembe vett hatásokkal. Mindezek alapján kijelentem, hogy az átmeneti ballisztika fogalmára is szükség lesz, ha a teljes lövésfolyamatot precízen kívánnánk leírni.

- a harcos
- a lőfegyvere
- a lövedéke, melyek együttesen képesek a «7» megállapításban foglaltak teljesítésére.

Nem pusztán olyan megfontolásból, hogy a rendszer egyetlen tudatos eleme a harcos, aki akaratát a tárgyi elemeken keresztül vetíti ki, hanem a valóságos viszonyoknak megfelelően a lőfegyvert és a lövedéket a rendszeren belül kételemű részrendszernek tekintettem. Döntésem megalapozottságát azzal bizonyítom, hogy

- a részrendszer elemei szoros összefüggésben állnak egymással és bizonyos feltételek hiánya esetén nem cserélhetők másra[32];
- a humán tényező sokkal tágabb peremfeltételek között cserélhető a részrendszerhez;
- a rendszert jellemző pontosságot a humán tényező csak a részrendszeren keresztül tudja befolyásolni, annak elemein keresztül közvetlenül nem.

Az általam bevezetett R eszközrendszer tehát a következőképp épül fel:



1. ábra az R elemi eszközrendszer elemei

ahol az R_f jelölésű fegyver–lövedék rendszer az R rendszer részrendszere.

Ezzel meghatároztam azt az érdemben vizsgálható elemi eszközrendszert, amelyiket lehetséges a funkcióanalízis eszközeivel vizsgálni.

A harc «7»-ben meghatározott célját szem előtt tartva, az R eszközrendszert a mai korra alkalmazva, napjaink haditechnikai eszközparkját figyelembe véve a következő pontosításokat vezettem be:

- harcosnak a lövészkatonát;
- lőfegyvernek a lövészkatona alapvető lövészfegyverét[33];
- lövedéknek az egyesített tölténybe[34] szerelt lövedéket tekintem.

Ezzel a változtatással a harc «7»-ben meghatározott jellege nem más, mint a lövészkatona alapvető lőfegyverével lefolytatott tűzharc (lövész tűzharc), amelyet a következő R_f részrendszer jellemez a XXI. század elején:

[32] Például könnyen belátható, hogy nem lőhető ki minden lövedék bármely fegyverből

[33] A lövészkatona alapvető lövészfegyvere a XX. – XXI. század fordulóján a gépkarabély, vagy a rohampuska, 5–8 mm közötti űrméretben.

[34] A modern lőfegyverek szerelt töltényt használnak, amelynek csak egyetlen eleme a lövedék. Mégis ragaszkodom a lövedékhez, mint rendszer részelemhez, mert a töltény többi eleme csak a töltés-ürítés és a belballisztikai folyamatok leírásakor kap szerepet.

- a lőporgázok elégetéséből származó gázok munkavégző képességét felhasználó kézi lőfegyver, ez a fegyver alkalmas a lövésfolyamat korlátozott számú reprodukálására;
- egyesített töltény, amely fém hüvelyébe van elhelyezve a lőpor, valamint a hüvelybe szerelve a csappantyú és a lövedék.

A LÖVÉSZ ALAPVETŐ LÖVÉSZFEGYVERÉNEK ELEMZÉSE

A kérdést tovább vizsgálva a lövész alapvető egyéni lőfegyveréről a következő megállapításokat tettem.

A lövész alapvető egyéni lőfegyvere az általános nemzetközi (alapvetően nyugati) terminológiát alkalmazva a rohampuska (más terminológiák szerint: gépkarabély). A jelenleg használt rohampuskákat vizsgálva kimondható, hogy vannak olyan közös jellemzőik, amelyekkel egy úgynevezett általános rohampuska leírható. A továbbiak ezzel, a csak elméletileg létező rohampuskával foglalkozom.

Mi a jellegzetessége ennek a fegyvernek. Az eddig lefektetett elméleti alapokra támaszkodva kijelenthető:

- a fegyver lövedéket lő ki, tehát lőfegyver;
- a transzportáló energiát kémiai úton (lőpor elégetéséből) nyeri, tehát tűzfegyver[35];
- a fegyver „α" típusú lövedéket lő ki, mert a lövedék mérhető formájú és tömegű, pontosan leírható szerkezetű tárgy;
- a fegyver a károsító energiát a „b" módszerrel juttatja a célba, mert a lövedék mozgási energiáját használja a károsító energia transzportálására;
- a lövedék a károsító energiát az „E" módszerrel közvetíti, amely egyenlő a lövedék célban mért mozgási energiájával.
- az energiatermelés a fegyverben, ezen belül a fegyvercsőben zajlik le, tehát belső égésű erőgépnek (motornak) tekinthető[36];
- a fegyver alkalmas a lövésfolyamat reprodukálása többféle tűznemben[37] is;
- a fegyverhez szükséges lövedékmennyiséget a fegyverhez kapcsolható (vagy rászerelt) tartozékban (tárban) tárolja.

A rohampuska elemzéséhez szükségesnek tartok még egy rövid fegyverszerkezeti kitérőt. Mindenképpen elemezni szükséges a további értékelésekhez a tűzfegyverek viselkedését (a majdani értékelési jellemzők konkretizálásához) a lövésfolyamat reprodukálása során.

Legelébb is le kell szögezni, hogy a tűzfegyver olyan hőenergetikai gép, amely alapvetően csak szerkezeti kialakításában különbözik egy belső égésű motortól, hőtani elveiben nem.

---

[35] Fontos megemlíteni, hogy bár az energiaátalakítás a fegyverben megy végbe, a transzportáló energia hordozója (a lőpor) nem a fegyver, hanem a lövedék tartozéka. Az egyesített tölténynek (röviden tölténynek) nevezett szerkezeti egység tartalmazza a lövedéket, a lőport, a csőfar tömítésére szolgáló és az alkatrészeket egybefogó hüvelyt, valamint a lőporégés kiváltását biztosító iniciáló elegyet befogadó csappantyút. A tűzfegyverek az alapvető lövészfegyverek hosszútávon elképzelhető családjának csak egy szegmensét adják, annak ellenére, hogy jelenleg ez a szegmens a családon belül az abszolút domináns. Annak a kérdésnek a boncolgatásától, hogy a lövésfolyamatra milyen hatással vannak a töltény és alkatrészei (a lövedék kivételével, mert azt részletesen elemeztem) inkább eltekintenék, mert a lövedéket tartom a töltény igazán meghatározó részének. Az ugyanis a tapasztalatom, hogy egy adott lövedékhez általában a maximálisan kihasznált lőpor- csappantyú-hüvely kombinációt alkalmazzák, legalább is addigra, mire a töltény valóban sorozatgyártásra kerül. Kijelenthetjük tehát, hogy a lövedék elvárásai meghatározzák a töltény többi elemének minőségét.

[36] Az ideális csőhossz meghatározásához tudni kell, hogy a sebesség-út függvény görbéje egy bizonyos csőhossz felett már meglehetősen lapos, tehát az energiaszint emelkedés minimális. Ugyanakkor legalább olyan hosszú cső szükséges, hogy a rendelkezésre álló térben biztosan a teljes lőpormennyiség elégjen.

[37] Lásd a lövésfolyamat reprodukálásával foglalkozó gondolatokat az azzal foglalkozó bekezdésben alább!

Könnyen belátható, hogy a henger a fegyvercső, a dugattyú a lövedék, az üzemanyag a lőpor, a gyújtóelem a csappantyú. A tűzfegyverek működésének (a lövésfolyamat fenntartásának) biztosítása érdekében mindenképpen elengedhetetlen, hogy a lövedék mozgásvektorával ellentétes irányba a cső vége (csőfar) megbízhatóan (gáztömören, vagy a lehető legkisebb mértékű gázkifúvás mellett) le legyen zárolva. Egészen addig a jól meghatározható Δt_z ideig, amíg a lövedék az átmeneti ballisztika zónáját elhagyva, a külső ballisztika által meghatározott röppályára[38] tér. A lezárolásnak viszont olyannak kell lennie, hogy lehetővé tegye a lövésfolyamat reprodukálását is. Különösebb műszaki részletezések nélkül a tűzfegyverek zárolására a következő módszerek terjedtek el:

- a merev zárolás, amikor Δt_z ideig a csőfar és a zároló szerkezet zárt hatásláncban, mechanikus kötésbe kerül egymással (mereven reteszelt rendszerek). A zároló szerkezet kioldását (kizárolás) mindig külön gázmotor végzi[39] (gázelvételes rendszer);
- tömegzárolás, amikor a csőfar zárolását a zárolótest (tömegzár) tömegének tehetetlensége biztosítja[40] (szabad tömegzáras rendszerek);
- a két előbbi mód kombinálásával, amikor a zár tömege a csak egy ($<\Delta t_z$) ideig fennálló merev reteszelés miatt számottevően csökkenthető (késleltetett tömegzáras[41] rendszerek), ezeknél nincs gázmotor.

A rohampuskáknál a szabad tömegzáras rendszereket, a viszonylag nagy lövedékteljesítményekből adódó nagy zártömegek miatt, nemigen lehet alkalmazni.

A lövésfolyamat reprodukálása szempontjából azt is szükséges megvizsgálni, hogy milyen folyamatok játszódnak le a reprodukálás érdekében. Mivel a lövésfolyamathoz minden esetben egy transzportáló energia hordozó elemet és egy lövedéket kell az energia-átalakítóba (a fegyvercsőbe) juttatni, a lövés feltételeit biztosítani kell, majd ezután a felesleges segédanyagokat a lövés után onnan el kell távolítani, a folyamat ütemezése könnyen felírható:

töltés → lezárolás → lövés → kizárolás → ürítés

Amennyiben, mint jeleztem, a tűzfegyver működését egy belső égésű motorénak feleltetem meg, itt is meghatározható, hogy jelen esetben (és ezt az esetet tekintve általánosnak) ez egy ötütemű folyamat, melynek:

- első ütemében megtörténik a lövedék fegyvercsőbe történő juttatása (pl. a tölténytárból), a hagyományos kialakítású egyéni lövészfegyverekre jellemző módon, a zároló elem fegyvercső irányában történő mozgásával;
- második ütemében megtörténik a fegyvercső lezárolása a zároló elem és a fegyvercső szilárd összekötésével (közvetlenül, vagy közvetítő szerkezeti elem útján);

[38] Egyáltalán nem szükséges viszont, hogy ekkorra a lőporgázok nyomása *teljes mértékben* a környezeti nyomásra csökkenjen a fegyvercsőben.

[39] Gázelvételes rendszer. A fegyvercső meghatározott helyéről a lőporgázok egy szükséges mértékű hányadát gázhengerbe vezetik, ahol expandálva az energia - mozgási energia formájában - egy gázdugattyúnak adódik át. A gázdugattyú működteti a zároló szerkezet kioldó mechanizmusát.

[40] Már a lövésből származó impulzus ismertetésénél kifejtésre került, hogy az impulzus-tétel értelmében a lövedék megindulásának pillanatában az impulzust átvevő elem is megmozdul (jelen esetben ez a tömegzár). Megfelelő tömítési rendszerekkel (hüvelykonstrukció), valamint a zár tömegének meghatározásával elkerülhető, hogy lényegesebb gázkifúvást okozhasson a zár megmozdulása.

[41] Késleltetni alakos kötéssel, aszimmetrikus lengőkarok alkalmazásával, excentricitással, stb. szokásos.

- harmadik ütemében leadásra kerül a lövés az elsütőberendezés működtetésével (a megfelelő szerkezeti elem[42] a csappantyúra ütve iniciálja a lőpor égését);
- negyedik ütemében oldásra kerül a zárolási szilárd kapcsolat;
- ötödik ütemében kivetésre kerül a lövésfolyamat hulladéka (itt a töltényhüvely) a záró elem fegyvercsőtől távolodó mozgásával és általában ebben az ütemben töltődik fel energiával az elsütőberendezés végrehajtó eleme és a zármozgatás energiahordozója is.

A bemutatott ötütemű működésre egyaránt példa a gázelvételes, merev reteszelésű fegyverszerkezet és a késleltetett tömegzáras is. Jellemző továbbá, hogy a lövész a lövésfolyamat megindítására szolgáló akaratát a harmadik ütemben közli a fegyverrel, az elsütőberendezés működtetése[43] útján. A folyamat lejátszódásához szükséges idő meghatározásához figyelembe kell venni, hogy a rohampuska töltények viszonylag hosszú méretűek (továbbá az elcsettent[44] töltényt ki kell üríteni, általában kézzel működtetve, tehát az ürítési úthossz sem lehet kevesebb, mint a töltési) a fegyverből, tehát a töltés-ürítéshez szükséges úthosszak viszonylag nagyok, ezért időigényesek. Nem elhanyagolható az a tény sem, hogy az ürítés megkezdésekor a zárszerkezetnek álló helyzetből kell felgyorsulnia, amely természetesen több időt igényel, mint a mozgásban („repülőstarttal") megkezdett (pl.: zárolási) folyamat kezdet. A szükséges részidők megszabta teljes tűzütem-idő[45] ráadásul nem egyenletes, sőt a sorozatlövés kezdetekor nagyobb, mint a sorozat közben.

Más rendszereknél az ütemszám csökkenthető, tehát a tűzütem is csökken, az időegység alatt leadott lövések száma (a tűzgyorsaság[46]) nő. Merev ütőszeges szabad tömegzáras zárolásnál a háromütemű működés a jellemző, mert a be és kizárolás üteme elmarad (nem kell külön szerkezetet működtetni). Szabad tömegzáras rendszereknél a lövész az akaratát az első ütem megindításával viszi át a fegyverre[47]. Ezt a megoldást, tekintettel arra, hogy lövésre kész állapotban a töltény nincs a fegyvercsőben, nyitott töltényűrűnek (open bolt) nevezik, előnye, hogy a fegyvercsőfurat két nyitott vége miatt a csőfurat hűtése[48] jó.

A lövésfolyamat ütemszámának a sorozatlövés részletes elemzésénél van fontos szerepe, tekintettel arra, hogy a folyamat lejátszódásához idő szükséges és ez az idő a folyamat ütemszámával egyre emelkedik[49].

---

[42] Általában az ütőszeg (önálló, vagy a kakasba, vagy ütőtömbbe épített ütőhasáb)

[43] Zárt töltényűrű rendszernek is nevezik, mert a lövedék mindig és teljesen lezárolt állapotban várja, hogy a lövész kiváltsa a lövést.

[44] Hiába ütött a megfelelő szerkezeti elem a csappantyúra a lövésfolyamat nem indult meg, akár a töltény hibáiból, akár azért, mert az ütés energiája kevés volt a csappantyú működtetéséhez.

[45] A folyamatos sorozatlövés két lövése között eltelt átlagos időt nevezzük tűzütemidőnek, vagy röviden tűzütemnek.

[46] Általánosan a percenként leadható lövésszámot nevezzük tűzgyorsaságnak.

[47] Az elsütőbillentyű elhúzásával a tömegzár testét indítja útjára. A zárba mereven, vagy lazán szerelt ütőszeg a töltény betöltésének végén azonnal megindítja a csappantyút. Merev ütőszeg esetén a gyújtás már valamivel azelőtt megkezdődik, hogy a töltény teljesen kitöltené a csőfuratban számára kialakított helyet, a töltényűrt (előgyújtásos rendszer), de a gyújtási idő és a tehetetlenségek miatt a lövés szinte a teljesen zárolt állapotban történik meg, nem előtte.

[48] Ugyanakkor azonban pontos lövés céljára ilyen zárolás nem alkalmazható, a nagy zártömeg hirtelen lefékezéséből származó bólintó nyomaték miatt, ami elrántja a csőfurat tengelyét is.

[49] A merev reteszelésű fegyverek tűzgyorsasága alacsonyabb, tűzüteme magasabb, mint a szabad tömegzárasaké, de a legmagasabb tűzgyorsaságot (klasszikus felépítésű fegyverek esetében) az előgyújtásos rendszer szolgáltatja.

A jelenleg használt rohampuskák mindegyike a lövésfolyamatot automatikusan reprodukálja, olyan módon, hogy a lövész döntésétől[50] függ a reprodukálás:

- öntöltés (egyes lövés), az elsütő elemeket[51] minden lövés előtt a lövésznek külön működtetni kell;
- sorozatlövés, a lövés-ismétlések automatikusan követik egymást a sorozat hossza (az automatikusan egymást követő lövések száma) a lövész elhatározásától[52] függ, kivéve, ha közben a rendelkezésre álló tölténymennyiség elfogy;
- tűzlökés, azaz a fegyvermechanika által megkötött (2-3) lövésből álló rövid sorozat.

Minden fórumon (szakmai értekezletek, konferenciák, lövészeti bemutatók, valamint itt idézni nem kívánt cikkeim) rendszeresen kihangsúlyoztam azt a nézetemet, hogy a rohampuskák alapvető használati módja az öntöltő puskaként való alkalmazás. A sorozatlövés képessége a közelharc (legfeljebb 25 m) és abban a viszonylag zártan közeledő ellenség leküzdésére lenne igazán használható, távolabbról értelmetlen[53]. Hiába hivatkozik bármely ellenvélemény arra, hogy nagy távolságból is lehet rövid sorozat lövéssel eredményt elérni, mert az a valóságos helyzet, hogy ez a találat, mindig a sorozat első lövéséből származik. Ugyanis ez a lövés fegyver műszaki szempontból egyes lövésnek számít, mert mire a töltő-ürítő mechanizmus működésbe lép, a lövedék már kilépett az átmeneti ballisztika zónájából, a fegyvercső térbeli elmozdulása már nem hathat rá. Nos, emiatt nincs sok értelme a nagy lövésszámú sorozatlövésnek a modern harcmezőn, mert felesleges lőszerpocsékolás nagyszámú lövedéket útjára bocsátani, hátha „beleakad" valaki. Ma már nem „divat" sűrű zárt tömegekben szembetámadni az ellent! Ez a megállapítás fokozottan igaz a honvédség AMM típuscsaládba tartozó gépkarabélyaira[54], mert ezt az AK fegyverszerkezetet alapvetően öntöltő karabélynak tervezte M. Kalasnyikov, a sorozatlövést kiegészítő, önvédelmi üzemmódnak[55]!

Természetesen a sorozatlövés-hatásosság megítélésének az alapja is a pontosság, azzal kiegészítve, hogy a sorozatban leadott lövések nyomán hány lövedék csapódik a cél felületébe. Az R rendszer pontosságának egyik legfontosabb meghatározója, mint már az előzőekben kitértem rá, az a képesség, hogy a fegyvercsőfurat tengelye milyen mértékben változtatja meg a helyzetét a lövéskor, a célzás során elfoglalthoz képest (a lövedék kezdősebesség v_0 vektorának térbeli helyzetét jelöli ki), azaz mennyire tér el a lövedék tényleges röppályája a tervezettől[56] [7].

---

[50] Az erre a célra kialakított, általában egy darab kezelőelem (tűzváltó) beállításával. Egyes esetekben (Steyer AUG) a tűznem váltása az elsütőbillentyű elhúzási hosszának megváltoztatásával történik.

[51] A rohampuskáknál és a lövész oldaláról ez az elsütő billentyű.

[52] Ameddig az elsütőbillentyűt működteti (el nem engedi).

[53] Különösen igaz ez a 7,62 mm-es AK rendszerű gépkarabélyok használatára! A HTI táborfalvai lőterén lőkísérlet-sorozattal igazoltuk, hogy átlagos és annál jelentősebben jobb képességű lövészek sem voltak képesek 50 m lőtávolságon fekvő testhelyzetből egynél több találatot elérni a mellalak méretű célban.

[54] Némiképp árnyalja a képet, az AKM-63F gépkarabélyunk NAMZA SOW alapján végrehajtott fegyver modernizálása (AK-63FM), amely során a felszerelt mellső markolat/bipod alkalmazásával váratlan, szinte ugrásszerű pontosság javulást érhettünk el, még hosszú sorozatok fekvő testhelyzetben való lövésekor. Lásd: a következő, ötödik bekezdésben! Részletesen megadva az eredményt és a műszaki megoldást. Az eredményeket a videofelvételek és az elkészült jegyzőkönyvek egyaránt tartalmazzák.

[55] Az 1994. novemberi C+D kiállításon történt beszélgetésünkből személyesen tőle származó információ.

[56] Elmozdulás mindig van, azonban csak akkor érdemes figyelembe venni, ha olyan mértékű röppályaváltozást okoz, amely már veszélyezteti a cél eltalálhatóságát. A sorozatlövés során a pontosság követelménye azt jelenti, kívánatos, hogy a kilőtt lövedékek minél nagyobb hányada csapódjon a cél felületébe. Az elmozdulásból keletkező röppályaváltozás ugyanakkor azt is jelenti, hogy a pontosság (egy adott rendszernél) szigorúan lőtávolságfüggő, az egymást követő röppályák görbeseregének széttartása miatt.

A rohampuska sorozatlövés közbeni viselkedése minden egyes fegyvertípus esetében más és más. Általánosan csak az állapítható meg, hogy a viselkedést (ha a lövész kondícióját konstans értéknek tekintjük) az adott R_f (fegyver-lövedék) részrendszer kölcsönhatásai, ezen belül legfőképpen a fegyver ergonómiai és szerkezeti kialakítása határozza meg, mert a részrendszer hatásai a lövész azon képességét rontják, hogy a fegyvert lövéskor a célzással meghatározott térbeli helyzetben megtartsa.

A fegyverszerkezet bőségesen tartalmaz mozgó mechanizmusokat, főleg lengő rendszereket (a töltés-ürítéshez, elsütéshez, stb.). Ezek mozgásjellemzőinek és a lövésből származó hátralökésnek a pillanatnyi eredője[57] terheli a lövészt. Az R_f részrendszer figyelmen kívül nem hagyható hatásai megítélésem szerint a következők:

- a lövedék torkolati energia és a fegyvertömeg viszonya meghatározza a hátraható erőt[58], azaz az elugrási hajlamot, főleg annak mértékét;
- a fegyvercső furat tengelyének és a válltámasz (tusa[59]) lövészhez támaszkodási pontjának térbeli helyzetének eltérése határozza meg a csőelugrás jellegét, az előbbivel együtt a mértékét;
- a sorozatlövés tűzgyorsasága meghatározza a lövészre ható káros rezgések periódusát[60];
- a fegyvermechanizmus kialakítása meghatározza a fegyverlengés jellemzőit[61];
- az R_f alrendszer dinamikus tömegközéppont vándorlása[62] befolyásolja a fegyver kézben tarthatóságát.

Mindezen hatásokat komplexen elemezve megállapítható, hogy nagy tűzgyorsaságú, kis lengő tömegeket tartalmazó fegyver (főleg ha a töltött tár tömegközéppontjának függőleges hatásvonala a fegyver tömegközéppontjának környezetébe esik), amennyiben a fegyver/lövedék tömegarány is jól megválasztott, sokkal jobb pontosságot fog produkálni sorozatlövés esetén is, mint abban az esetben, ha ezeket a kérdéseket nem tanulmányozták kellő gondossággal. Tekintettel arra, hogy a sorozatlövés során a lövedékek által bejárt röppályák a

---

[57] Az erőhatás vektorának térbeli helyzete, valamint a vektor nagysága is pillanatról pillanatra változik.

[58] A torkolati energiából számítható lövedékimpulzus a tömegarányoknak megfelelő fegyverimpulzust ébreszt. Tehát, ha a fegyver hátralökő impulzusát a lövész az időben el tudja húzni (nem merev fegyver megfogással, hanem elmozdulásának biztosításával, majd e mozgás megfelelő mértékű lefékezésével) akkor lényegesen csökkenthető a hátralökő erő nagysága. Gyakorlott lövők ezt a fegyverrel szembeni engedékenységükkel érik el. A hátramozgás során azonban mindenképp biztosítani kell, hogy a fegyvercső csak a saját tengelyében mozduljon el, mert ekkor nem kell röppályaváltozással számolni.

[59] Helytelen a tus kifejezés, főleg a számos más, félreérthető jelentés miatt, a kézi lőfegyvernek tusája van!

[60] Minél magasabb a tűzgyorsaság, annál kevésbé érzékeny (tehetetlensége miatt) a lövész teste a hátralökések hatására. Minél rövidebb a tűzütem, időegység alatt annál több lökés éri a lövészt, amelyet emiatt kevésbé érzékel ütésnek, inkább egybefolyó tolásként, amit nem akar görcsös igyekezettel kompenzálni. Emellett célszerű a test (törzs) 4 - 8 Hz-es önrezgésszámától [10; 2-234 old.] minél jobban elhangolni a sorozatlövés okozta rezgés frekvenciáját (f_t = percenkénti lövésszám/60 |Hz|). Sajnálatosan a rohampuska kategóriában általános 600 lövés/perc tűzgyorsaság 10 Hz rezgéssel terheli a lövész karjait. Ilyen szempontból a 900-1100 lövés/perc tűzgyorsaság sokkal ideálisabbnak tekinthető, mert elhangolt még a felharmonikusoktól is.

[61] A zárolást végző (teljes) szerkezet tömege és a mozgás végpontjain mérhető sebessége határozza meg, hogy milyen ütésszerű terhelést ró a lövészre. Lágy ütközőkkel az ütés mértéke csökkenthető. A rángatás mértéke attól is függ, hogy a nagytömegű elemek lengésének síkja milyen messze esik a fegyver eredő tömegközéppontjától. Az oroszok készítettek olyan fegyverszerkezetet is, ahol a zárszerkezet két darabja ellenirányba mozog (boxer), a lengésből származó nyomatékok némiképp kioltják egymást. Azonban nem lett követendő példa (ugyan miért?)

[62] A lengőrendszer pillanatnyi helyzete és a töltényfogyás által meghatározott az R_f alrendszer eredő tömegközéppontja által a térben egy görbefelületen leírt folyamatos mozgás, melynek pillanatról, pillanatra változó dinamikai jellemzői (az ébredő erő vektorának iránya, értelme és nagysága) határozzák meg a lövész terhelését.

lövésszám emelkedésével egyre inkább széttartóvá válnak, valamint a lövészre ható terhelés a tűzgyorsaságtól is függ, mert nagy tűzgyorsaság mellett az emberi test tehetetlensége a rendszer pontosságának megtartása irányába hat, érthetővé válik a tűzlökés, mint tűznem bevezetése és annak továbbfejlesztése a tűzlökés alatti emelt tűzgyorsasággal. A röppályák széttartása azonban az egyeslövéshez képest mindig lényegesen alacsonyabb hatásos lőtávolságot biztosít sorozatlövésnél.

Ugyancsak ehhez a kérdéskörhöz tartozik egy néhány éves újdonság, a rohampuska villaállvánnyal való felszerelése. A 7,62 mm-es AMM gépkarabélyunk modernizálási kísérletei során a mellső faágy helyett felszerelt Picatinny sínrendszer alsó sínjére felfogott markolatba rejtett bipod állványon feltámasztott gépkarabéllyal a hosszú, harminc lövéses sorozattal, fekvő testhelyzetből, 100 m céltávolságra, az állóalak méretű céllapra minden egyes lövedékkel találatot tudtunk (kollégáim és én is) elérni! Csak gyakorlás kérdése volt ez az egész.

Az ezredforduló általános egyéni lövészfegyverének tekintett rohampuska (gépkarabély) nagy részletességű elemzését az [5] és [7] – [9] tanulmányaimban már elvégeztem, amelyekben részletesen foglalkozom a fegyver szerepével a harcban, és kifejtem gondolataimat a pontosság, a hatásosság és a használhatóság képességekről, minden esetben számszerűsítve azokat.

KÖVETKEZTETÉSEK

Mindenesetre, mintegy összefoglalásként megállapítom, hogy a modern rohampuska működési elvét tekintve messze nem követte a haditechnika sem XX. századbeli, sem XXI. század eleji forradalmát. A rohampuska még mindig az évszázadok óta ismert és alkalmazott (és feltehetően lehetőségeinek a végéhez igen közel érkezett) károsító energia transzportáló módszert és lövedék típust alkalmazza, mert még mindig a lőporgázok égéséből nyert mozgási energiával hajtott tömeggel bíró lövedék becsapódási energiáját használja fel az ellenség harcképtelenné tételéhez, továbbá ez a lövedék ballisztikus röppályán jut el a célba. Ennél a műszaki megoldásnál a lövedék röppálya befolyásolására, a biztos találathoz szükséges mértékű módosítására – miután a lövedék elhagyta a fegyver csövét – nincs mód. Az alkalmazott módszernek az a legnagyobb hátránya, hogy viszonylag alacsony a hatékonysága, mert átlagos harctéri helyzetet alapul véve a cél(ok) folyamatos mozgása, illetve fel és eltűnése erősen nehezíti a korrekt célzást. Azonban még korrektnek tekinthető célzás mellett sem garantálja a ballisztikus röppálya a biztos találatot, hiszen a lövedék, repülése közben, folyamatosan ki van téve a környezet hatásainak, tehát a röppálya alakja a behatások mértékének megfelelően módosul. A módosító tényezők sem állandóak sem az idő, sem a tér függvényében, mert a lövedéket érő mindig más eredő hatással kell számolni és ezek a változások a legkevésbé lineárisak, sokkal jellemzőbben váratlanok, mondhatnánk kiszámíthatatlanok. Főleg nagy lőtávolságokon várható az R rendszer pontosságának jelentős csökkenése. A harcmezőn azonban az van előnyben, aki messzebbre és pontosabban lő. Bár a viszonylag pontatlan R rendszerek alkalmazásakor a tűzsűrűség[63] növelése némiképp javíthat a helyzeten. A tűzsűrűség a lövészek számának növelésével[64], illetve a lövésfolyamat folyamatos reprodukálásával (sorozatlövés) növelhető. Természetesen a sorozatlövés szórásképe döntő hatással van a

[63] A tűzsűrűség (itt: találati sűrűség, vagy harcitűz sűrűség) egy adott felületegységre eső találatok száma. Eloszlása korántsem egyenletes, hanem az egyes lövészekhez rendelt R rendszerek találati képének eredője. Szoros összefüggésben van a célok felületegységre eső számával, a célsűrűséggel, mert a célsűrűség növelésével a tűzsűrűség csökkenthető.

[64] Ekkor viszont a saját célsűrűség nő, manapság viszont nem támadnak sűrű zárt tömbben!

valóságos tűzsűrűségre[65]. A sorozatlövéssel létrehozott tűzsűrűség növelés viszont erősen apasztja az amúgy is mindig kevésnek bizonyuló lőszerkészletet[66]. Be kell látni tehát, hogy a pontos találat lehetőségének biztosítására – a hatásos lőtávolságig és szélsőséges, gyorsan változó környezeti körülmény között – az ezredforduló rohampuskái/gépkarabélyai egyszerűen alkalmatlanok. Bár kétségtelenül igaz, hogy a lövedék kezdősebességének drasztikus emelésével[67] a pontossága és a hatásosság némiképp növelhető (ugyanakkor a még elviselhető hátralökés érdekében a lövedéktömeget csökkenteni kell![68]), de a környezet zavaró hatásai ekkor sem kerülhetők meg.

Összefoglalva: az ezredforduló rohampuskája és annak lövedéke (az R_f alrendszer) még igen távol van az ideálistól, ugyanakkor az R rendszer ezen R_f alrendszer alkalmazásával érezhetően a lehetőségeinek határához ért. Természetesen továbbfejlesztéssel az R rendszer hatásfoka némiképp növelhető, de igazán forradalmi javulás - meglátásom szerint – reálisan már nem várható el tőle!

Figyelembe véve a károsító energia jellegére, valamint az energia transzponálására vonatkozó megállapításaimat, arra a felismerésre jutottam, hogy a kézi lőfegyverek terén az elmúlt 100-120 év alatt – miközben a haditechnikai más téren hatalmas fejlődést mutatott – műszaki szempontból nem történt érdemi előrelépés. Ezt az állításomat azzal bizonyítottam, hogy a károsító energia-fajta felhasználásának legalább 5 módjából még mindig csak egyet (b.), az energia transzportáló elem fajtából még mindig csak az elsőt (α) és az energiaközvetítés egyetlen módszerét (E)[69] alkalmazzák a rendszeresített alapvető lövészfegyverek, függetlenül minden modernizálásuktól[70].

Megállapítottam, hogy a haditechnika elmúlt száz év alatti viharos fejlődéséből épp az alapvető lövészfegyverek fejlődése maradt ki a technikai szintnek legalábbis megfelelő mértékben.

Elemzésemben azt is kimutattam, hogy a pontosság hiányát esetleg lehet pótolni a tűzsűrűség növelésével, de az erre a célra szolgáló sorozatlövés nagyságrendekkel kisebb pontosságot eredményez a fegyvermechanika működéséből keletkező hibanyomatékok kitérítő hatása miatt.

---

[65] Sorozatlövéskor felfelé erősen elmozduló fegyver egy adott lőtávolságon túl alkalmatlan a tűzsűrűség növelésére, legfeljebb a harctér mélységében. AK rendszerű gépkarabélyokkal is csak közvetlen közelre (25 m-en belül), vagy akkor érdemes sorozatlövést leadni, ha az ellen meredek domboldalon jobbról balra lefelé támad, és összezárt alakzatban jönnek, mert sorozatlövéskor a fegyvercső erősen elhúz balra, felfelé.

[66] Több ellenőrizhetetlen nyugati forrás alapján egy sebesítő találat eléréséhez majd 50.000 lövést kell leadni. Én ezt az adatot irreálisnak, fordítási hibának, hazugságnak, vagy egyszerűen statisztikai szemfényvesztésnek tartom (lehet, hogy a lövést kapott sérültek számát vetették össze a lőszergyárakból kiadott töltények számával, ami messze nem a leadott lövések száma. Ismereteim szerint az USA a II. világháborúban csak a segélyhelyre bejutott sebesültjein vizsgálta, hogy kézi lőfegyverekből származott-e a sérülés, a halottakon állítólag már nem). Ha ez a szám valós lenne, már rég felhagytak volna a modern hadseregek az egyéni lövészfegyverek alkalmazásával, illetve nem lenne igazolható, hogy terület megtartására és folyamatos ellenőrzésére csak a gyalogság alkalmas. Utánaszámolva (napi 150 töltény javadalmazás alapján) egy lövészraj több mint egy hónapos folyamatos és intenzív *lövöldözés* után érne csak el egyetlen találatot az ellenségen.

[67] Nő a becsapódási sebesség, stabilabb lesz a röppálya, stb.

[68] 8 g-os lövedék 4 kg tömegű fegyverből csak akkor indítható 1800 m/s sebességgel, ha a fegyver komoly és összetett amortizációs rendszerrel rendelkezik. Amortizáció nélkül pl. egy M16A2-ből 1800 m/s-mal indított SS109 lövedék tömege nem lehet 2,1 g-nál több (ha a fegyverszerkezet a szükséges nyomás nagyságát egyáltalán elviseli). Ezt a lövedéket viszont „elfújja a szél".

[69] Igaz az „M" módszert a nemzetközi szerződések a katonai alkalmazásban általában tiltják, mint "felesleges szenvedés"-t okozót.

[70] A rohampuskához kapcsolt gránátvetők legfeljebb érdekes színfoltot jelentenek (annál a haderőnél, ahol persze alkalmazzák őket), mert megítélésem szerint, egyszerűen egy dobótávolságnál jóval messzebbre elhajított kisteljesítményű kézigránátoknak tekinthetők. És nincs minden rohampuskán ilyen kiegészítő lőfegyver!

Pont a nagy távolságra szükséges pontos találat elérésének lenne legnagyobb akadálya a sorozatlövés.

FELHASZNÁLT IRODALOM

[1] CLAUSEWITZ K.: *A háborúról*; Athenaeum Irodalmi és Nyadai R.-T. Kiadása 1917 második kiadás (reprint Göttinger kiadó Veszprém 1999. 400. számozott példány)

[2] KEAGAN, J.: *A hadviselés története*; Corvina 2002

[3] KEAGAN, J.: *A csata arca*; LAP-ICS 2001

[4] O'CONNEL, R. L.: *A kard lelke*; Gold Book (évsz. nélk.)

[5] FÖLDI F.: *Gondolatok a fegyverek szerepéről a harcban* – Hadmérnök 2006. 1. szám. http://www.hadmernok.hu/archivum/2006/1/2006_1_foldi1.html (letöltve: 2018.02.10.)

[6] SEILLER, K. G.- KNEUBUEHL, B. P.: *Wound Ballistics* (angolra fordította: Ruth Rufer és Jack Hawley) Elsevier Science B.V. Asterdam 1994.

[7] FÖLDI F.: *Gondolatok a pontosságról* (tanulmány) – Hadmérnök 2006. 1. szám http://www.hadmernok.hu/archivum/2006/1/2006_1_foldi2.html (letöltve: 2018.02.10.)

[8] FÖLDI F.: *Gondolatok a hatásosságról* (tanulmány) – Hadmérnök 2006. 3. szám http://www.hadmernok.hu/archivum/2006/3/2006_3_foldi2.html (letöltve: 2018.02.10.)

[9] FÖLDI F.: *Gondolatok a használhatóságról* (tanulmány) – Hadmérnök 2006. 3. számhttp://www.hadmernok.hu/archivum/2006/3/2006_3_foldi1.html (letöltve: 2018.02.10.)

[10] WOODSON-CONOVER: Ember – Gép - Üzem Munkahelytervezés; Műszaki Könyvkiadó 1973.

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

UAV-K ALKALMAZÁSA A KÖZFELADATOK ELLÁTÁSA SORÁN II.

APPLICATION OF UAVs IN PUPLIC SERVICE II.

NÉMETH András

(ORCID: 0000-0003-2397-189X)

nemeth.andras@uni-nke.hu

Absztrakt

Az állami feladatrendszer, valamint az annak szerkezetét és az egyes elemek egymáshoz képesti viszonyát, a funkciók megosztását, a kapcsolati hálót és működést meghatározó komplex jogszabályi struktúra sok tekintetben hasonlítható egy pilóta nélküli légijármű rendszer felépítéséhez és működéséhez. A közfeladatok ellátásáért felelős szervezetek munkájukat akkor tudják hatékonyan végezni, ha az egymásrautaltságból is következő együttműködési kényszernek való megfelelés során, az információcserét, a közös gondolkodást nem akadályozzák a hivatásrendi sajátosságokból eredő értelmezésbeli különbségek. Különösen igaz ez az alkalmazott technikai eszközrendszer esetében, ahol az esetleges ineroperabilitási problémák jelentősen akadályozhatják a kormányzat által meghatározott célok elérését.
Jelen publikáció célja az állami feladatrendszer és az azt hatékonyan támogatni képes pilóta nélküli légijármű rendszerek lehetséges kapcsolódási pontjainak meghatározása, a technikai fejlődés várható irányainak a közszolgálati alkalmazásokra gyakorolt perspektivikus hatásainak feltérképezése, illetve az erre való felkészülés egyes feladatainak meghatározása.

„Az Emberi Erőforrások Minisztériuma ÚNKP-17-4-3-NKE-71 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült”

Kulcsszavak: *állami funkciók, közszolgálati feladatrendszer, társadalom, UAS, UAV, drón*

Abstract

The system of state functions and the complex structure of legal regulations determining its structure and the relationship between each part compared to each other, the division of functions, network and functioning might be compared to the structure and functioning of an unmanned aerial vehicle system in many aspects. The organizations responsible for carrying out public functions can perform their work effectively - while corresponding with the need for cooperation resulting also from the interdependence -, if the differences in interpretation due to the specialties of the different professions do not hinder to exchange information and to think mutually. It is especially applicable in case of applied technical tools, where the occurrent interoperability problems might significantly hinder to reach the goals set by the government. The purpose of this publication is to determine the possible connections between the state functions and the unmanned aerial systems being able to support them effectively, to discover the perspective effects affecting public service applications of the direction of the expected technical development and to determine certain tasks of preparing for it.

Keywords: *state functions, tasks of public service, UAS, UAV, drone*

A kézirat benyújtásának dátuma (Date of the submission): 2018.06.05.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.26.

BEVEZETÉS

A társadalmi fejlődéssel összefüggő kutatások egyik iránya, az egyes korcsoportok különböző generációkhoz való tartozásának meghatározása valamely tulajdonság, nemzedéki tudat és egyéb közösségi jegyek alapján. A közös tapasztalat, helyzetértékelés és cselekvési formák elemzésével a generációváltások ciklusát évtizedekkel ezelőtt 15-20 évre becsülték. [1][2] Erre építkezve, a társadalom és a technológia viszonyát is figyelembe vevő kutatások, amelyek az információs forradalom hatásait, és az ebből eredő új kihívásokat [3] is elemezték, megalkották új modelljeiket, az X, Y és Z generációk fogalmát és ismérveit. Ezek szerint az X generáció (60-as,70-es években születettek) „digitális bevándorlónak" tekinthető, az ő fiatalságuk ideje alatt kezdődött a mai digitális korszak kialakulása. Az Y generáció (80-as, 90-es évek) tagjai alkotják az „első digitális bennszülöttek" halmazát, akiknek már tejesen természetes a digitális vívmányok mindennapi használata, és életüket a valós és virtuális világban sokszor párhuzamosan élik. A Z generáció (ezredforduló után születettek) tekinthető a „facebook-nemzedéknek", tagjai az „igazi digitális bennszülötteknek, akiknek az internettől és a közösségi médiától való függőség az egyik legfontosabb ismérvük, szociális, társadalmi viszonyaik gyökeresen különböznek az idősebbekétől, fejlődésüket alapjaiban határozza meg a digitális hálózatalapú szolgáltatások fejlődése, a legújabb technikai eszközök használata. [4] Természetesen ezek a generációs különbségek rányomják bélyegüket az alkalmazott módszerekre (pl. tanulás, kommunikáció, munka), a döntéshozatali mechanizmusokra, a mindennapos viselkedéskultúrára egyaránt. A mobilkommunikációs „okos" eszközök használata, a helyfüggetlen szolgáltatások igénybevétele ezzel a generációval már végérvényesen bekerült a közszolgálati feladatrendszer ellátásának eszköztárába is, és követel egyre növekvő teret magának, ami alkalmazkodásra kényszeríti az idősebb generációk tagjait is.

Fontos kérdés, hogy mi lesz a kapocs a következő generáció tagjai között, akiket a kutatók általában az 'alfa (α)' jelzővel illetnek, és tagjainak a 2010 után születetteket tekintik. Egyes társadalomtudósok véleménye szerint az új generáció a Z generáció örökségét viszi tovább, így célszerűbb lenne a „Z 2.0" kifejezés használata. [4] Mérnöki személettel, a fejlődési tendenciák ismeretében ugyanakkor lehet olyan jegyeket találni, amelyek alapján meg lehet majd különböztetni a két generációt egymástól. A fő jellemző a közvetlen ember-ember interakciók arányának drasztikus csökkenése, eszközhasználat tekintetében pedig a robotika vívmányainak beépülése az élet minden területére. Ennek két fontos – jelenleg is előrehaladott stádiumban lévő – eleme az „önvezető járművek" megjelenése, illetve a drónok alkalmazásának nagyarányú elterjedése. Ez utóbbiaknak a köztudatban, és a kereskedelmi, valamint rekreációs célú alkalmazásokban való megjelenése közel egybeesik az α generáció első tagjainak megszületésével. A tendenciákat figyelembe véve, a bürokratikus korlátok fokozatos lebontásával, valamint a repülésbiztonság technikai dimenziójának erősítésével, a magas autonómia szinttel rendelkező pilóta nélküli légijármű rendszerek (UAS[1]) az α generáció felnövésével párhuzamosan fognak a mindennapi élet részévé válni. Ezért is kiemelten fontos az állami felkészülés minél korábbi megkezdése egyrészt a kereskedelmi alkalmazások bevezetéséhez szükséges infrastrukturális feltételeinek megteremése, másrészt az ilyen eszközök állami feladatrendszerbe történő minél nagyobb arányú bevonása területén.

[1] Unmanned Aerial System

Ehhez természetesen állami részről a hatóságok és a felhasználásban érdekelt szervezetek, a piaci szereplők, fejlesztő és gyártó vállalatok minél szélesebb körű együttműködésére (nem csak formális), valamint az Y és Z generációhoz tartozó szakemberek, akadémiai és felsőoktatási kutatóműhelyek minél nagyobb arányú bevonására lenne szükség. [5]

KÖZSZOLGÁLATI FELADATRENDSZER

Az államszervezet hatékony működésének illetve működtetésének egyik alapfeltétele, hogy a kapcsolódó feladatrendszer egyes elemeihez rendelt hatás- és felelőségi körök egyértelműen kerüljenek lehatárolásra, és ellentmondásmentesen leszabályozásra. Ennek eszköze a mindenkori hatályos, a kor kihívásihoz adaptívan igazodó jogrend, amelyet alkotó, hierarchikusan egymásra épülő és egymással harmonizált jogszabályok tematizált rendszere biztosítja az államhatalom gyakorlásának feltétel-, eszköz-, illetve intézményrendszerét, valamint meghatározza az intézmény- és feladatrendszer kapcsolatát. Magyarország Alaptörvénye [6], mint a legmagasabb szintű nemzeti jogforrás, nevesíti a klasszikus államhatalmi ágakhoz sorolható, illetve be nem sorolható alkotmányos szerveztek körét, amelyeknek a hatalommegosztás elve alapján, rendeltetésükből és feladatrendszerükből fakadóan együttműködési kötelezettségük van. A 45. cikk a *Magyar Honvédséget* (MH) emeli ki, mint az ország függetlenségének területi épségének és határainak védelmezőjét, de tevékenységi körébe sorolja a békefenntartó, valamint humanitárius feladatok ellátását, illetve a katasztrófák megelőzésében, következményeinek elhárításában és felszámolásában való részvételt. A 46. cikk rendelkezik *a rendőrség* és a *nemzetbiztonsági szolgálatok* fő feladatairól, azzal a kiegészítéssel, hogy a részletes szabályozást – a Magyar Honvédséghez hasonlóan – sarkalatos törvény határozza meg. Az állam, komplex feladatrendszerének ellátása érdekében természetesen számos más szervezetet, intézményt működtet, illetve tart fent. Az államigazgatási szervek felsorolását a 2010. évi XLIII. törvény [7] 1. § (2-6) bekezdései tartalmazzák az alábbi tagozódás szerint. A központi államigazgatási szerven belül, a Kormány, kormánybizottság, minisztériumok és Miniszterelnöki Kormányiroda mellett szerepelnek az autonóm államigazgatási szervek[2], kormányhivatalok[3], *rendvédelmi szervek és a Katonai Nemzetbiztonsági Szolgálat* (KNBSZ), illetve az önálló szabályozó szervek[4]. A rendvédelmi szervek között kerülnek nevesítésre a rendőrség, a büntetés-végrehajtási szervezet, a hivatásos katasztrófavédelmi szerv, illetve a polgári nemzetbiztonsági szolgálatok. A rendőrségről szóló 1994. évi XXXIV. törvény [8] 4/A. § (1) bekezdése tartalmazza az általános rendőri feladatok ellátására létrehozott szerv tagozódását (központi szerv[5], megyei/fővárosi[6] rendőr-főkapitányságok, rendőrkapitányságok, határrendészeti kirendeltségek), valamint megadja a lehetőségét más rendőri szervezet törvénnyel, vagy kormányrendelettel történő létrehozására, míg (2) bekezdése belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szervet és terrorizmust elhárító szervet említ. A jelenlegi struktúrában ez a három szerv a Rendőrség, a Nemzeti Védelmi Szolgálat (NVSZ) és a Terrorelhárítási Központ (TEK). [9][10] A rendészeti szervek sorába tartozik továbbá a szintén a Belügyminisztériumot (BM) vezető miniszter irányítása alatt működő Nemzetbiztonsági Szakszolgálat (NBSZ), az Alkotmányvédelmi

[2] Közbeszerzési Hatóság, Egyenlő Bánásmód Hatóság, a Gazdasági Versenyhivatal, Nemzeti Adatvédelmi és Információszabadság Hatóság, a Nemzeti Választási Iroda

[3] Központi Statisztikai Hivatal, Országos Atomenergia Hivatal, a Szellemi Tulajdon Nemzeti Hivatala, Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal

[4] Nemzeti Média- és Hírközlési Hatóság, Magyar Energetikai és Közmű-szabályozási Hivatal

[5] Országos Rendőr-főkapitányság

[6] Budapesti Rendőr-főkapitányság

Hivatal (AH), az Országos Katasztrófavédelmi Főigazgatóság (BM OKF) és az irányítása alá tartozó szervek, a Büntetés-végrehajtás Országos Parancsnoksága (BvOP) és az irányítása alá tartozó szervek, a Terrorelhárítási Információs és Bűnügyi Elemző Központ (TIBEK), a Bevándorlási és Menekültügyi Hivatal (BM BMH), a Pénzügyminisztériumot vezető miniszter irányítása alatt működő Nemzeti Adó- és Vámhivatal (NAV), továbbá a Külgazdasági és Külügyminisztériumot vezető miniszter irányítása alatt tevékenykedő Információs Hivatal (IH). [11][12][13][14][15][16]

Az állami feladatok egyik legnagyobb szegmense tehát a rendészethez köthető, amelynek égisze alatt túlnyomó többségben a belügyminiszter irányítása alatt álló szervezetek tevékenykednek alaprendeltetésüknek megfelelően. Ugyanakkor vannak olyan szakfeladatok, amelyeket más minisztériumi felügyelet álló intézmények látnak el, illetve egyes rendészeti feladatok (pl. határvédelem) ellátásába a honvédelemért felelős szervezet, a Magyar Honvédség állománya is bevonható. A fentiek figyelembevételével, a rendészeti feladatrendszerben érintett országos hatáskörű szervezeti elemeket az 1. ábra szemlélteti.

1. ábra A rendészeti feladatrendszerben érintett országos hatáskörű szervek (saját szerkesztés)

A pilóta nélküli légijármű rendszerek jelenlegi és jövőbeni legnagyobb arányú állami célú felhasználása alapvetően a rendészeti és honvédelmi szakterületekhez köthető, míg a rendészetin belül a rendőrségi felhasználás dominálhat. Az ehhez kapcsolódó besorolás

[17][18] szerint beszélhetünk belső bűnmegelőzési és bűnfelderítési, bűnügyi, határrendészeti, igazgatásrendészeti, közlekedésrendészeti, közrendvédelmi, személy- és objektumvédelmi, valamint terrorelhárítási szolgálati ágakról, illetve állami futár-, bevetési, bűnügyi technikai és szakértői, légirendészeti, rendőri csapaterő, repülőtéri rendőri, tűzszerész, ügyeleti, védelmi igazgatási, továbbá vízirendészeti szolgálatokról. Az általános rendőrségi feladatokat területi tagozódás szempontjából 19 megyei és a budapesti rendőr-főkapitányság, valamint 154 rendőrkapitányság és 21 határőrizeti kirendeltség látja el, míg egyes szakfeladatok és tevékenységek különálló szervezeti elemek (pl. Készenléti Rendőrség) hatáskörébe tartoznak [19].

Ugyanakkor rendészeti tevékenységet az államiakon felül önkormányzati szervek és civil szervezetek is végezhetnek. A csoportosítás szerint rendészeti tevékenységet végző állami fegyveres rendészeti szervnek minősül a fentiek közül a rendőrség, a polgári nemzetbiztonsági szolgálatok, a büntetés-végrehajtási szervezet és a pénzügyőri tevékenységen keresztül a NAV, de bizonyos értékek mentén ide sorolható a hivatásos katasztrófavédelmi szerv is, ami azonban tevékenységét fegyver nélkül látja el. Állami, de nem fegyveres rendészeti szervnek minősül a BMH, az Állami Népegészségügyi és Tisztiorvosi Szolgálat[7] (ÁNTSZ), a Nemzeti Közlekedési Hatóság[8] (NKH), a Nemzeti Élelmiszerlánc-biztonsági Hivatal[9] (NÉBIH) és a Nemzeti Fogyasztóvédelmi Hatóság (NFH). [20][21][22][23][24][25] Önkormányzati rendészeti szervnek minősül a természetvédelmi őr, a hegyőr, a halászati őr, a közterület-felügyelő és a mezőőr, illetve civil rendészeti szervnek a polgárőrség. [26][27][28][29][30][31] A központi költségvetési szervként működő Országgyűlési Őrség feladatát fegyveresen látja el, és egyenruhás állományára vonatkozik a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló törvény, így tevékenysége illeszkedik a rendészeti feladatrendszerhez.[10] [32][33]

Az állami feladatokat ellátó szervezetek és intézmények közül tevékenységük okán érdemes még kiemelni a BM háttérintézményeként működő Országos Vízügyi Főigazgatóságot és az irányítása alá tartozó szerveket, az önálló szabályozó szervként működő Nemzeti Média és Hírközlési Hatóságot és a Magyar Energetikai és Közmű-szabályozási Hivatalt, valamint központi költségvetési szervként, az EMMI irányítása alatt működő Országos Mentőszolgálatot, továbbá az agrárminiszter irányítása alatt működő Országos Meteorológiai Szolgálatot. [36][37][38][39][40][41]

A kormányhivatalok, mint a területi közigazgatás általános hatáskörrel rendelkező szervei több mint ezer államigazgatási hatósági feladat- és hatáskörben járnak el többek között az agrár- és vidékfejlesztési, bányafelügyeleti, fogyasztóvédelmi, élelmiszerlánc-biztonsági, földhivatali, növény- és talajvédelmi, erdészeti, környezet- és természetvédelmi, vagy éppen építésügyi területeken. [42][43][44] Az állami feladatrendszer hatékony végrehajtását a fentieken túl kiterjedt intézményrendszer támogatja.

A vázolt szervezeti struktúrát, a kapcsolódó állami feladatokat és hatásköröket áttekintve, a hatályos jogszabályok elemzésének eredménye alapján megállapítható, hogy ezek egy olyan komplex rendszert alkotnak, amelyben a működés hatékonyságát az együttműködés minősége

[7] Irányító szerve az Emberi Erőforrások Minisztériuma (EMMI) Egészségügyért Felelős Államtitkársága

[8] 2016. december 31-én jogutódlással megszűnt, tevékenységét a Nemzeti Fejlesztési Minisztérium, majd az Innovációs és Technológiai Minisztérium vette át, míg egyes hatósági feladatai a Budapest Főváros Kormányhivatalához kerültek delegálásra

[9] Az Agrárminisztérium háttérintézményeként működik

[10] A Nemzeti Honvéd Díszegység szervezetéhez tartozó Honvéd Koronaőrség és Honvéd Palotaőrség nem tartozik a rendészeti feladatokat ellátó szervezetek sorába, tevékenységét a Magyar Honvédség kötelékében a honvédelemért felelős miniszter irányítása alatt végzi. [34][35]

alapjaiban határozza meg. Az említett szervezetek tevékenységeinek sorában számtalan olyan szakfeladattal találkozhatunk, amelyek végrehajtásának hatékonyságát nagymértékben meg lehet növelni pilóta nélküli légijármű rendszerek alkalmazásával. A kör tovább bővíthető, ha az többségi állami tulajdonú közműszolgáltató, energetikai, vagy egyéb vállaltok tevékenységi körét is vizsgálat alá vonjuk.

DRÓNOK KATONAI ALKALMAZÁSA

A fenti komplex feladatrendszerrel összefüggésben magyarországi viszonyok között felhasználható pilóta nélküli légijármű rendszerek tekintetében érdemes megvizsgálni a szóba jöhető megoldások körét. Elsőnek a katonai alkalmazásokból érdemes kiindulni, hiszen ezen a területen rendelkezünk a legnagyobb tapasztalattal.

A hagyományos, pilóta által vezetett repülőeszközök alkalmazását két fő tényező korlátozza. A technikai dimenzióban a rendelkezésre álló műszaki megoldások által meghatásozott határértékek, míg a humán faktor esetén az emberi szervezet fizikai tűrőképessége, valamint a fiziológiai szükségletek befolyásolják egymással szoros összefüggésben a felhasználás lehetséges módozatait és körülményeit. Tekintettel arra, hogy szinte a repülés kezdetétől fogva ez utóbbi bizonyult a szűkebb, és a technikai lehetőségekhez képest azóta is egyre szűkülő keresztmetszetnek, a személyzet „eltávolítása” a repülő fedélzetéről logikus törekvés volt. Ennek elsődleges jelentősége az emberi élet, illetve egészség megóvásában keresendő. Az ilyen eszközök alkalmazása ugyanakkor minden monoton (pl. hosszú távú felderítő repülések), „piszkos” (pl. radioaktív, vegyi, vagy biológiai anyagok által szennyezett területek feletti repülések), vagy veszélyes (pl. fokozott légvédelmi tevékenység által védett területek feletti repülések) feladat végrehajtása esetén indokolt, és ma már technikailag lehetséges is. [45]
Történetileg az első UAV alkalmazások a fegyverként való használathoz köthetőek, melyeket a légvédelmi csapatok gyakoroltatása során igénybe vett légi célok követtek, míg a későbbi korokban már a légi felderítés játszotta a főszerepet. Napjainkban is ez utóbbi dominálja (a polgári célú közszolgálati felhasználásoz hasonlóan) a katonai dimenziót, miközben minden alkalmazási terület folyamatos fejlesztés alatt áll.

A rendelkezésre álló fejlesztési kapacitások, és az általuk előállított eszközrendszer nagysága és képességei szoros összefüggésben állnak az országok gazdasági erejével és hagyományos katonai potenciáljuk volumenével, így az Amerikai Egyesült Államok (USA) rendelkezik világviszonylatban a legnagyobb előnnyel, és uralja piac minden szegmensét. Ugyanakkor a kormányzati törekvések a legtöbb állam esetében a pilóta nélküli légijárművek arányának növelése irányába mutatnak. Miközben az USA a 2017-es költségvetési évre 4,5 Mrd dollárt különített el drónbeszerzésekre, ezzel lehetővé téve új kutatási és fejlesztési programok beindítását, India 22 tengeri járőrdrónra kötött szerződést az amerikai General Atomics-sal 2 Mrd dollár értékben. [46] Az amerikai piac 2016-os vizsgálatából jól látszik az a tendencia, miszerint a forgószárnyas eszközözök, multicopterek alkalmazására egyre nagyobb igény mutatkozik a merevszárnyas konstrukciókhoz képest, miközben a hibrid megoldások aránya is gyorsan növekszik. A forgószárnyas eszközök piaci részesedése abban az esztendőben meghaladta a 65%-ot, míg a hibrid UAS-ok becsült átlagos piaci növekedési üteme 2024-ig 15%-felett várható. Autonómia szempontjából jelenleg a „fél-autonóm” eszközök vezetik a statisztikákat, ugyanakkor a tendenciák egyértelműen az autonómiaszint folyamatos növelésére irányuló törekvések erősödését jelzik. [47] Érdemes megjelezni, hogy a fent hivatkozott kutatások a kormányzati alkalmazásokat (forgalomfelügyelet, rendőrségi, tűzoltó, vagy katasztrófavédelmi alkalmazások) is a katonai drónpiachoz sorolják, ami több más tényező mellett magyarázhatja a multikopteres beszerzések magasabb arányát.

A katonai alkalmazások tekintetében egyre több területen és egyre nagyobb arányban váltják ki az UAV rendszerek a hagyományos légijárműveket. A hírszerzés, megfigyelés, precíziós

célmegjelölés és felderítés, a jelfelderítés, valamint az ABV[11] felderítés területén már napjainkban is prioritást élveznek a pilóta nélküli megoldások. Ugyanakkor a harcvezetés, híradás és adatkommunikáció, a hadszíntér gazdálkodás, a harctéri kutatás, mentés, a távérzékelés, digitális térképészet, az elektronikai és információs hadviselés, az aknakutatás, a harctéri érzékelők rejtett telepítése, a megtévesztés, elterelés, és a támadó műveletek esetén is egyre nagyobb arányban lehet számítani alkalmazásukra. Az ISTAR[12] feladatok közé sorolhatjuk a különböző spektrumtartományban működő szenzorrendszerekkel végzett képi felderítést (IMINT[13]). A látható fény tartományban és az infravörös tartományban optikai felderítést végeznek, míg a rádiófrekvenciás tartományban képi mikrohullámú radarszenzorokat alkalmaznak (SAR[14]), a harmadik területnek pedig a mozgó célpont felderítést tekinthetjük (MTI[15]). A másik nagy csoportba a kisugárzás- és jelfelderítés (SIGINT[16]) területeit sorolhatjuk, mint a kommunikációs rendszerek felderítése (COMINT[17]), vagy a rádióelektronikai felderítés (ELINT[18]). [48] A fenti képességekkel rendelkező legismertebb eszköz a Global Hawk RQ-4 (2. ábra), melyet az Northrop Grumman vállalat gyárt elsősorban az amerikai haderő számára. A csaknem 15 tonnás felszálló tömeggel rendelkező szerkezet korszerű szenzorrendszerével multispektrális felderítést képes végezni akár 18 km-es magasságból. Hatótávolsága meghaladhatja a 22 000 km-ert, és akár 32 órát is képes egyhuzamban a levegőben tölteni. [49] Hasonló, stratégiai szintű eszközökkel jelenleg kizárólag olyan „nagyhatalmi" státuszú államok rendelkeznek, mint például Oroszország, vagy Kína, míg kisebb rendszereket ma már a fejlett haderők csaknem mindegyike használ. A fegyverek hordozására is alkalmas eszközök (harci drónok) alkalmazására ugyanakkor lényegesen kevesebb haderő rendelkezik képességgel.

A műveleti területeken történő alkalmazások során eltérő környezeti feltételek mellett kell az UAS-oknak különböző feladatokat végrehajtva küldetésüket teljesíteni a harcászati, hadműveleti, vagy éppen a hadászati célok elérése érdekében. A szárazföldi támogató műveletek közé tartozik a csapásmérés (közvetlen légi támogatás, légi lefogás), a konvojkísérés, a menetútvonal ellenőrzés, a célmegjelölés és a légicsapások hatékonyságának értékelése. Az egyéb műveletek sorában *harci kiszolgáló támogatásként* az infokommunikációs támogatást (légi kommunikációs csomópont), vagy az ABV felderítést érdemes kiemelni, míg a *haditengerészeti műveletek támogatása* területén történő alkalmazások esetén beszélhetünk többek között a part menti vizek felderítéséről, a csapások hatásainak felméréséről, kiértékeléséről, kikötők megfigyeléséről, vagy kommunikációs csatornák átjátszásáról. A *légi logisztikai műveletek* elsősorban a más módon csak nehezen megközelíthető, vagy teljesen megközelíthetetlen helyekre történő utánpótlás-szállítási feladatok ellátására, valamint a légi ledobási helyek előzetes felmérésére összpontosulnak. Külön kategóriaként érdemes kezelni az egyéb műveletek sorában a *térképészeti és meteorológiai támogatási* tevékenységeket. [48][50]

[11] Atom, biológiai, vegyi
[12] Intelligence Surveillance Target Acquisition Reconnaissance
[13] Imagery Intelligence
[14] Synthetic Aperture Radar
[15] Moving Tartget Indication
[16] Signals Intelligence
[17] Communications Intelligence
[18] Electronic Intelligence

2. ábra Global Hawk RQ-4 [51]

A Magyar Honvédség vonatkozásában, napjainkban három területen kerülnek alkalmazásra pilóta nélküli légijárművek. A HM Geoinformációs Szolgálat térképészeti (légi fényképezés) célú repüléseket hajt végre eszközeivel, a debreceni MH 5. Bocskai István Lövészdandár rendelkezik légi-felderítő képességgel, míg a MH 12. Arrabona Légvédelmi Rakétaezred a HM EI Zrt. által fejlesztett és biztosított Meteor típusú gázturbinás meghajtású célrepülőgépek segítségével hajtja végre gyakorló éleslövészeteit. Érdemes megjegyezni, hogy jelenleg mindhárom feladatrendszer esetén harcászati szintű műveletek végrehajtására alkalmas, korlátozott manőverező-képességű merevszárnyas eszközpark áll csak rendelkezésre, amelyek kizárólag adott célfeladatok ellátására használhatóak. Ugyanakkor a nemzetközi katonai tapasztalatok alapján a jövőben számos olyan feladattal is számolni lehet, amelyek végrehajtása során a multirotoros villamos meghajtású eszközök használata célravezetőbb lehet.

A honvédelem feladatrendszerében meghatározottak szerint az ilyen eszközöket hatékonyan lehet alkalmazni, akár missziós területeken zajló katonai műveletek közvetett vagy közvetlen támogatására (felderítés, konvojkísérés, útvonal ellenőrzés, kockázatot jelentő csoportok, vagy objektumok megfigyelése, táborvédelem, művelettervezés, kutatás mentés, rádióelektronikai felderítés, tömegtájékoztatás stb.), akár kiképzési célokra (gyakorlatok tervezésére, a végrehajtás ellenőrzésére, kiértékelésére), vagy az országvédelmi feladatokra való felkészülés és a védekezés időszakában (felderítés, elterelés, megtévesztés, megfigyelés, zavarás, lefogás, támadás stb.). Ugyanakkor az egyéb feladatok között meghatározott határvédelem, vagy a katasztrófák elleni védekezés során is hatékony segítséget jelentene az ilyen eszközök minél nagyobb arányú bevonása. Természetesen a fenti feladatrendszer támogatásához szükséges eszközök beszerzése mellett, azok szervezeti struktúrába történő integrációjára, a szakállomány folyamatos kiképzésére és gyakoroltatására, illetve a logisztikai támogatás rendszerének kialakítására és akadálytalan működtetésére lenne szükség.

DRÓNOK KÖZSZOLGÁLATI ALKALMAZÁSA

A pilóta nélküli légijármű rendszerek csoportosítására számos megoldás létezik, többnyire általában az UAV valamilyen fizikai tulajdonsága, vagy repülési paramétere alapján történik, mint például a maximális felszálló tömeg, a hatósugár, a repülési magasság, vagy az időtartam.

A kézirat benyújtásának dátuma (Date of the submission): (SZERKESZTŐSÉG TÖLTI KI)
A kézirat elfogadásának dátuma (Date of the acceptance): (SZERKESZTŐSÉG TÖLTI KI)

Egy általánosan elfogadott besorolást az UVSI[19] készített nemzetközi összefogással, alapvetően a katonai osztályozás alapján, de a polgári eszközök tulajdonságainak figyelembevételével. A harcászati szint eszerint 10 alkategóriát tartalmaz (nano, micro, mini, CR[20], SR[21], MR[22], MRE[23], LADP[24], LALE[25], MALE[26]), melyek közül a legnagyobb eszköz súlyhatára 1500 kg, a legnagyobb hatótávolságúé 500 km-t meghaladó hatósugár, a legnagyobb repülési magasság 14.000 m, míg a maximális repülési idő 48 óra. A stratégiai szinthez sorolódik a HALE[27] és UCAV[28] kategória, míg a speciális rendeltetésű eszközök csoportját a harci (LETH[29]) és zavaró (DEC[30]) UAV-k alkotják. [52] A magyarországi viszonyok és a várható alkalmazási területek figyelembevételével a harcászati szint alsó öt kategóriájába tartozó eszközök felhasználása lehet indokolt a legnagyobb mennyiségben a közszolgálati igénybevételek során, míg egyes esetekben szükség lehet valamely paraméterek tekintetében (repülési idő és/vagy magasság) megnövelt képességű drónok alkalmazására.

Csoportosítási szempont lehet a felépítés (merevszárnyas, forgószárnyas, hibrid), a meghajtás típusa (dugattyús, gázturbinás, elektromos), az irányítás (távirányítású, programvezérelt, kombinált), vagy az indítás- és visszatérés módja, vagy éppen a rendeltetés.
Az elmúlt években jellemző tendenciák alapján megállapítható, hogy a repülésvezérlő rendszerek fejlődésének köszönhetően stabil repülési és kedvező vezetési tulajdonságokkal rendelkező multirotoros konstrukciók részesedése a polgári és katonai eszközök piacán egyaránt megnőtt. A GNSS[31] vevők [53] és a repülést támogató szenzorrendszer precíz vezérlést, pontos feladat-végrehajtást tesz lehetővé. A különböző autonóm ütközés- és akadálykerülő, vészleszállító megoldások pedig jelentősen csökkentik az emberi tényező „káros hatásait", a balesetek bekövetkezésének valószínűségét, azaz megnövelik az alkalmazás biztonságát. A korszerű digitális térképészeti megoldásokat felhasználó geoinformatikai (GIS[32]) alapú repüléstervező- és vezérlőrendszerek, a szélessávú, védett, többcsatornás rádiófrekvenciás kapcsolat, és az akár repülés közben is állítható repülési paraméterek, illetve a biztosított szolgáltatások a felhasználási lehetőségek egyre szélesebb spektrumát kínálják. A mai akkumulátorok a sárkányszerkezet és a meghajtás paramétereitől, a repülés dinamikájától, a meteorológiai viszonyoktól, valamint a hasznos teher méretétől, típusától és az alkalmazás módjától függően akár 30 percet is meghaladó repülési időt tesznek lehetővé. Néhány ezer dollárért vásárolhatunk különböző felépítésű 6-8, vagy akár 12 rotoros UAV-t is, amik akár 30 kg-os payloadokat is képesek hordozni [54], és egy-egy rotor meghibásodása esetén is biztonságosan tudnak landolni (3. ábra). Ebben az árkategóriában az adott feladathoz optimalizált konstrukciók kialakítására is lehetőség nyílik, amelyek fedélzetén akár ultrazoom kamerák, multispektrális felderítő eszközök, rádiófrekvenciás átjátszók, zavarók, szállítókonténerek, vagy további akkumulátorcsoportok is elhelyezhetők.

[19] Unmanned Vehicle Systems International
[20] Close-Range – Kis hatótávolságú
[21] Short-Range – Rövid hatótávolságú
[22] Medium-Range – Közepes hatótávolságú
[23] Medium-Range Endurance – Közepes hatótávolságú megnövelt repülési időtartamú
[24] Low Altitude Deep Penetration – Kis repülési magasságú áthatoló
[25] Low Altitude Long Endurance – Kis repülési magasságú hosszú repülési időtartamú
[26] Medium Altitude Long Endurance – Közepes repülési magasságú hosszú repülési időtartamú
[27] High Altitude Long Endurance – Nagy repülési magasságú, hosszú repülési időtartamú
[28] Unmanned (or uninhabited) Combat Air Vehicle – Pilóta nélküli harci légijármű
[29] Lethal – halálos
[30] Decoy – csali
[31] Global Navigation Satellite Systems – Globális Navigációs Műholdrendszer
[32] Geographic Information System – Földrajzi Információs Rendszer, Geoinformációs Rendszer

A multikopterek alkalmazását indokolja továbbá az is, hogy a fel- és leszállás helyből történik, és nem igényel speciális infrastruktúrát, hosszadalmas előkészítést és az eszközök karbantartási igénye is minimális. A repülési magasság eléréséhez, majd a landoláshoz akár fél perc is elegendő lehet, ami az alacsony zajszinttel párosulva biztosítja a rejtett alkalmazás lehetőségét.

A fedélzetre helyezhető akkumulátorok korlátozott kapacitására megoldást jelent a földről való energiaellátás biztosítása, amely korlátozza ugyan az eszköz mozgásszabadságát, azonban ilyen módon 80-100 m magasságból akár órákon [55], vagy napokon keresztül folyamatos megfigyelés, vagy felügyelet valósítható meg egyetlen felszállással. Ezek az eszközök alternatívái lehetnek a sokszor költséges ballonos megoldásoknak [56] többek között olyan rendészeti alkalmazások esetén is, mint egy határszakasz, tömegrendezvények, fesztiválok, illetve védett objektumok megfigyelése, vagy a távközlési átjátszóként való üzemelés.

3. ábra OnyxStar HYDRA-12 [57]

Ezzel áttérve a közfeladatok ellátásában való alkalmazás lehetőségeire, az alábbi gondolatmenetet célszerű követni. A hatályos magyar jogrendben meghatározott állami feladatrendszernek, illetve az annak ellátásáért felelős szervezeti struktúrának minden időszakban hatékony választ kell adnia a kor kihívásaira, a felmerülő biztonsági kockázatokra. Az ennek érdekében igénybevett eszközrendszernek minden körülmények között a legkorszerűbb technológiák, technikák és eljárások által biztosított szolgáltatásokon kell alapulnia. A drónok közszolgálati alkalmazása a fenti követelmények alapján kézenfekvő, és illeszkedik a nemzetközi trendekhez. Ugyanakkor tekintettel ennek a piacnak a várható volumenére, a jövőbeni alkalmazások nagyságrendjére, ennek a területnek a kezelését stratégiai szintre kell emelni annak érdekében, hogy az állami szereplők számára mindenkor saját igényei alapján fejlesztett eszközpark álljon rendelkezésre. Az UAS kategóriák tulajdonságait elemezve megállapítható, hogy néhány speciális alkalmazást leszámítva – mint például a nagy távolságú felderítés, katonai térképészeti felhasználás, illetve a légvédelem számára biztosított csali célok, az autópálya felügyelet, vagy tűzoltás – a multikopterek területére érdemes koncentrálni azok pozitív tulajdonságai miatt. Ezek a gyors irány és helyváltoztatásra, akár stabil lebegésre, vagy megjelölt mozgó célobjektumok követésére képes eszközök már ma is eredményesen

használhatóak városi, vagy más bonyolult környezetben. Zéró emisszió és más környezetkárosító hatás, illetve minimális zajkibocsátás mellett képesek üzemelni, ami biztosítja a drónokkal való műveletek rejtettségét. Ezek a tulajdonságok minden alkalmazási területen nagy jelentőséggel bírnak, de talán a legfontosabb szerep a rendőrségi, titkosszolgálati, vagy környezetvédelmi célú igénybevételek során jut nekik.

A rendőrségi szervek feladatrendszerében számos szakfeladat végrehajtása során lehet használatuk célravezető. [58] A bűnmegelőzés során veszélyeztetett területek feletti járőrözés végrehajtásával csökkenthető az elkövetések kockázata, míg bekövetkezett cselekmény esetén a felderítés során lehet hasznos segítség. Ugyanakkor akár balesetek, vagy bűncselekmények helyszínelése, vagy más nyomozati cselekmények, bizonyítási eljárások, vagy titkos adatgyűjtés során is számos érv szól az ilyen rendszerek alkalmazása mellett. További felhasználási területet jelenthetnek a különböző rendőrségi műveletek, helyszín-, vagy rendezvénybiztosítási feladatok, csapaterők bevetése, rajtaütések előkészítése, vagy a korábban említett határőrizeti-, felügyeleti feladatok, az illegális bevándorlás és embercsempészet elleni küzdelem komplex feladatrendszere. Ezekkel összefüggésben a felhasználók köre a terrorizmus elleni harc során kiemelt szerepkörrel rendelkező Terrorelhárítási Központ állományával is kibővül. Az eszközrendszer a jövőben fejleszthető lenne beltéri repülésre alkalmas ultra kisméretű UAV-kal, amelyekkel például a túszszabadítási tevékenységeket megelőző időszakban zárt térben végezhető felderítés, vagy a művelet során figyelemelterelés, de segítségükkel bejuttathatók kommunikációs eszközök, vagy a túszok életének megóvását segítő egyéb berendezések is. Ehhez a tevékenységi körhöz közel áll a Nemzeti Adó és Vámhivatal egyes egységeinek feladatrendszere, így hasonló alkalmazási lehetőségek esetükben is elképzelhetőek. A büntetés-végrehajtás rendszerében a végrehajtási intézmények szökés elleni, valamint illegális eszközök bejuttatása elleni védelmének növelése, illetve az ilyen létesítményeken kívüli munkavégzések helyszínének felügyelete lehet kiemelt feladat, amelyek ellátása során drónok igénybevétele hatékonyságot növelő tényezővé válhat a jövőben.

A katasztrófavédelemi és mentési, illetve ahhoz köthető területeken, a tűzoltási, iparbiztonsági, polgári védelmi és vízügyi tevékenységekkel összefüggő feladatok során nyílik lehetőség a különböző UAS megoldások felhasználására a műveletek teljes spektrumában. [59][60][61] A nukleáris, vagy ipari balesetekkel, veszélyes árukat szállító járműszerelvények baleseteivel, épület és erdőtüzekkel, földrengésekkel, árvizekkel vagy éppen tömeges közlekedési balesetekkel kapcsolatos tevékenységek során a felderítési, helyszínbiztosítási és kutatás-mentési feladatok mellet számos egyéb speciális alkalmazási lehetőség is felmerülhet. Ilyen lehet például a tűzfészkek felkutatása, terjedési paraméterek vizsgálata, töltések állapotának felmérése, kockázati tényezők kiszűrése, tűzoltó konténerek alkalmazása, semlegesítő agyagok kiszórása, a kritikus infrastruktúra elemeit képező létesítmények, hálózatok állapotának felmérése.

A hatósági feladatok támogatása közül a környezetvédelem, vad- és erdőgazdálkodás, vagy a települési önkormányzatok munkájához köthető alkalmazásokat érdemes kiemelni. Ez előbbi esetén kiemelhetnénk a más módon nehezen megközelíthető vizes mocsaras élőhelyek, árterek költséghatékony felmérését, a veszélyeztetett, vagy különböző szintű védelem alatt álló területek határainak védelmét például a művelt birtokok közelében, időszakosan végrehajtott, programozott repülések során készített felvételek fotometriai összehasonlító elemzésével. [60] A drónok alkalmazása illegális, engedély nélküli tevékenységek egész sora ellen jelenthet hatékony „távfelügyeleti” megoldást, mint például hulladéklerakás, szennyvízkezelés, tűzgyújtás, fakitermelés, vadászat, halászat, vagy egyéb természetkárosító tevékenységek. De felhasználható állatcsoportok mozgásának megfigyelésére, populáció számlálásra, vagy természetes élőhelyek megfigyelésére az élővilág jelentősebb megzavarása nélkül. Települési környezetben az építési hatóság előírásainak, vagy az önkormányzati rendeletek betartásának ellenőrzése, illegális építkezések felderítése lehet az egyik kiemelt alkalmazási terület, de

energiahatékonysági felmérések készítésére, vagy fűtési szezonban akár a fosszilis, vagy más tüzelőanyagokkal üzemelő fűtési rendszerek állapotának ellenőrzésére (károsanyag-kibocsátás) is alkalmas. Ipari területek, veszélyes létesítmények fölött speciális vegyi, biológiai, optikai szenzorrendszerekkel a károsanyag-kibocsátási előírások betartása vizsgálható akár rendszeresen, akár szúrópróba szerűen, úgy hogy a drónok által készített felvételek és elektronikus mérési jegyzőkönyvek bizonyítékként is szolgálhatnak a hatóságok által indított szabálysértési, vagy büntetőeljárások során. De a frekvenciagazdálkodással összefüggésben az engedély nélküli rádiófrekvenciás sugárforrások felkutatásában és azonosításában is hasznos megoldást jelenthet a drónok használata. Speciális payload-okkal veszélyes környezetben, vagy más módon megközelíthetetlen területeken vegyi, biológiai mintavételezési feladatok is végrehajthatóak alacsony kockázat mellet multikopterek alkalmazásával.

Bár a fenti felsorolás korántsem tekinthető teljesnek, az egyértelműen látszik, milyen hihetetlenül széles lehet a jövőben a nem katonai célú közszolgálati UAS alkalmazások köre. Az alkalmazhatóság kérdésében azt is érdemes megjegyezni, hogy napjainkban a hangsúly folyamatosan tolódik el a hordozóplatformról a hasznos terhek [62], illetve az ezek által szolgáltatott valós idejű információk automatizált feldolgozása irányába, így a jövőben erre lényegesen nagyobb hangsúlyt érdemes majd fektetni. Az egyes feladatrendszerekhez tartó kategóriák és a kapcsolódó műszaki követelményrendszer meghatározása és naprakészen tartása lényegesen komplexebb feladat, mint elsőre tűnhet. Magyarországi viszonylatban a 150 kg alatti kategóriába csaknem minden alkalmazási változatnak bele kell férnie, de kompromisszumokkal a felső határ akár 25 kg alá is csökkenthető, köszönhetően az eszközök folyamatos fejődésének. Amit azonban mindenképpen figyelembe kell venni, hogy az állami feladatrendszer hatékony ellátása a szervezetek közötti szoros együttműködésen alapszik, ami érinti az UAV rendszerek használatát is, így már a kategóriák meghatározása során is elengedhetetlen a kooperáció.

TENDENCIÁK ÉS PERSPEKTÍVÁK

Az üzleti előrejelzések a katonai és polgári UAS-ok piacán egyaránt jelentős bővüléssel számolnak az elkövetkezendő évtizedekben, ami a pilóta nélküli légijárművek használatának tömeges elterjedése utal. A növekedés motorját, a katonai alkalmazások dominanciája mellett az egyéb állami, közszolgálati célú, valamint a stratégiai ágazatokhoz kapcsolódó (energetika) ipari felhasználások, továbbá a kereskedelmi célú igénybevétel bővülése fogja jelenteni.

A bővüléshez ugyanakkor elengedhetetlenül szükségesek azok – az elsősorban a polgári célú eszközök piaca által is gerjesztett –, a technikai dimenzióban zajló gyorsuló fejlődési folyamatok, amelyeknek egyik lényeges törekvése a repülésbiztonság szintjének folyamatos emelése, a drónok egységes légtérbe történő integrációja technikai feltételeinek megteremtése. Ennek legnagyobb területe egyfelől az egyes eszközök autonómia szintjének növelése [63] annak érdekében, hogy az emberi tényező által jelentett kockázatot minimálisra csökkentsük, másfelől pedig annak az infrastruktúrának a megteremtése (útvonaltervezés, és forgalomirányítás), amely biztosítja nagyszámú eszköz egyidejű alkalmazása esetén is a balesetmentes közlekedéshez szükséges hátteret. Ennek érdekében a funkciók egyre nagyobb arányban kerülnek átadásra a fedélzeti számítógépnek (robotpilóta), amely döntéseit a komplex szenzorrendszerek, valamint egy központi forgalomirányító rendszer által szolgáltatott információk segítségével hozza meg akár a másodperc törtrésze alatt. Így akár a dinamikusan változó környezethez adaptívan alkalmazkodva képes előre meghatározott feladatát elvégezni, vagy veszélyhelyzet esetén központi utasítások és eljárásrendek alapján biztonságosan kivonni

magát a forgalomból emberi életekben, vagy anyagi javakban történő károkozás kockázatának minimalizálása mellett. [5]

A fenti törekvéseknek is köszönhetően a költséges haditechnikai fejlesztések fokozatosan vesztik el technológiai előnyüket, ezért egyre nagyobb igény mutatkozik a költséghatékonyabb polgári célú technikai megoldások, eszközök és eszközrendszerek adaptálása, integrációja iránt. Ennek köszönhetően konvergencia figyelhető meg a katonai és a polgári technológiák között, azaz a korábban tapasztalható technikai színvonalbeli különbség fokozatosan csökken elsősorban a harcászati szintű UAS-ok esetében. Konvergencia figyelhető meg ugyanakkor – bár jelenleg elsősorban még csak a katonai alkalmazások területén – a pilóta által vezetett eszközök és a pilóta nélküli légijárművek funkciói között. Ezt alátámasztják például azok az amerikai haderőben évek óta zajló tesztek is, melyeket személyzet nélküli „hagyományos" vadászgépekkel végeznek. [64]

Katonai alkalmazásokban az UAV-k szenzor, kommunikációs, fegyveres és szállító payload-okkal lesznek majd felszerelhetőek. Az szenzorplatformok a klasszikus ISTAR felderítő funkciókat lesznek képesek biztosítani, míg kommunikációs modulok olyan átjátszókat fognak tartalmazni, amelyek kapcsolási funkciót is megvalósítanak a különböző típusú rádiók, adatterminálok, vagy hálózatok között. A fegyveres payload-ok lehetnek halálos és nem-halálos képességűek, alkalmasak lesznek személyek likvidálására, megsebesítésére, vagy cselekvőképtelenné tételére, rombolhatnak, károsíthatnak, vagy más módon használhatatlanná tehetnek eszközöket, infrastruktúrát. A szállítókonténerek használhatóak lesznek mindenféle utánpótlás, eszközök, vagy éppen személyek felvételére, szállítására (kézbesítésére) és lerakására, sérültek kimenekítésére. Az UAS-ok használatára való áttérés a hagyományos eszközökről eltérő ütemezéssel ugyan, de folyamatosan zajlik az Amerikai Egyesült Államok haderejében. A felderítésben ez már közel 80%-ban meg is történt, míg a kommunikációs célú eszközök esetében ez az arány nem éri el az 50%-ot. A felfegyverzett légijárművek és szállítójárművek esetén még dominálnak a hagyományos megoldások, míg a MEDEVAC[33] szerepkörben egyáltalán nem használtak pilóta nélküli megoldást. A középtávú előrejelzések szerint 2026-ig mind a felderítés, mind pedig a kommunikációs platformok tekintetében csaknem teljesen kiszorulnak a hagyományos, pilóta által vezetett repülőeszközök, és a felfegyverzett alkalmazásokban is 50%-alá csökken majd arányuk, míg a többi funkció esetében dominanciájuk csak csökkenni fog. A 2035-ig szóló prognózisok szerint a kommunikációs területen teljesen áttérnek az UAV rendszerek használatára, és a felderítési feladatoknak is már csak néhány százalékát végzik majd hagyományos légijárművekkel. A támadó és szállítási funkciók esetében az áttérés megközelíti majd a 80%-ot, miközben a harctéri kimenekítésben a drónok szerepe továbbra is csekély marad. [65] Ez utóbbi megállapítás annak köszönhető, hogy napjaink gondolkodásmódjában emberi életeket ilyen formában „gépekre bízni" még komoly morális kérdéseket vet fel, ami a prognózisokat készítők véleményalkotását is jelentősen befolyásolja (generációs szakadék) annak ellenére, hogy 15-20 év múlva valószínűsíthetően a „légi robotok" fognak ezen a területen is jobban teljesíteni.

A pilóta nélküli légijármű rendszerek ilyen arányú alkalmazása megköveteli a katonai struktúrák folyamatos alkalmazkodását, így a támogató drón alegységek mellett, egységszintű önálló drón alakulatok létrehozására is lehet a jövőben számítani. Az önálló haderőnemmé válás nem valószínű, hiszen várhatóan a klasszikus légierő haderőnem fog átalakulni fokozatosan az alkalmazási arányok változásával párhuzamosan.

A fenti tendenciák, ha kis késleltetéssel is, de jellemzőek lesznek a közszolgálati alkalmazások minden területére. Az egyre nagyobb autonómiával rendelkező „légi robotok"-at

[33] Medical Evacuation – harctéri (egészségügyi) kimenekítés

az operátorok már nem vezetni, hanem parancsokkal irányítani, illetve tevékenységüket csak felügyelni fogják feladat-végrehajtás közben. A városi környezetben ma még közúthálózathoz kötött tevékenységek egy része fokozatosan kerül majd át a levegőbe, melynek úttörője a szállítási (futár, posta) üzletág lesz. Ugyanakkor hosszútávon a közszolgálati feladatkörökhöz kapcsolódóan lehet számítani akár olyan mentődrónok alkalmazására is, amelyek távoli orvosi felügyelet mellett a beépített műszerek segítségével képesek egy gyors diagnózis felállítására, és szükség esetén rövid időn belül a legközelebbi kórházba szállítják a sérült, vagy beteg embereket. Vagy egy égő toronyházból mentőkapszulákat hordozó drónok segítségével menekíthetnék az embereket tűzoltók életének kockáztatása nélkül. A fenti alkalmazásokat lehetővé tevő technikai fejlettségi szint mellett ugyanakkor bármely területen már csak a képzelet szabhat határt a felhasználási módozatoknak. Egy X, Y, Z generációs ember számára ezek a lehetőségek talán még ijesztőnek tűnhetnek, de egy α generációs számára lehet, hogy az ilyen megoldások is a mindennapi élet részévé válnak majd.

ÖSSZEGZÉS

Ha a kutatás tanulságát röviden és általános érvényűen szeretnénk megfogalmazni, az az lehetne, hogy a jövő már elkezdődött és mi magunk (egyén, közösség, állam) dönthetjük el, hogy részesei leszünk-e vagy sem. Ha úgy döntöttünk, hogy igen, a lehető legkorábban fel kell ismernünk azokat a folyamatokat, kihívásokat, amelyek a jövőben nagy hatással lesznek életünkre. Annak érdekében, hogy a megfelelő időben, illetve módon tudjunk rájuk reagálni, ki kell dolgozni az adott körülmények között legjobbnak ítélt stratégiát.

Az államnak alapvető feladata, hogy polgárainak biztonságát, annak minden dimenziójában garantálja a rendelkezésre álló legkorszerűbb, leghatékonyabb eszközökkel. Az elmúlt években a dimenziók közül a kibertér vált az egyik legjelentősebb tényezővé, hiszen annak biztonsága az összes többi dimenzió minőségére is hatással van. A technikai fejlődés jelenlegi üteme alapján a pilóta nélküli légijármű rendszerek szegmense (és a robottechnika általában) is jó úton halad abba az irányba, hogy önálló dimenzióvá váljon a kiber- és a fizikai tér határán.

Annak érdekében, hogy az állami feladatrendszer egyes szereplői tartani tudják a lépést ezekkel a folyamatokkal, teljes koncepcióváltásra van szükség, ami a korábbinál lényegesen nagyobb rugalmasságot és magasabb szintű kooperációt vár el az érintettektől. A korábban megfogalmazott „Pilóta Nélküli Légijármű Rendszerek Információs, Támogatási, Tudás- és Oktatási Központ” [5] olyan stratégiai tervezési, döntés-előkészítési, és fejlesztési szervezetként funkcionálna, amely komplex problémaként kezeli a kapcsolódó jogi szabályozási, műszaki-fejlesztési és hatósági területeken felmerülő kérdéseket, az állami felhasználók igényeinek figyelembevételével.

A kutatás egyik fontos eredménye, hogy általános érvényű és fenntartható statikus műszaki követelményrendszert nem lehet felállítani, hiszen mire a jelenlegi fejlődési tendenciák mellet az életbe léptethető lenne, a technikai lehetőségek már régen meghaladták az abban megfogalmazottakat. Ezért egy olyan dinamikus megoldásra van szükség, ami a fejlesztőket és felhasználókat egyaránt rugalmasan képes támogatni egy adott feladat végrehajtásához szükséges optimális eszközrendszer kialakításában. Ennek érdekében egy olyan kiterjedt központi adatbázis és a hozzá tartozó többszintű döntés-előkészítő rendszer kerülne kialakításra, amely tartalmazza a piacon elérhető összes pilóta nélküli légijármű rendszert, azok műszaki paramétereivel, repülési jellemzőivel, tulajdonosi és beszállítói hátterével. Ezen felül naprakész információkat tartalmaz a világban folyó fejlesztésekről, továbbá az egyes alrendszerek esetében hozzáférhető modulokról (robotpilóták, akkumulátorok, motorok, szenzorok, kommunikációs rendszerek, sárkányszerkezetek stb.) azok minden fizikai paraméterével, karakterisztikáival, határértékeivel, illetve egyéb kiegészítő adatokkal. A speciális keresőmotor a felhasználók által megadott szűrési feltételek mellet egy online katalógushoz hasonlóan megoldási alternatívákat kínál az egyes részegységekre, illetve a

komplex rendszerre vonatkozóan, értékelve azok keresési feltételeknek való megfelelésének mértékét.

A kutatás másik fontos megállapítása, hogy a kereskedelmi és a közszolgálati alkalmazások támogatásához egy olyan magas autonómiával rendelkező forgalomszervezési és forgalomirányítási rendszer kidolgozására, majd megvalósítására van szükség, amellyel biztonságosan kezelhető például egy városi környezetben kialakított drónlégtér forgalma. A működés alapja, hogy minden UAS rádiókapcsolaton keresztül közvetlenül továbbítja azonosítóját és telemetriai adatait a rendszer regionális feldolgozó központja felé, amely így nyomon tudja követni az eszközöket, illetve előre megbecsülni pályájukat. A veszélyhelyzetek elkerülése érdekében be tud avatkozni az egyes eszközök vezérlésbe, figyelembe véve azok prioritás szintjét (pl. állami, kereskedelmi, hobbi), típusát (pl. merevszárnyas, forgószárnyas) és repülési tulajdonságait. Egy ilyen, vagy ehhez hasonló megoldás természetesen komoly infrastruktúrát, szabványosított eszközparkot és kommunikációs protokollokat igényel, de a jelenlegi fejlődési tendenciák alapján erre mindenképpen szükség lesz, ha élni szeretnénk a pilóta nélküli rendszerek alkalmazása által kínált lehetőségekkel.

FELHASZNÁLT IRODALOM

[1] MANNHEIM K.: Mannheim, Karl (1969), *„A nemzedéki probléma”* In: Ifjúságszociológia, Közgazdasági és Jogi Könyvkiadó, Budapest, 1969. 31-68. o.

[2] HOWE, N., STRAUSS, W.: *Generations: The History of America’s Future, 1584 to 2069.* William Morrow & Company, New York, 1991.

[3] HAIG ZS.: *Információ – Társadalom – Biztonság*, NKE Szolgáltató, 2015, ISBN: 9786155527081

[4] NAGY Á., KÖLCSEY A.: *Az Alfa-generáció margójára: Marketing vagy tudomány?!*, In: Korszerű szemlélet a tudományban és az oktatásban, Selye János Egyetem, Komárno, 2016. ISBN 978 80 8122 187 3, 1-11. o. http://real.mtak.hu/62421/1/0_alfagenerac_selyekonf_u.pdf (Letöltve: 2018.06.20.)

[5] NÉMETH A.: *UAV-k alkalmazása a közfeladatok ellátása során I.*, Hadmérnök, 2018/2, 37-60. o.

[6] Magyarország Alaptörvénye (2011. április 25.) https://net.jogtar.hu/jogszabaly?docid=A1100425.ATV (Letöltve: 2018.02.20.)

[7] 2010. évi XLIII. törvény a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról https://net.jogtar.hu/jogszabaly?docid=a1000043.tv (Letöltve: 2018.02.20.)

[8] 1994. évi XXXIV. törvény a Rendőrségről https://net.jogtar.hu/jogszabaly?docid=99400034.TV (Letöltve: 2018.02.20.)

[9] 293/2010. (XII. 22.) Korm. rendelet a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve kijelöléséről, valamint feladatai ellátásának, a kifogástalan életvitel ellenőrzés és a megbízhatósági vizsgálat részletes szabályainak megállapításáról https://net.jogtar.hu/jogszabaly?docid=a1000293.kor (Letöltve: 2018.02.20.)

[10] Terrorelhárítási Központ alapító okirata, módosításokkal egységes szerkezetben https://net.jogtar.hu/jogszabaly?docid=A12K0542.MKA&getdoc=1

(Letöltve: 2018.02.20.)

[11] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról https://net.jogtar.hu/jogszabaly?docid=99500125.TV (Letöltve: 2018.02.20.)

[12] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról https://net.jogtar.hu/jogszabaly?docid=a1100128.tv

(Letöltve: 2018.02.21.)

[13] 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről https://net.jogtar.hu/jogszabaly?docid=99500107.tv (Letöltve: 2018.02.21.)

[14] 2016. évi LXIX. törvény a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról https://net.jogtar.hu/jogszabaly?docid=A1600069.TV&timeshift=fffffff4&txtreferer=00000001.TXT (Letöltve: 2018.02.21.)

[15] 361/2016. (XI. 29.) Korm. rendelet a Bevándorlási és Menekültügyi Hivatalról https://net.jogtar.hu/jogszabaly?dbnum=1&docid=A1600361.KOR&mahu=1

(Letöltve: 2018.02.21.)

[16] 2010. évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról https://net.jogtar.hu/jogszabaly?docid=a1000122.tv (Letöltve: 2018.02.21.)

[17] 30/2011. (IX. 22.) BM rendelet a rendőrség szolgálati szabályzatáról https://net.jogtar.hu/jogszabaly?docid=A1100030.BM&celpara=163&goto=-1

(Letöltve: 2018.02.22.)

[18] FINSZTER G.: *Rendészettan*, Dialóg Campus Kiadó, Budapest, 2018. 204-205. o. http://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_EKM_Rendeszettan.pdf

(Letöltve: 2018.06.12.)

[19] A rendőrség szervezete http://www.police.hu/hu/a-rendorsegrol/testulet/altalanosan/a-rendorseg-szervezete (Letöltve: 2018.02.22.)

[20] 323/2010. (XII. 27.) Korm. rendelet az Állami Népegészségügyi és Tisztiorvosi Szolgálatról, a népegészségügyi szakigazgatási feladatok ellátásáról, valamint a gyógyszerészeti államigazgatási szerv kijelöléséről https://net.jogtar.hu/jogszabaly?docid=A1000323.KOR&mahu=1 (Letöltve: 2018.02.22.)

[21] 378/2016. (XII. 2.) Korm. rendelet egyes központi hivatalok és költségvetési szervi formában működő minisztériumi háttérintézmények felülvizsgálatával összefüggő jogutódlásáról, valamint egyes közfeladatok átvételéről https://net.jogtar.hu/jogszabaly?docid=A1600378.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (Letöltve: 2018.02.22.)

[22] 382/2016. (XII. 2.) Korm. rendelet a közlekedési igazgatási feladatokkal összefüggő hatósági feladatokat ellátó szervek kijelöléséről https://net.jogtar.hu/jogszabaly?docid=a1600382.kor (Letöltve: 2018.02.23.)

[23] 392/2016. (XII. 5.) Korm. rendelet a katonai légügyi hatóság kijelöléséről https://net.jogtar.hu/jogszabaly?docid=A1600392.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (Letöltve: 2018.02.23.)

[24] 22/2012. (II. 29.) Korm. rendelet a Nemzeti Élelmiszerlánc-biztonsági Hivatalról https://net.jogtar.hu/jogszabaly?docid=a1200022.kor (Letöltve: 2018.02.23.)

[25] 387/2016. (XII. 2.) Korm. rendelet a fogyasztóvédelmi hatóság kijelöléséről https://net.jogtar.hu/jogszabaly?docid=A1600387.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (Letöltve: 2018.02.23.)

[26] 1997. évi CLIX. törvény a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról https://net.jogtar.hu/jogszabaly?docid=99700159.TV

(Letöltve: 2018.02.24.)

[27] 4/2000. (I. 21.) Korm. rendelet a természetvédelmi őrökre, illetve őrszolgálatokra vonatkozó részletes szabályokról https://net.jogtar.hu/jogszabaly?docid=a0000004.kor

(Letöltve: 2018.02.24.)

[28] 29/1998. (IV. 30.) FM rendelet a mezőőrök és a hegyőrök szolgálati viszonyáról https://net.jogtar.hu/jogszabaly?docid=99800029.fm (Letöltve: 2018.02.24.)

[29] 2013. évi CII. törvény a halgazdálkodásról és a hal védelméről https://net.jogtar.hu/jogszabaly?docid=a1300102.tv (Letöltve: 2018.02.24.)

[30] 1999. évi LXIII. törvény a közterület-felügyeletről https://net.jogtar.hu/jogszabaly?docid=99900063.TV (Letöltve: 2018.02.24.)

[31] 2011. évi CLXV. törvény a polgárőrségről és a polgárőri tevékenység szabályairól https://net.jogtar.hu/jogszabaly?docid=a1100165.tv (Letöltve: 2018.02.24.)

[32] 2012. évi XXXVI. törvény az Országgyűlésről https://net.jogtar.hu/jogszabaly?dbnum=1&docid=A1200036.TV&mahu=1

(Letöltve: 2018.02.24.)

[33] 2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról https://net.jogtar.hu/jogszabaly?docid=A1500042.TV

(Letöltve: 2018.02.24.)

[34] 2004. évi CV. törvény a honvédelemről és a Magyar Honvédségről https://mkogy.jogtar.hu/jogszabaly?docid=a0400105.TV (Letöltve: 2018.03.01.)

[35] 78/2011. (V. 12.) Korm. rendelet a Magyar Honvédség által védendő létesítmények kijelöléséről, valamint a magyar állam folytonosságát és függetlenségét megtestesítő ereklyék köréről és az őrzésükre vonatkozó szabályokról https://net.jogtar.hu/jogszabaly?docid=A1100078.KOR (Letöltve: 2018.03.01.)

[36] 223/2014. (IX. 4.) Korm. rendelet a vízügyi igazgatási és a vízügyi, valamint a vízvédelmi hatósági feladatokat ellátó szervek kijelöléséről https://net.jogtar.hu/jogszabaly?docid=A1400223.KOR (Letöltve: 2018.03.01.)

[37] 1993. évi LXII. törvény a frekvenciagazdálkodásról https://mkogy.jogtar.hu/jogszabaly?docid=99300062.TV (Letöltve: 2018.03.01.)

[38] 2010. évi CLXXXV. törvény a médiaszolgáltatásokról és a tömegkommunikációról https://net.jogtar.hu/jogszabaly?docid=A1000185.TV (Letöltve: 2018.03.01.)

[39] 2013. évi XXII. törvény a Magyar Energetikai és Közmű-szabályozási Hivatalról https://net.jogtar.hu/jogszabaly?docid=a1300022.tv (Letöltve: 2018.03.01.)

[40] 322/2006. (XII. 23.) Korm. rendelet az Országos Mentőszolgálatról https://net.jogtar.hu/jogszabaly?docid=a0600322.kor (Letöltve: 2018.03.01.)

[41] 322/2006. (XII. 23.) Korm. rendelet az Országos Mentőszolgálatról https://net.jogtar.hu/jogszabaly?docid=a0600322.kor (Letöltve: 2018.03.01.)

[42] 2010. évi CXXVI. törvény a fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról https://net.jogtar.hu/jogszabaly?docid=a1000126.tv

(Letöltve: 2018.03.03.)

[43] 66/2015. (III. 30.) Korm. rendelet a fővárosi és megyei kormányhivatalokról, valamint a járási (fővárosi kerületi) hivatalokról https://net.jogtar.hu/jogszabaly?docid=a1500066.kor

[44] http://www.kormanyhivatal.hu/hu/pest/szervezet (Letöltve: 2018.03.03.)

[45] PALIK M.: *A Pilóta nélküli repülés rövid története* In: PALIK M. (szerk.): Pilóta nélküli repülés profiknak és amatőröknek, NKE, Budapest, 2013, 281-298. o. ISBN: 978-963-08-6923-2; http://www.repulestudomany.hu/kiadvanyok/UAV_handbook_Secon_edition.pdf (letöltve: 2017.11.30.)

[46] *Military Drone Market worth over $13bn by 2024, Global Market Insights*, 2018.04.06 https://www.gminsights.com/pressrelease/military-drone-uav-market

(Letöltve: 2018.05.13.)

[47] https://www.gminsights.com/industry-analysis/military-drone-market

(Letöltve: 2018.05.13.)

[48] *Unmanned Aircraft Systems Roadmap 2005-2030* https://fas.org/irp/program/collect/uav_roadmap2005.pdf (Letöltve: 2017.10.02.)

[49] http://www.northropgrumman.com/Capabilities/GlobalHawk/Documents/Datasheet_GH_Block_40.pdf (Letöltve: 2018.06.12.)

[50] PAPP I.: *A pilóta nélküli légijárművek alkalmazása harctéri műveletek során*, Repüléstudományi Közlemények, 2014/2. 499-510. o. http://www.repulestudomany.hu/kulonszamok/2014_cikkek/2014-2-39-0120_Papp_Istvan.pdf (letöltve: 2018.04.12.)

[51] http://cms.ipressroom.com.s3.amazonaws.com/295/files/20166/577f18372cfac249594371b4_pgL_GL-10001_002/pgL_GL-10001_002_abd7ad96-eaea-4cac-ab35-33436b962d17-prv.jpg (letöltve: 2018.05.20.)

[52] BÉKÉSI B.: *Pilóta nélküli légijárművek jellemzése, osztályozásuk*, In: PALIK M.: Pilóta nélküli repülés profiknak és amatőröknek, második, javított kiadás, 2015, 65-109. o. ISBN: 978-615-5057-64-9

[53] KÁROLY K.: *Globális Műholdas Navigációs Rendszerek alkalmazási lehetőségei katonai és polgári célú flotta- és erőkövetési rendszerekben*, Honvédségi Szemle, 2018/1. 83-97.o.

[54] *Top 10 Heavy Lift Drones* https://filmora.wondershare.com/drones/top-heavy-lift-drones.html (letöltve: 2018.06.10)

[55] *Vezetékes táplálású drón* https://rotorsandcams.com/drotosdron/ (Letöltve: 2018.06.05.)

[56] KÁROLY K.: Kis magasságú ballonok honvédelmi alkalmazásának lehetőségei, különös tekintettel a Magyar Honvédség távközlési igényeinek támogatására, Repüléstudományi Közlemények, 2017/2. 293-308. o. http://www.repulestudomany.hu/folyoirat/2017_2/2017-2-21-0397-Karoly_K-Miko_Gy.pdf (letöltve: 2018.06.10)

[57] https://upload.wikimedia.org/wikipedia/commons/8/8d/OnyxStar_HYDRA-12.jpeg (letöltve: 2018.06.10)

[58] PETRÉTEI D.: *A drónok krimináltechnikai és rendészeti felhasználása,* Magyar Bűnüldöző, 4 évf. 1-3. szám, 2015, 70-81. o.

[59] BODNÁR L., RESTÁS Á., QIANG, X.: *Conceptual Approach of Measuring the Professional and Economic Effectiveness of Drone Applications Supporting Forest fire Management*, Procedia Engineering, Vol. 211, 2018, 8-17. o.

[60] RESTÁS Á.: *Az UAV közszolgálati alkalmazásai*, In: PALIK M.: *Pilóta nélküli repülés profiknak és amatőröknek*, második, javított kiadás, 2015, ISBN: 978-615-5057-64-9, 241-280. o.

[61] PALIK M., RESTÁS Á.: *Pilóta nélküli légijárművek alkalmazásának lehetőségei az árvízi védekezésben*, Repüléstudományi Közlemények, 2014/3. 57-65. o. http://www.repulestudomany.hu/folyoirat/2014_3/2014-3-05-0223_Palik_M-Restas_A.pdf (letöltve: 2018.04.30.)

[62] MAKKAY I.: *Pilóta nélküli légijárművek hasznos terhei*, In: PALIK M.: *Pilóta nélküli repülés profiknak és amatőröknek*, második, javított kiadás, 2015, ISBN: 978-615-5057-64-9, 143-172. o.

[63] PÁNYA N.: *A pilóta nélküli légi járművek vizsgálata autonómia szempontjából*, Repüléstudományi Közlemények, 2016/1. 81-94. o. http://www.repulestudomany.hu/folyoirat/2016_1/2016-1-08-0322_Panya_Nandor.pdf (letöltve: 2018.04.30.)

[64] DUNJOHN, C.: *Boeing converts F-16 fighter jet into an unmanned drone*, New Atlas, 2013.09.27. https://newatlas.com/boeing-f16-jet-unmanned-drone/29203/

(letöltve: 2018.06.10)

[65] *Unmanned Aircraft Systems Roadmap 2010-2035* http://www.rucker.army.mil/usaace/uas/US%20Army%20UAS%20RoadMap%202010%202035.pdf (letöltve: 2017.11.10)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

INVESTIGATING DAMAGE EVENTS RELATED TO THE TRANSPORT OF DANGEROUS GASES

VESZÉLYES GÁZOK SZÁLLÍTÁSÁVAL KAPCSOLATOS KÁRESEMÉNYEK VIZSGÁLATA

ENGLER Ádám

(ORCID ID: 0000-0002-0337-2497)

engler.f.adam@gmail.com;

Abstract

In the article, I will present four different, dangerous-gas-related accidents that occurred in railway, road and partly industrial conditions. These accidents took place in Hungary or abroad, and are based on true events. I would argue that conclusions drawn from these tragic events confirm the significance of safety regulations applying to storing and transporting dangerous goods on the road in avoiding further accidents of this kind. I would also like to prove that an adequate public safety plan, including personal education and technical preparation, is equally important

Keywords: *dangerous goods, safety, accident, dangerous gases, case study*

Absztrakt

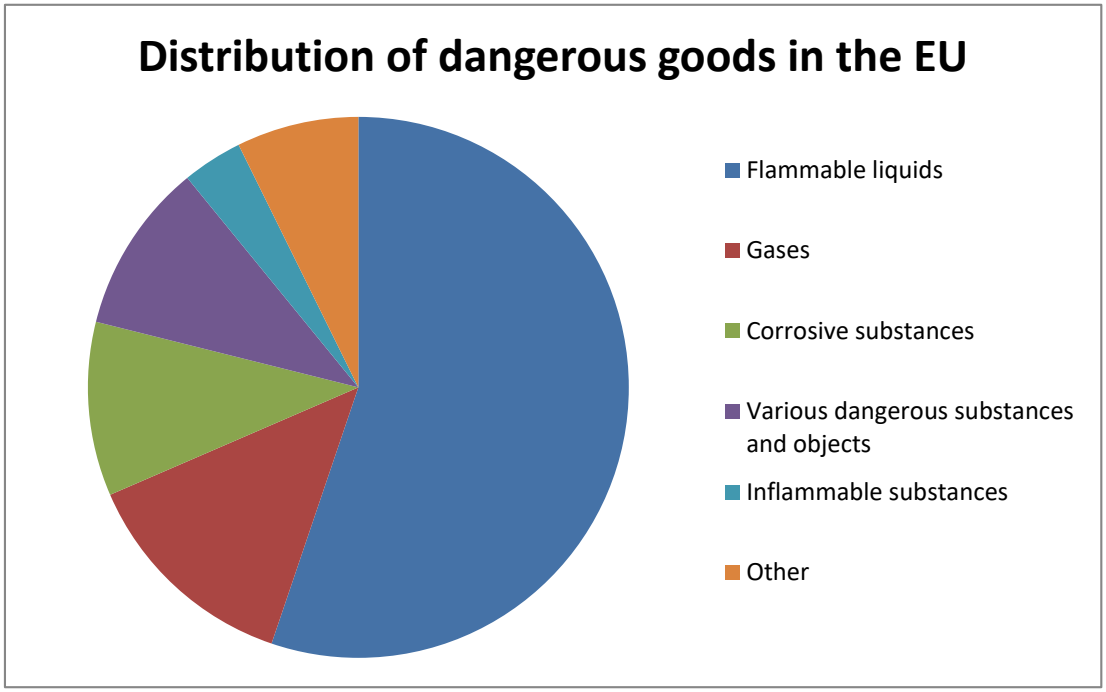
A cikkben bemutatok négy darab, veszélyes gázokhoz köthető közúti, vasúti és részben üzemi körülmények között bekövetkezett balesetet. Az ismertetett haváriák hazai és külföldi, valós eseteket dolgoznak fel, melyek tanulságaiból és az azokból levont következetésekből a veszélyes áru szállítás tárolási és szállítási biztonságát szeretném tovább erősíteni. Szeretném bebizonyítani a megfelelő védelmi tervek alkalmazásának szükségességét, valamint a személyi és technikai állomány felkészítésének fontosságát is.

Kulcsszavak: *veszélyes áru, biztonság, baleset, veszélyes gáz, esettanulmány*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.02.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.05.22.

INTRODUCTION

Given the general characteristics of dangerous goods, dangerous gases constitute the second most transported substance group on EU roads. As mentioned in my previous article, 55% of all dangerous goods are flammable liquids, and 14% of this portion is made up by gases. As a result of this, accidents related to dangerous gases occur more often than those of any other types of dangerous goods. [1]



1. **figure** Distribution of dangerous goods within the European Union (Self-made Diagram Based on [1])

What is more, even the apparent results of the increasing green house effect are unable to stop the production of these dangerous gases on a massive scale because of the developing chemical industry creating high demands for them. [2]

Definitions of these dangerous gases differ from one another, and these diverging names are based on the aspects of examination of their components.

According to ADR and RID, gas is a substance with a vapour pressure of 300kPa at 50 °C and a completely gaseous state at normal pressure (101.3 kPa at 20 °C). This definition applies to clean or pure gases, gas mixes as well as mixtures of gases with one or more components. In other definitions, gas is built up by atoms and molecules moving randomly and "bumping into each other" in space. These molecules are expanding and their movement is dependent on temperature and pressure. [3]

GROUPING OF GASES

According to ADR's and RID's definition on gases, these substances can be grouped as follows:

- Compressed Gas: in wrapping for transportation under overpressure in in gaseous form, the critical temperature is at 50 degrees Celsius or below.
- Liquefied Gas: in wrapping for transportation under overpressure in a partly in liquid form; we have to distinguish high- or low-pressure liquid gas.
- Frozen Liquefied Gas: in wrapping for transportation at low temperature is partially in liquid form as a result of its low temperature

- Dissolved Gas: in wrapping for transportation under overpressure is dissolved in liquid phase solvent
- Aerosol Wrappings and Small Tanks Filled with Gas (gas cartridges)
- Other Objects Containing Excess Gas Under Overpressure
- Gases Without Overpressure, Regulated by Special Rules (gas samples)
- Chemicals Under Overpressure: liquid, paste or dust under pressure fuelled by a substance the definition of which equals that of compressed or liquefied gas and their mixture.
- Absorbed Gas: gas absorbed on a solid, porous substance with the containing tank's inner pressure less at 20 degrees Celsius than 101,3kPa and at 50 degrees than 300kPa.

Based on the characteristics of dangerousness, these gases can be divided further as laid out in the Agreement:

- *asphyxiant*
- *inflammatory*
- *F flammable*
- *T toxic*
- *TF toxic, flammable*
- *TC toxic, corrosive*
- *TO toxic, inflammatory*
- *TFC toxic, oxidative, corrosive*
- *TOC toxic, inflammatory, corrosive*

In the UN Sample Policy, the IMDG Code and the ICAO Technical Specification gases are proportioned according their main "danger characteristics" and are put into three subgroups:

- 2.1 subgroup: flammable gases (corresponds to gases belonging to group F)
- 2.2 subgroup: non-flammable, non-toxic gases (corresponds to gases of group A / O)
- 2.3 subgroup: toxic gases (corresponds to gases belonging to group T such as T, TF, TC, TO, TFC and TOC) [3]

In the following chapters, I will present Hungarian and foreign road accidents that are related to dangerous goods, especially to dangerous gases. And in which the process and approach of authorities show many differences from country to country. Chemical safety is a set of activities and institutions aimed at reducing and avoiding the risks damage the life cycle of chemical substances causes environment. [4]

In a dangerous goods factory or work it is necessary to invent safety measures to ensure proper operation. for example: moving machines, electronic devices, switchers, valves, pipelines, fittings, tanks, reactors, furnace, pressure-gauge control, renovation and maintenance. In a mean time it is essential to prepare the employment to danger, leakage, toxic cases and fire cases with the development of safety infrastructure. [5]

If there is a car accident on the road it is necessary to investigate the driver, the car/ lorry and the status of the road. Usually infrastructure development serves economic growth, but I think it is also important to highlight road safety too. [6]

Already a 45 year old British factory accident's minute book show an example that dangerous accidents can not be avoid 100%, but with proper preparation and measures the damage can be minimize / reduce. [7]

TOXIC GAS DOWNLOAD IN SZABOLCS-SZATMÁR-BEREG COUNTY (HU) [8]

On the 27th of July 2017. short after midday a call run into the emergency centre, according to that in between Komoró and Tiszabezdéd a tank car carrying UN 1040 etilen-oxid nitrogene called dangerous good, prostrated into a pit/ trench and the driver stuck in the lorry/ tank car driver's cabin. The fireman and disaster recovery unit arrived to the scene identifying the load of the truck by using safety equipment and gasmasks/scuba. The ambulance stated that the driver who was stuck in the driver's cabin is already dead. The police closed all the three road leading to the scene of the accident and the disaster recovery made a 300 metres safety zone plus they closed the area. The Romanian owner of the truck and the Austrian owner of the tank's Hungarian agent arrived on the scene, because of the carried dangerous good downloading a special equipment was needed a German technician group arrived to the scene as well. Using a gas sensor they have made a lot of measurements by proving that the disaster recovery measurement were right and the tank is not leaking.

Right after this the hoist of the disaster recovery get down the semi-trailer from the tank car so via this they were able to cut out the driver from the wreck. To the technical rescue the German chemical company's expert gave advice. The tank car left on scene got secured more by the police and the disaster recovery whilst the Mobile Chemical Laboratory of the disaster recovery made measurements to control the air. Until this they were waiting to the special equipment to arrive from Germany as well more experts. In the view of the dangerousness of the transported substance, the need of the special equipment to download and the download system on scene that has never happened before in Hungary they could finish the download and the washing of the tank car with inert gas in the evening of the fourth night from the accident.

In the damaged tank car 1860 kg of etilen-oxid remained, but they could not download that quantity without moving the tank car and risking the environment. Therefore they started burning this substance with the torching method so they released the gas- harmless- in the air. Towards this a special machine was brought to scene and got installed together so they could finish torching and burning all the substance on the ninth day.

Besides of the total road close , with help of a Hungarian company the damaged tank car got rinsed with an inert gas (nitrogene), and after the Romanian owner transported away. The wind up of the accident and road close got finished on the tenth day from the accident.

The main risk of the operation was that the transported dangerous good was toxic and had an explosive characteristic. Therefore the wind up of the accident commanded high caution. It was also a challenge that the special equipment it's installations to download the dangerous good neither was in Hungary nor the torching machine so the rescue team had to wait for that to arrive from Germany and it took a long time.

Professional and measured intervention plus the Hungarian Authorities the inland company and the foreign company co-working resulted that no dangerous substance got released in the air. Throughout the intervention no personal injury has happened.

Parallel to the damage control the competent disaster recovery made the review of the scene and made it's proceeding as result of the last one they did not find any failure by transport the dangerous good or anything that was against the ADR. [8]

2. figure Picture of the accident [8]

TANK CAR ACCIDENT ON A HUNGARIAN HIGH-WAY [8]

On the 10th of January 2016 on the M2 high-way tank car transporting deep-frozen liquid nitrogene run into /crashed into a personal car and as a result of that both vehicle fired. The fire partment of the disaster recovery authority turn off the flames of the fire and until the technician rescue they diverted the traffic by closing two lanes. The driver of the truck got carried away by the ambulance whilst the other driver died in the accident.

A company from the side upset tank car download the 10.000 l liquid nitrogen and until this operation the police and the disaster recovery authority secured the scene. The transported gas on low degree is in a liquid form and choky, therefore without any sign can cause suffocation. [8]

3. figure Pictures of the accident [8]

THE RELEASE OF A TOXIC GAS IN GERMANY [9, 10]

The accident happened on 29th of December 2005 in the commercial port of Stuttgart. Various vehicles arrive here with different dangerous waste. Most of the waste was handled in the facility of the port but some of it was transported away for further consumption. In the accident on employee died and six other got injured out of this two was the member of the rescue team and needed hospital treatment. According the data the cause of the accident was the leakage of hydrogene- sulphid while the tank car was filled/ uploaded by liquid waste (purely sinthesized hydrogene- sulphid is an achromatic, see through, extremely stinky gas and has a toxic effect to the human body). [10]

The forklift operator who nearby died in the accident because of the toxic impact of the hydrogene-sulphid. The fire department has not measured any concentration of dangerous gas in the air therefore they have left the scene of the accident. The police secured the scene and they ordered the pipe for downloading the continent of the tank cars to be downdraught. As they restarted the sucking pump immediately dangerous substances started to leak from the download aperture. Therefore the driver of the truck/lorry collapsed so they finished the downloading and they called the ambulance/ emergency and the fire department to the scene. According to the tests what the expert made the reason why the toxic gas formed was that the liquid waste reacted with a hydrogene-sulphid. As the organic sulphur was mixed with the organic compound hydrogene- sulphid released. The previous measures that was made by the company was not enough to prevent the accident even the employee who made the upload was not prepared for a sudden action. There was no plan or measure to neutralize the released gases. Because of the accident the police started a crime investigation. as a result of the accident the previous practice got finished and from that point the operator transport away the dangerous waste to another plant to further treatment and that is not happening in the trucks.

As a consequence of the accident was that the attention of the employees must be raised that these trucks are dangerous and chemical reaction inside of them must be stopped. The treatment of the dangerous waste must be done in a proper environment among regulations and by using proper measurements and reactors.

To avoid further similar accidents safety plans should be made and only certified tanks, IBC-s should be use. The necessary examinations and measures, controls should be made and the results should be documented and used. The cargo should be transported with the documents and on it he dangerousness of the substance should be seen, just as when up/download is happening an exhaust system should in operation to neutralize the released gases. During u por download only the employee who makes the process can be ont he scene and the area should be clearly signed and closed with cordons.

The further lesson that we studied from the accident was that dangerous chemical reaction can happen so any kind of leakage must be banned/ stopped and the employees should be/ must be protected as well. The previously used vehicles are not proper to handle the waste, because this type of the handling requires more safety. The responsibility should be define and the system must be supervised constantly and should be tested too and the experiences that we can get from them should be documented and used. [9]

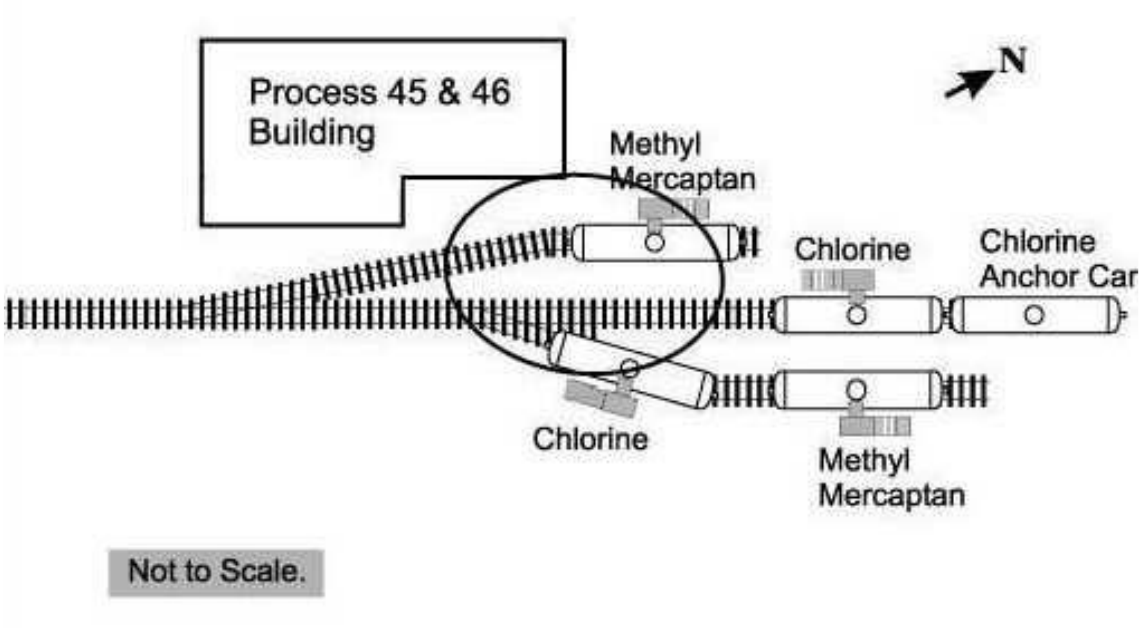
A RAILWAY TANK-CAR ACCIDENT IN THE USA [11]

In the United States, Phildelphia there is a chemical agent producer concern's center. The concern employs 400 employees twenty on-site only in the Us and sixteen more all over the world. The concern has an Unit in Michingan which is operating since 1898 and employs 212 employee in Riverwiev .The company produces hidroxilamin, amil-fenol and disulphides, sulphur and it's derives. These chemical agents are used for example: in pharmaceuticals, electronic devices (e.g.:PC-s, TV-s, CD player), beauty products, rubber/ tire, paint,

agricultural goods, water treatment, photo papers. during the manufacturing they use metilmercaptan too.

4. figure State of Michigan, accident site [11]

The company's 46 on-site during the manufacturing uses chloride and methilmercaptan and through synthesis producing methansulphonil chloride and metansulphonil acid. The components of metansulphonil chloride group are used for photography goods and agricultural and pharmaceuticals, but as destabilizer and catalyst too, further as disinfectant.
The accident was on the 14th of July 2001. Three empty railway tank car was standing in the zone fr downloading close to the unit 46 building. The three empty car was changed to three filled railway tank car one was filled with metilmercaptan and the other two was filled with chlorine. all and all five railway tank car was waiting on the on-site two was filled with methilmercaptan the other two was with chlorine and the last one was an anchor car. The cars containing methilmercaptan was originally manufactured with pipes connected straight to the unit 46 as seen on the figure. The chlorine was download to the anchor car that was in a direct connection to the unit. At 3am both tank car filled with chlorine got connected and an expert employee connected the other car filled with methylmercaptan to the pipe system.



5. figure The location of railway wagons [11]

At 3:45 two employee download the mheytlmercaptan from the railway tank car when the connected and the secured pipe come off from the pipe system and the wrong valve. According to the accident reports and minute books approximately 67 and in between 74 tonnes of mhetylmercaptan released in the air. After recongnising the accident the mechanic pulled the alarm and the technician alerted the other employees and at the same/meantime the fire department. At 3:47 the signalling devices measured a high concentration of methylmercaptan on the second floor of the unit/building.

As the operator was stepping out of the building saw that the shift leader was lying on the floor close to the fire alarm and to the download zone. After the alert other employees arrived to the scene by wearing gas masks to be able to enter the zone. At the scene of the accident two dead body was found on was the operator and the other one was the shift leader. Meanwhile the fireman arrived whom started to water the tank cars that were constantly fumigating. At 3:52 other two fireman unit arrived to the scene and 3:68 two police squad arrived too. At 4:09 25 minutes after the accident as the result of the leakage toxic gas released followed by banging sounds and the tank car was in blaze the flames were approximately 60 metres tall.

The railway car exploded and as result of the explosion mhetylmercaptan released in the air. The released substance caused skin irritation, and heavy breathing. Because of the accident the fireman captain on the scene called the other fireman departments nearby for help for more fireman squads to come to the scene and as result of that they could water the the cars so the fire did not spread to the other car containing mhetylmercaptan and to the other three containing chlorine.

The weather conditions were favourable because the wind was blowing t the north-west direction so it blew away the fume from the city. The toxic cloud went to south-east direction toward the Grosseile island, that was close to the Detroit river and two brides connected to the mainland. At 5Am a smoke cloud was visible above on the northern part of the island. According to the police report the ones leaved nearby sensed some stubby smell in the air. As it was early in the morning most of the inhabitants were home at that time. To avoid further catastrophe and to measure what has happened, the decision was that they were calling the people living there and going to be evacuated from the island until the south bridge. To keep the security measure within a 1km circle 400 inhabitant got evacuated and within 10hrs 2000

people got evacuated from Riverview, Trenton, Grosseile and Wyandotte. Because of the fume the American and Canadian authorities decided that they prohibit sailing on the precise part of the Detroit river until 16:45 pm.

As to fulfil the previous request fireman arrived from five different cities and with their help they could circle the fire on the on-site within 8:30 and 9:30.

After extinguishing the fire the employees were wearing gas masks ad the found the body of the other operator lyg next to the railway tank car. After this they stated that the iron pipe was fractured and the first and the second adapter was turned out from the open valve. They could close the valve only later but the second valve that was connected to unit 46 was closed and as a luck only the sac got burned.

The sac was connecting the car containing chlorine and connected to the pipe system got damaged too. Every valve that was carrying chlorine was open so when the rescue team arrived ont he scene approximately 12 and in between 81 tonnes of chlorine released in the air and as the sac got ruptured they could only stop the leakage when they closed the valves.

The leakage stopped at 12:47.

after the accident on 14 July Saturday dawn the environmental authority at 13:00 pm with its mobil lab made measures in the air and they find the quality of the air fine and started to examine the environment too whether environmental damage happened or not.

At 14:48 the fire department ensured that the units valves and tanks dot closed and they resolve the evacuation order. From 15:00 the citizens could go back to their homes.

The fire department left the scene of the accident on the 15th of July at 2:00 am but a unit to ensure/ secure the area/stayed remained until the 17th of July.

As the result of the catastrophe huge property damage generated. The car containing methylmercaptan got destroyed 90%. The left side of the car containing the chlorine got damaged which was standing beside the car containing methylmercaptan. The tube connected to the car containing methylmercaptan melted in the fire. The guide under the car containing methylmercaptan deformed because of the intense heat. Because of the explosion the system used for measurement got destroyed.

Consequence of the accident: three lethal victim (employee) two out of them because of the inhalation of methylmercaptan and the third died because of the inhalation of fume and tissue damage. In the accident 9 worker, 3 fireman and 40 citizen got injured.1 employee after inhaling the methylmercaptan gas fainted and fall down and broke his ribs. Other 5 got injured slightly because of poisoning. The three of the rescue team got burned slightly and felt irritation in their. The citizens living close to the unit were complaining to headache, dry throat and dizziness.

Types of injury	Workers Rescue	Participants in rescue	Other persons	In total
Deadly	3	0	0	3
Serious	1	0	0	1
Easy	5	3	40	48
In total	9	3	40	52

1 table Number of injured (Self-made table Based on [11])

Characteristics of Methylmercaptan [11]

Extremely flammable, heavier than the air, and can be found above the soil. while the substance s burning toxic gas releases and it contains sulphuroxide and hydrogenesulphid. The methylmercaptan steps into a vehement reaction with oxidative substances and with water during the process steams and acid releases toxic gases (dymethil sulphid). Mixed with air and gas it creates explosive mixture, therefore in a closed system equipped with a ventilation system and explosive secure electronic device.

According to the competent authorities the main reason of the accident was that they did not keep the safety measures. The report stated that the pipes were corroded and was rusty inside and outside plus damaged was seen. At the download process they did not recognise the 1cm difference from 2,5 cm iron pipe. According to the measures the inner wall was 23% less at the fracture than a new pipe. The previously presented shows that one reason of the accident was the wrong maintenance and control of the pipe system and the other was the wrong supervision from the competent/centre authority. In the manufacturers statem stand that the pipes were not controlled the previous five year before the accident.

The manufacturer secured the provisions to download the methylmercaptan with the „usual practice script" in the users manual. This document includes the necessary processes how to install the pipes with the railway cars containing methylmercaptan and the tests to prohibit leakage during download. On the other hand the users manual did not highlighted enough that at download gas mask or respirator should be worn or an escape hood with a filter able to filter up to 5-10 minutes that would make the able to escape from the scene. The employees did not wear the proper equipment that would have detect the leaking methylmercaptan.

At the download of the chlorine the following provisions must be comply: the operator has to wear a gas mask and to detect chlorine ammonium should be used which makes white cloud when leaking, the only method to stop the leaking is to close the valve on the top of the car.

It was also stated that the on-site had no havaria plan. The local authorities stated that the released chlorine gas and other two chemical substance created the explosion sodoumhypoclorite and tefzel, which is a modified etilen, tetrafluoretilen and fluor polymer. The experts investigated on the scene the tefzel reaction with the methylmercaptan release result was heat and toxic gas. According to other opinions the sodiumhypoklorite (highly oxidative substance) and the methymercaptan reaction led to the flames.

If there would have been methylmercaptan sensor installed at zone 46 it would have been sensed the leakage between 0 and 30 ppm. The installed sensors did not sense any methylmercaptan or they showed 0 and probably they were not functioning for 24 hours.

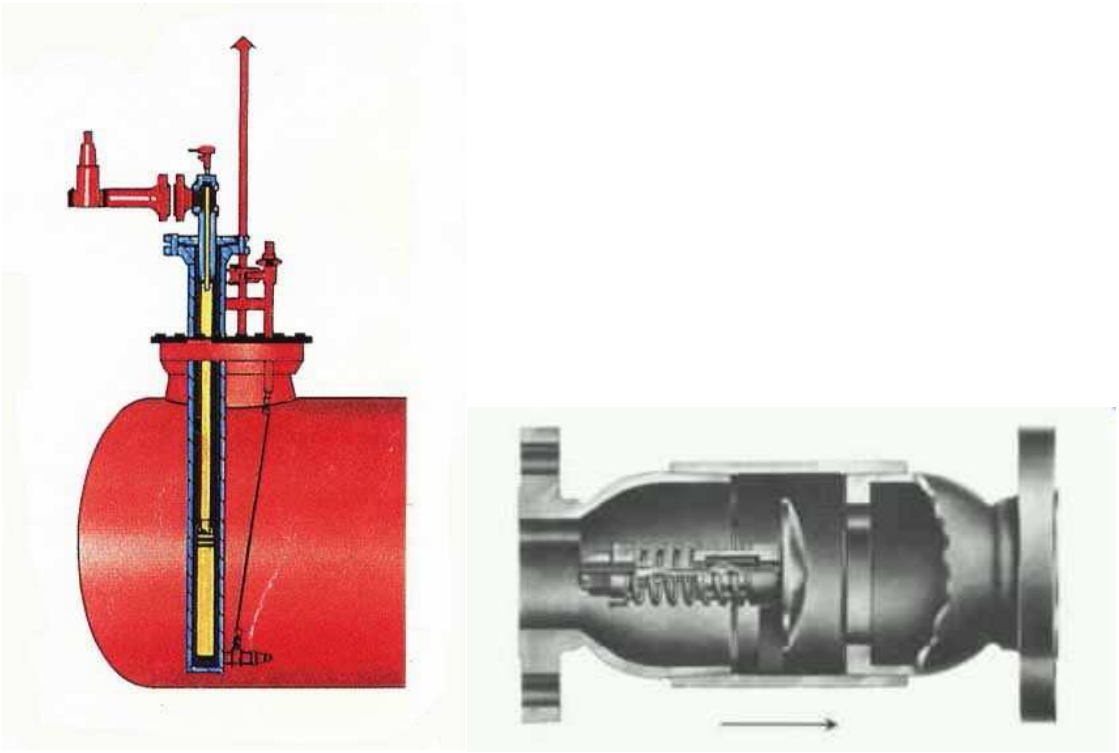
The factories in the US are supervised by several different authorities such as the central railway authority, the environmental authority, the labour and healthcare authority.

The railway authority checked the scene seven times between 1996 and 2001. These tests reflected that there were no proper equipment ot handle dangerous goods and the regulation was aslo missing so as the marking.

The environmental authority got the public safety plan only on the 3 of July 2000. At that time 14 different activities was done by the company one of it was at the unit 46 where they have to fulfil / live up to environmental a regulations/ standards. The public safety plan should be used from 4,5 tonnes for methylmercaptan and from 1,1 to chlorine. According to the scenarios at the release of the dangerous gases the installation should have been connected to the fixed parts of the building. Every each and single plan should have include the use of the safety valves to reduce the risk of an accident.

The public safety program determines the frequency with which a review is to be made between the discharging pipes, the gas detection systems and the leakage systems. Between July 2001 and June 1996, the environmental authority held an on-site visit and identified 3 of

the 2800 connection points as risky. Since the accident, the environmental authority has conducted several inspections on the site.



6. figure Safety valve [11]

From September 8 to November 2, 1994, the Labor and Health Authority of Michigan controlled the production, but Unit 46 was not tested. The inspectors found that, although they have a public safety programme, they have many shortcomings. 31 serious shortcomings and a casual offense took place. Of these 31 cases, 18 resulted from non-compliance with the safety rules and, in one case, tank, reactor and piping were not tested. Thereafter, the manufacturer agreed to introduce written procedures for checking the connection points and to carry out tests to ensure proper mechanical operation of the units. The Michigan Labor and Health Authority is not sure that these inspections have taken place at the manufacturer's premises. The manufacturer did not specify the frequency of reviews, which was why he had checked many times, sometimes did not reach the minimum. The authority emphasized the deformation of the devices and the pipe fracture. In the investigation following the accident, the authority found only 22 breaches of law regarding labor and health rules. The company paid USD 500.000 in fines and spent over USD 5.000.000 to improve worker safety.

As a post-accident measure, in March 2000, the manufacturer established a general emergency program, in particular for Block 46. This document seeks to reduce the risk of explosion, fire extinguishing, and the release of toxic substances. A single copy of the document was sent to the Riverview Emergency Services and the surrounding cities. Further training programs have been introduced at the Riverview and Wyandot firefighting stations. As a result of the accident, the company changed its operating procedures and changed the equipment. Discharging units and pipes connected thereto are dismantled every two years and check the connection points. In connection with this, the reconditioning units were redesigned. Handlers must wear a breathing apparatus when they are near the mercaptan tank and wear a protective mask that, in case of emergency, provides adequate oxygen in the discharge zone. Since the accident, every worker has to run a leak check test on the landing gear before opening the rail wagon valve.

The company decided to develop its security support system.

- a new sprinkler system has been installed,
- an underground fire extinguisher was installed and an additional 11 fire hydrants,
- re-designed the recirculation zone to separate the ferrous wagon containing methyl mercaptans from the chlorine,
- a new, more efficient sewage system was introduced in the filling area,
- firewalls, alarm and sound system were built.

Federal law stipulates that a havaria plan must be drawn up for the Riverview site for civilians and emergency intervention authorities. Despite the fact that the site had such a plan, there was no adequate information on air testing.

Local residents were not satisfied with the evacuation, especially those who lived in the northern part of Grosseile Island, because the procedure was too long for them. The head of the fire department promised to review the authorities' evacuation methods.

Local residents sued the company for negligence. The State of Michigan agreed with the company on the following terms: 6.2 million dollars for damage management.

The Ontario State Emergency Service claimed that they did not receive information about the accident at the right time. Canadian Amhertzburgi authorities only received information about the accident after several hours of passing the toxic cloud, a cloud of clouds affecting its inhabitants. The Amhertsburg Fire Department has requested that an alienation protocol between the authorities be introduced on both sides of the river in case of chemical leakage.

The director of the Riverview site proposed a meeting between the five cities' authorities and the three manufacturers to prepare a coordinated emergency alert system.

In 2002, the company undertook to pay USD 6.2 million in damages. This agreement included inter alia:

- a fine of USD 500.000,
- compensation of the evacuees of USD 550 / person,
- USD 100.000 to Riverview, USD 50.000 to Grosseil, and USD 25.000 to Trenton and Wyandot,
- Developing and implementing a USD 250.000 evaluation and monitoring program that analyzes security and emergency procedures,
- organizing emergency exercises for USD 80.000,
- training a payment fund for the deceased and the injured in the accident for USD 250.000 worth of a security center to commemorate those who died in the accident. [11]

SUMMARY

In this article, in which I summarized the currently available definitions of hazardous gases, it became clear that the existing various sorting systems are due to the different approaches towards the characteristics of these gases. The presented cases – although counting as accidents on varying levels and of sorts – all well exemplify the general threat, danger and risk posed by dangerous goods and their transportation. From the closing section of this article, it hopefully became apparent and clear how divergent the data reporting, analysing and publicity of accidents is in various countries – even though I only presented two European and a US method. A common conclusion of these case studies is the significance of the widespread understanding and application of the protection and prevention plan. In my view, the pragmatic and practical application of the protection plan is not mature enough in Hungary, and as such, I believe it to be of absolute importance to adequately inform the

market about the various solutions. Unfortunately, in many cases the very people handling these dangerous substances aren't fully aware of the danger and hazard posed by these materials, despite the fact that even a minimal sense of the risk and preparedness would help reducing or even preventing the occurrence of such events. Since the accident analyses presented in the articles above also mention the existence of protection plans (havarias), I consider preparing them to be of great importance. It has also become proven that in these protection plans, realistic protective and damage control goals have to be set out and drawn up as the main and primary aim of these plans is the prevention of a minor accident becoming a serious one. The elimination of an already escalated and dangerous situation is impossible for a crew consisting usually of only a few people. In these cases, their task remains the notification of disaster recovery forces and their adequate informing. [12, 13, 14]

Within the field of dangerous goods, hazardous gases require special attention. Through the presented cases, we could see that it is rather difficult to identify the causes leading to an accident as these may be technical, electric and human-related errors. However, it is quite complicated to find a protective and preventive plan that applies to such a wide array of possible causes. As such, it would be useful to formulate and practice a set of safety and preventive measures centred around hazardous substance awareness and personnel responsibility. Finally, I deem it to be important for the intervening authorities to have a shared and unified (at least in the EU) protocol when it comes to crime scene investigation. Furthermore, I would also argue for the publication of these reports of common criteria as this would surely prove instrumental in planning safety measures for every market participant.

BIBLIOGRAPHY

[1] http://ec.europa.eu/eurostat/statistics-explained/images/1/16/EU-28_transport_of_dangerous_goods_by_type_of_dangerous_goods%2C_2016.png (letöltve: 2018.02.25.)

[2] Food and Agriculture Organization (FAO) of the United Nations and Earthscan, 2011, *The state of the Worlds's land and water resources for food and agriculture. Managing systems at risk*. FAO ISBN: 978-92-5-106614-0 http://www.fao.org/docrep/017/i1688e/i1688e.pdf

[3] 178/2017. (VII. 5.) *Korm. rendelet a Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Európai Megállapodás „A" és „B" Melléklete kihirdetéséről, valamint a belföldi alkalmazásának egyes kérdéseiről*

[4] 2000. évi XXV. *törvény a kémiai biztonságról*

[5] DOBOR J.: *Veszélyes szerves anyagok felhasználásának katasztrófavédelmi szempontú elemzése és a szerves kémia technológiai folyamatainak összefoglalása*; http://www.hadmernok.hu/180kofop_03_dobor2.pdf (letöltve:2018.03.11.)

[6] SZÁSZI G.: *A nemzeti közlekedési infrastruktúra – a fejlesztési stratégiában meghatározott fejlesztési célok katonai aspektusai;* http://epa.oszk.hu/02700/02735/00083/pdf/EPA02735_katonai_logisztika_2016_ksz_462-482.pdf p. 478. (letöltve:2018.03.12.)

[7] Department of employment, The Flixborough disaster, Report of the Court of Inquiry, 1975, London: Her Majesty's Stationery Office, ISBN 011 3610750; https://www.icheme.org/communities/special-interest-groups/safety%20and%20loss%20prevention/resources/~/media/Documents/Subject%20Groups/Safety_Loss_Prevention/HSE%20Accident%20Reports/The%20Flixborough%20Disaster%20-%20Report%20of%20the%20Court%20of%20Inquiry.pdf

[8] BM OKF saját forrás

[9] French Ministry of the Environment - DPPR / SEI / BARPI No. 32574 Last update: June 2007 https://www.aria.developpement-durable.gouv.fr/wp-content/files_mf/A32574_ips32574_002.pdf (letöltve:2018.02.16.)

[10] Országos Közegészségügyi Intézet http://www.omfi.hu/icsc/PDF/PDF01/icsc0165_HUN.PDF (letöltve:2018.03.15.)

[11] French Ministry of the Environment - DPPR / SEI / BARPI No. 20821 Last update: October 2006 https://www.aria.developpement-durable.gouv.fr/wp-content/files_mf/FD_20821_riverview_2001_ang.pdf (letöltve:2017.12.20.)

[12] DOBOR J.: *Veszélyes gázok felhasználási lehetőségei az iparban és a mezőgazdaságban, illetve e tevékenységek kockázatai*; http://www.hadmernok.hu/180kofop_02_dobor1.pdf (letöltve:2018.03.02.)

[13] DOBOR J. – SZENDI R.: *Vegyi felderítés és mentesítés a veszélyes üzemek belső védelmi terveiben – a belső védelmi tervekkel kapcsolatban felmerülő problémák Hadtudományi Szemle, 7 1 (2014),;* p. 2.

http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10617/2014_1_hm_dobor_szendi.pdf?sequence=1&isAllowed=y (letöltve: 2018.03.16.)

[14] ENGLER Á.*: A veszélyes anyagok közúti szállításának kockázatai, különös tekintettel a terrorizmus aktuális helyzetére;* http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2017_4sz/02_Engler%20Adam_MKK%20cikk.pd p. 17. (letöltve:2018.03.02.)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

HOW TO ANALYZE TRAFFIC WAVES

HOGY VIZSGÁLJUNK FORGALMI HULLÁMOKAT

MIKA Péter

(ORCID: 0000-0002-9149-1882)

mika.peter@sze.hu

Abstract

The main problem with city traffic is the vehicles stuck in the junctions. The network disturbances cause the problem [1]. The network disturbance has significant effect from disaster prevention point of view. In case of disturbance the critic infrastructure [2] has an effect on the economic process, the social prosperity, the public health, the public safety. It is vital to recover the traffic flow on the critic infrastructure as soon as possible in this case. I suppose if the disturbance happen in downtown, where there is signalized junction, then this problem can be treated with signal program.

When happen an unexpected event on the network then appear a wave which disturbs the traffic flow. This wave is called oscillation and arises only in queue. The wave spread speed about 15 to 19 kilometers per hour according the measuring method.

In my article I analyzed wave propagation speed with three different methods, which brought different results. To analyze the traffic wave propagation process, we must have a reliable analyzing method. Whether which method the more reliable? I want to give an answer to this question with my investigation.

Keywords: *oscillation, traffic dense, traffic congestion, traffic wave propagation.*

Absztrakt

Városban a fő problémát a csomópontban bennragadt járművek jelentik. Ezt a problémát hálózati zavar okozza [1]. Katasztrófavédelmi szempontból jelentős hatása van a hálózati zavarnak. Egy zavar esetén a kritikus infrastruktúra [2] ideiglenesen hatást gyakorol a gazdasági folyamatokra, a szociális jólétre, a közegészségre és a közbiztonságra. Létfontosságú tehát, hogy ilyen esetben a kritikus infrastruktúrán levő forgalom minél előbb helyre álljon. Amennyiben ez belvárosi környezetben történik, ahol jelzőlámpás forgalomirányítás van, akkor ez a probléma kezelhető a jelzőlámpa programmal.

Amikor egy váratlan esemény következik be a hálózaton, akkor megjelenik egy hullám, amely zavarja a forgalom áramlását. Ezt a hullámot oszcillációnak nevezik és csak sorban alakul ki. Ezen hullámok terjedési sebessége 15 és 19 km/h körül alakul, függően a mérési módszertől.

A cikkemben három különböző mérési módszerrel vizsgáltam a hullámterjedés sebességét, amely különböző eredményeket hozott. A forgalmi hullám terjedési folyamatának vizsgálatához megbízható mérési módszerre van szükség. Vajon melyik módszer megbízhatóbb? Vizsgálataimmal erre a kérdésre kívánok választ adni.

Kulcsszavak: *oszcilláció, forgalomsűrűség, forgalmi dugó, forgalmi hullámterjedés*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.07.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.24.

INTRODUCTION

Several theoreticians have endeavoured to construct mathematical models to explain observed phenomena in traffic dynamics. These models have two main approaches. The first model is a car-following (microscopic), the second model is a "Traffic fluid" (macroscopic) which based on the equation of continuity. At present these models construct a considerable part of literature. The principal papers have been summarized in three published books [3,4,5].

I will show three different analysing methods which give three different results in this paper.

I created a simple simulation environment for the analysis of traffic oscillation. I made the analysis with traffic plan software. According to my thesis, if an unexpected incidence happen between two junctions, the cars stuck in the previous junction, which reducing the capacity, not only on the way it happened, but in the transverse direction as well.

The signal program can be treating the changed traffic conditions. The traffic volume specifies the green time. The traffic volume is zero, if the density is zero. Firstly, we speak about lower traffic density, while the traffic volume is low initially. Then the vehicle can move with free speed. The vehicle gets interacted with each other with increasing the traffic volume. Increasing density increase the traffic volume. There is a maximum point which is the maximum of the permeability of the link.

In the changed condition the traffic density is increased and the velocity is reduced. The traffic oscillation will be more because of traffic density, and congestion appears at the junction.

The traffic volume determines the signal program in the practice, but when we modifying a signal program then we must take account the oscillation. In the moving coordinate-system the density is constant in time. So the perturbation in the homogeneous traffic spreads with *c* velocity. Therefore, we say that the density moves as a wave. I will show how spread the oscillation caused wave in the next chapter.

THE EXAMINATION METHODS OF TRAFFIC WAVES

Fundamental diagram (macroscopic)

By the 1930s, vehicular traffic in the USA had already reached the level that required management. The first step towards this was to collect traffic data. Empirical data were collected by using photographic measurements at cross section, and the data were summarized by the so-called flux-density or fundamental diagram, where the flux (number of vehicles passing the cross section in unit time) was plotted as a function of traffic density (Greenshields 1935). Since then, FDs have been used to characterize traffic behaviour [6].

Lighthill and Whitham and later Richards presented a theory of flow. This theory is about a long crowded highway modelled with a continuous "traffic fluid" instead of individual vehicles [6]. This is the fundamental hypothesis, which has been created by Greenshields. He measured traffic on a highway then he presented the measured results in various diagrams.

The next connection exists between the traffic volume and density.

$$q(t,x) = \rho(t,x)v(t,x) \qquad (1)[7]$$

Thus the (1) equation creates a contact between the common macroscopic traffic variables, ρ, v. There are numerous velocity-density relationships demonstrated in the literature, e.g. GreenShields (1935), Greenberg (1959) [7]. Péter T. says that classical

literature does not pay attention to the environmental factor, but the velocity is determined by another environmental parameterization [8].

In case of a macroscopic model, the spatial average speed is equal with the equilibrium speed.

$$v(t,x) = V(\rho(t,x)) \quad (2)[9]$$

Therefore, the (2) LWR hypothesis declares that the traffic dense unambiguous define the average speed in steady state [9]. This relation describe immediately reaction, thus it doesn't take attention for the driver's finite reaction time and the vehicles acceleration and deceleration time. We can describe the traffic's properties with this traffic variable.

Luis Albert Pipes [10] says that shock wave spread speed is a S border line which divides two distinct concentrations of traffic ρ_1 and ρ_2 along a straight highway **Fig.1**. The vertical line S, which has velocity c, is assumed to be in the positive x direction. The mean speed of the vehicles in region A is v_1 and that in B is v_2 . It is easy to see that $(v_1 - c)$ is the relative speed in the region A to the moving line S and $(v_2 - c)$ is the relative speed of the vehicles in region B to the moving line S.

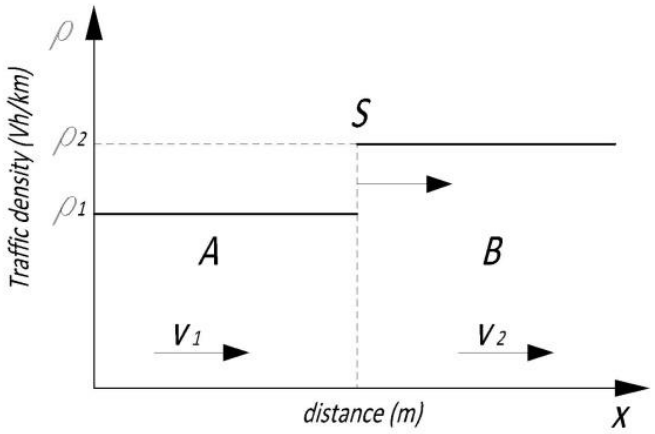


Fig. 1 The S line movement (own editing)

The shock wave velocity c as

$$c = (\rho_2 v_2 - \rho_1 v_1)/(\rho_2 - \rho_1) \quad (3)[10]$$

The equation (3) may be written in terms of the flow rates

$$c = (q_b - q_a)/(\rho_b - \rho_a) \quad (4)[10]$$

What is not other than the steepness of the fundamental diagram's two points line joining **Fig. 2.**

$$c = \Delta q(\rho)/\Delta\rho \quad (5)[10]$$

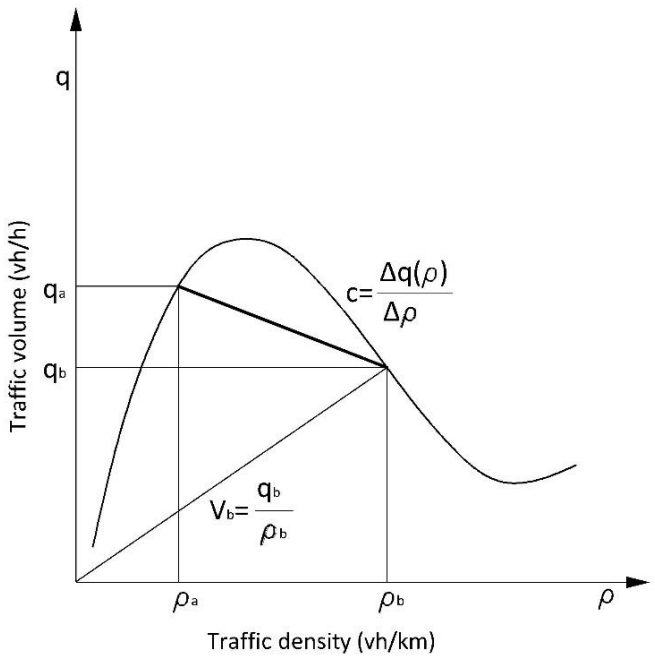


Fig. 2 The shock wave velocity (own editing)

In **Fig. 2** we can see a typical fundamental diagram [11]. We can see, that the place of $x = a$ is rare and place of $x = b$ is dense. So the wave speed line steepness is negative, therefore the wave spread back in space.

The velocity of the free flow is known. We must be defined the velocity of the flow belonging to the crowded area. Then we can read the value of the traffic volume and density at places $x_a(t)$ $x_b(t)$. After that we can calculate the c wave speed from the (4) equation.

Deviation curves (macroscopic)

Oscillation can be analysed with multi section measured traffic volume, thus the volume can be seen at different places at the same time. Furthermore, we can see how moving the traffic in space and in time. The maximum value of the traffic, time to time backs off in space. M. Mauch, M. J. Cassidy had completed an examination with this method. They said that the propagation of the wave speed is about 22 to 24 kilometre per hour, independent of the location within the queues and the flow measured there [12].

In my analysis six pieces of detectors were located on one lane road counting the vehicles passing. I modelled the network disturbance with a reduced speed area **Fig.3**. The distance between the first and the last detectors is *L=1km*.

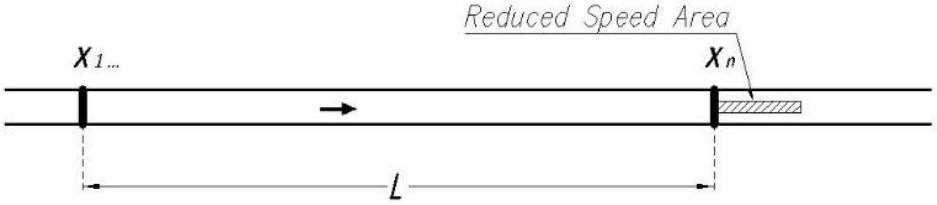


Fig. 3 Traffic lane with the detectors and the reduced speed area (own editing)

The traffic volume is a vehicle quantity, which overpassed under a time unit at the cross-section (5). The simulation software fixes the vehicle's time. See **Fig. 4**.

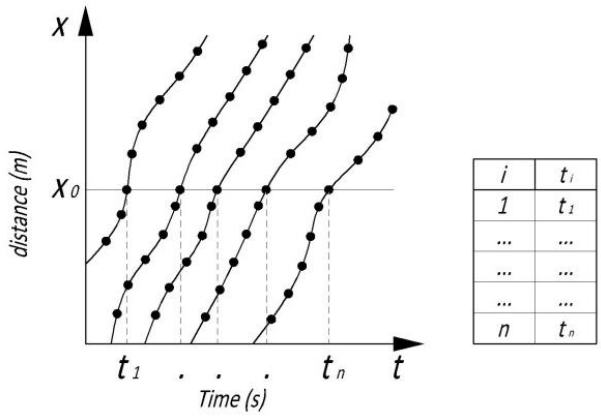


Fig. 4 The overpassed vehicles time (own editing)

$$q(x_0) = \frac{N_y(x_0)}{T_y} \tag{6}$$

Where,
$q(x_0)$: *the traffic volume*
$N_y(x_0)$: *number of vehicles at* x_0 place
T_y: *the time interval* (20sec)

I summarized the traffic in every twenty seconds, then I multiplied one hundred eighty times (6) thus I receive the hour traffic volume. After that I get a time series what I smoothed with a moving average (7).

$$Q_y(x_0) = N_y * 180 \tag{7}$$

$$Q_y^{(5)}(T_y) = \frac{Q(T_{y-2}) + Q(T_{y-1}) + Q(T_y) + Q(T_{y+1}) + Q(T_{y+2})}{5} \tag{8}$$

I sign the time interval with *Ty* and the number of vehicles *Ny*. I presented the interval in **Fig. 5**, and I counted the vehicle between two time points and I collected this data in a table.

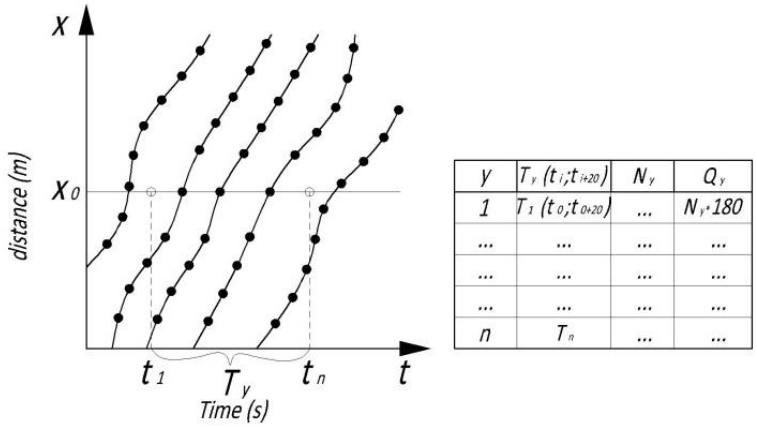


Fig. 5 The time interval (own editing)

The *c* traffic wave spread speed can be defined, with connecting the detector's graph deep points. I defined the graph's deep points at the first and the last measuring places, and I got the time when the wave starts. I defined the Q_l value, which is the minimal traffic value. Obviously there is some value under this limit, but it has a small deviation from the Q_l value. I considered one measuring hour, which is divided into 180 parts because of the time basic. I got t_i, where I cut the data series at Q_l value, then I chose the last one of the values.

I made the deviation curves from the measured data. The wiggles made prominent on some of the deviation curves are the oscillations themselves.

Fig. 6 shows the minimum point on the deviation curve. I connected the minimum points at the first and the last place, and I drew line which steepness gives the wave speed.

The dashed line traces the motion of oscillation **Fig.10**. This line is shown connecting the pit of wiggles. The line shows the oscillations propagated upstream against the flow of traffic.

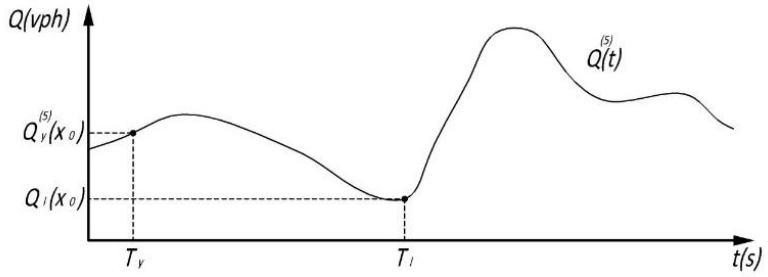


Fig. 6 The minimum point on the deviation curve (own editing)

After I had defined the first and the last time at the two measuring places, I calculated the *c* wave spread speed with the following formula.

$$c = \frac{1000}{t_i(x_1) - t_i(x_6)} * 3{,}6 \left[\frac{km}{h}\right] \tag{9}$$

Vehicles trajectory (microscopic)

I considered a car moving on a given track and I analysed this moving. When in motion, I recorded the position of the car in every s, which position was signed *x(t),* then I got a line, which is the vehicle trajectory **Fig.7**.

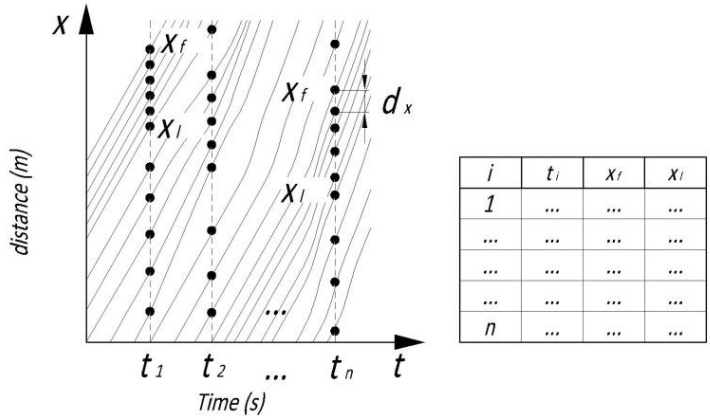


Fig. 7 Vehicle trajectory (own editing)

If I look one t_1 time moment, I can see the spatial distribution of the vehicles. The distance between two cars is defined by the (10) formula. I defined the minimal following distance and I signed it with d_{xmin}. Thus vehicles belong to a crowded area of which following distance is equal to or less than d_{xmin}.

$$d_x = (x_k - x_{k+1}) \tag{10}$$

I signed the first car x_f, and the last x_l in the crowded raw at t_1. I collected the position data at each $t - th$ s. Getting data in every twenty seconds is sufficient. From the fixed data I calculated the regression straight (11) and I divided it by twenty and multiply it with 3,6 so I got the *c* wave speed (12) in km/h. The wave speed can be calculated at the step out (x_f) and the step in (x_l) points.

$$a = \frac{\overline{(t_i * x_f(t_i))} - \bar{t}_i * \overline{x_f(t_i)}}{\overline{(t_i^2)} - (t_i^2)} \tag{11}$$

$$c = \frac{a}{20} * (-3{,}6) \left[\frac{km}{h}\right] \tag{12}$$

DESCRIPTION OF THE CASE STUDY

Building the model

First of all, I was must run a simulating process with the software and I got the data from it. I indicated the measurement places with Det.1-6. The distance between the detectors is 250m and the reduced speed area is placed after the sixth detector. This latter is needed because I can induce a traffic wave. I chose the distance of *1km* between the first and the last measuring points because I can calculate with it simply. I was must set up the traffic parameters and the measuring points and built up the model in the program **Fig. 8**. I set up the following parameters: the traffic volume was set up 2000vph, the RSA (Reduced Speed Area) time 300s-420s, the RSA desired speed 5km/h. The traffic flow speed is a variable.

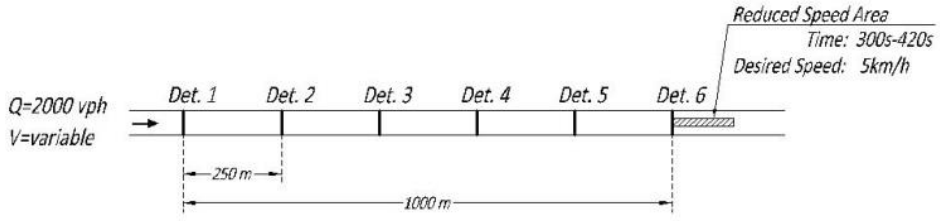


Fig. 8. The built of the model (own editing)

From the simulation I got raw data which contain the t(entry), vehicle number, vehicle speed data belong to data collection point and I got the network data which contain the vehicle number, position and speed belong to simulation seconds.

The data processing with the fundamental diagram

From the measurement I got the data illustrated in **Fig.9** below, by a point diagram. The fundamental diagram defines traffic volume in the function of traffic density. Onto this point flock can be fit a cubic polynomial and I can determine the wave speed with this.

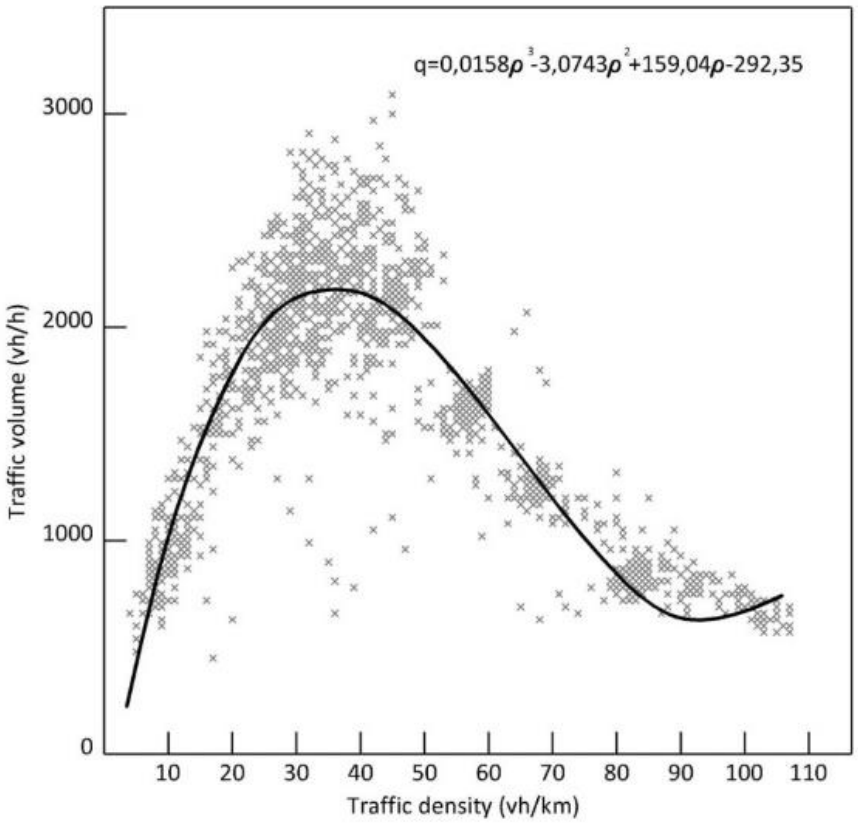


Fig. 9 The fundamental diagram (own editing)

The variable value is the traffic speed. Therefore I changed the speed from 20 km/h to 90 km/h. I calculated the wave speed with formula (5) and summarized with the analysis results in **Table 1.**

V(km/h)	20	30	40	50	60	70	80	90
q1	1331.0	1710.0	1970.0	2126.0	2185.0	2150.0	2016.0	1760.0
r1	66.0	57.0	49.0	42.0	36.0	31.0	25.0	19.0
V1	20.0	30.0	40.0	50.0	60.0	70.0	80.0	90.0
q2	617.0	2617.0	617.0	617.0	617.0	617.0	617.0	617.0
r2	95.0	95.0	95.0	95.0	95.0	95.0	95.0	95.0
V2	6.5	6.5	6.5	6.5	6.5	6.5	6.5	6.5
c (km/h)	**-24.6**	**-28.8**	**-29.4**	**-28.5**	**-26.6**	**-24.0**	**-20.0**	**-15.0**

Table 1. Traffic waves speed from the fundamental diagram (own editing)

The data processing with the deviation curves

The curve was decreased unambiguously at the fourth minute. It can be seen at **Fig. 10.** Because of extend reasons I presented the wave speed at 50km/h traffic speed.

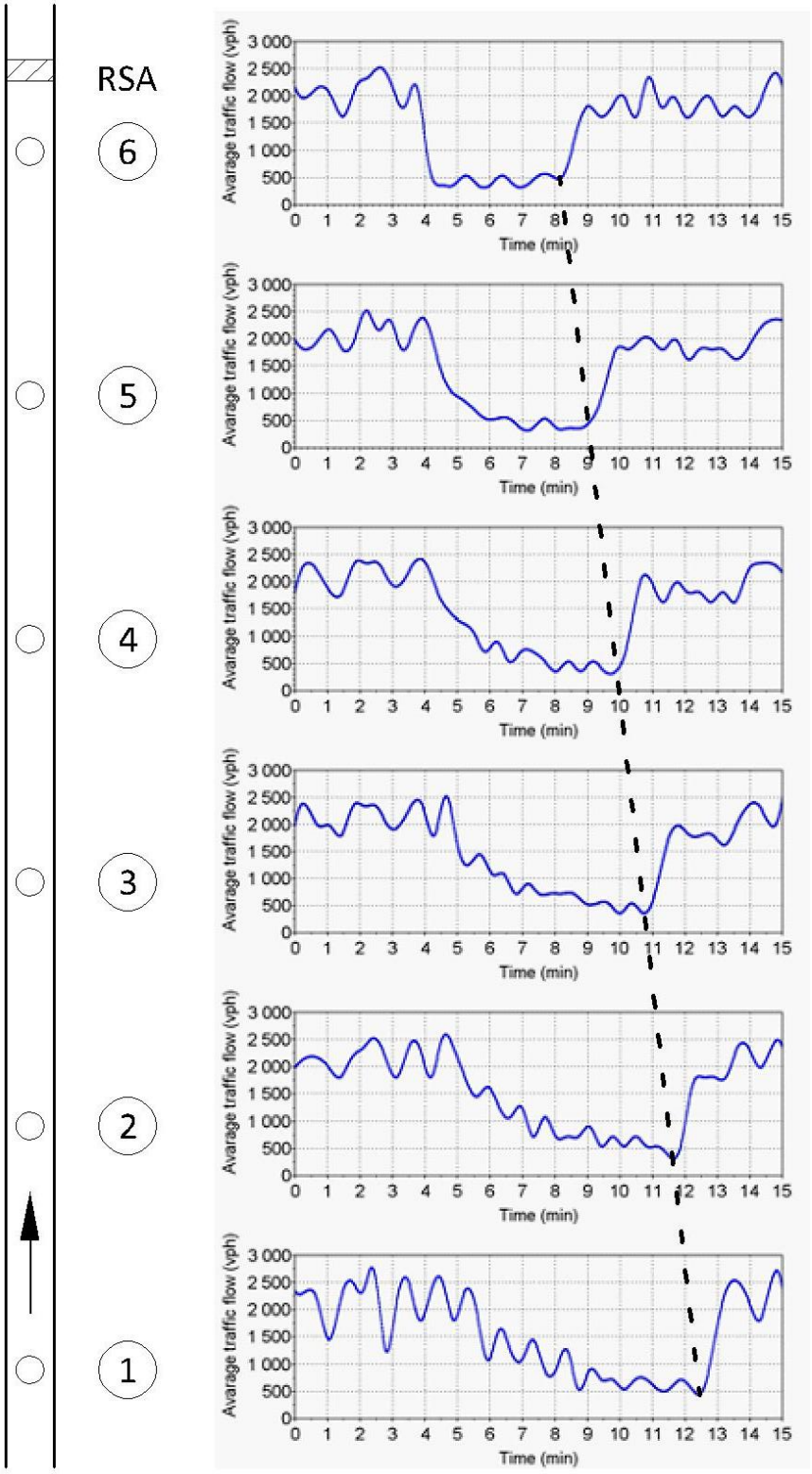


Fig. 10 The deviation curves at 50km/h (own editing)

I connected the visible lower points with a dashed line. At the lower points there is smaller traffic volume and high traffic density which means a traffic jam. The oscillation formed and spread can be shown with this method.

I identified the point where the graph starts to increase at each measurement point and connect each deep point with a dashed line. This line steepness gives the *c* wave spread speed. I summarized the wave speed in **Table 2.**

V(km/h) / Detector number	20	30	40	50	60	70	80	90
1	739	722	739	736	730	717	732	730
2	682	666	675	693	682	677	690	695
3	600	602	633	630	622	618	653	653
4	530	540	567	565	574	576	586	593
5	446	475	501	521	514	513	546	551
6	380	413	441	457	465	470	491	501
c (km/h)	**-10,0**	**11,7**	**-12,1**	**-12,9**	**-13,6**	**-14,6**	**-14,9**	**-15,7**

Table 2. Traffic wave speed of the deviation curves (own editing)

The data processing with the vehicle trajectory

With this method it is allowed that the traffic dense distribution in a particular road section and a given time moment to be observed. The individual vehicle position, which is called the vehicle trajectory, can be seen on **Fig. 11**. The picture below shows the wave emerging at 300s and exiting at approximately 800s. So I analysed this between just two time moments.

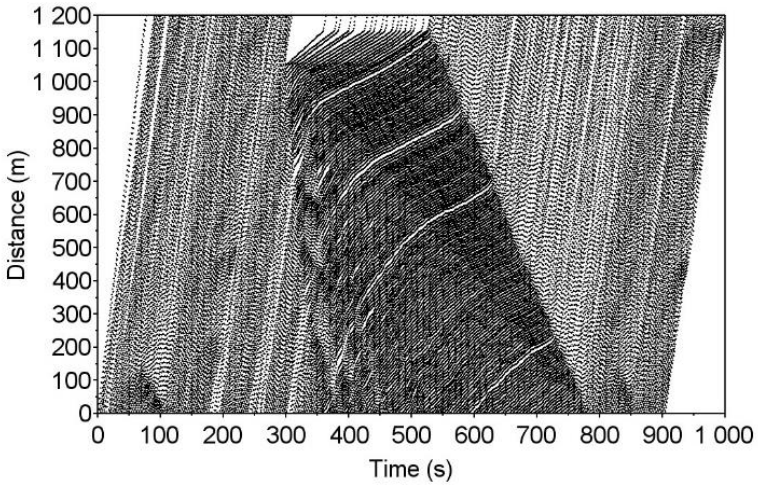


Fig. 11 Vehicle trajectory at 50km/h (own editing)

The steepness of the regression straight at the backside of the wave gives the wave spread speed. **Fig.12** depicts the wave spread speed with a red line. Because of the extend reasons just one picture is depicting, but I summarized all measured data in **Table 3.** Furthermore, if I would like to know where the wave is over, both speed lines are needed to get an intersection point which signs the end of the wave.

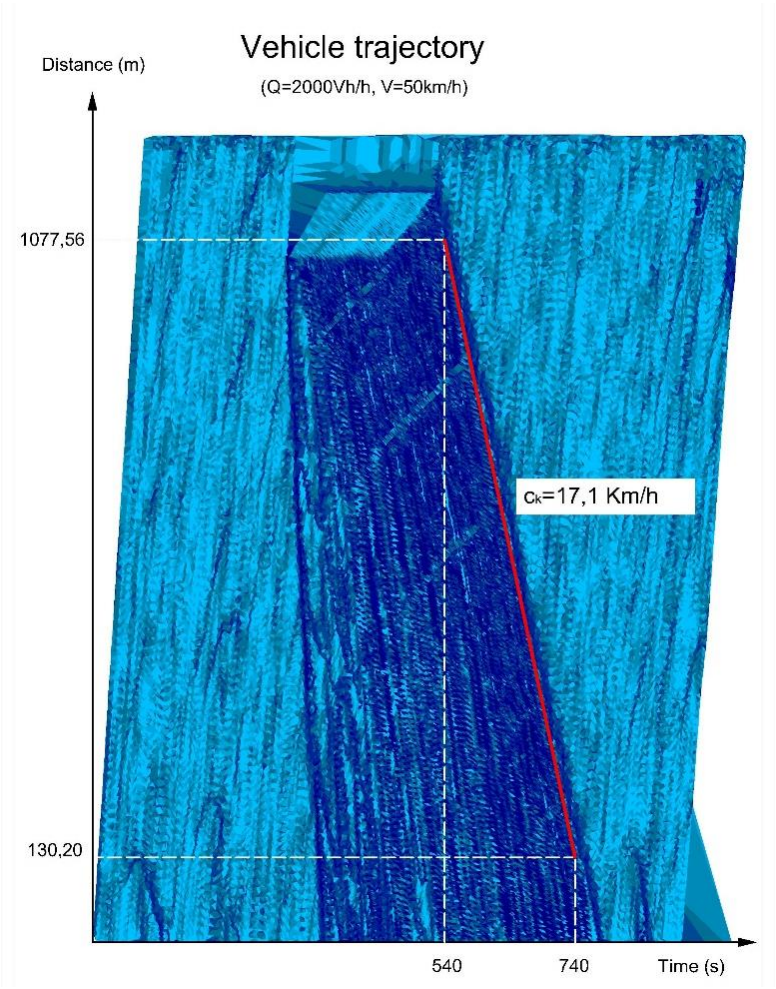


Fig.12 Steepness of the speed line (own editing)

The wave comes to an end when the wave spread speed at the wave front is more than on the "backside" of the wave. **Table 3** summarizes the wave spread speed at each traffic speed.

I defined the following distance $d_{xmin} = 10m$ and I considered a crowded area which contains minimum ten pieces of vehicles. **Table 3** below shows the c wave spread speed at difference traffic speeds.

V(km/h)	20	30	40	50	60	70	80	90
a	-85.90x +1132.30	-90.64x +1128.10	-92.88x+ 1166.00	-94.73x +1172.30	-97.34x +1155.50	-100.15x +1148.70	-101.75x +1195	-104.98x +1210.4
X1	1046.40	1037.46	1073.12	1077.56	1058.16	1048.55	1093.25	1105.42
X2	187.40	131.01	144.30	130.20	84.70	47.05	75.75	55.62
ΔX	-859.00	-906.45	-928.82	-947.36	-973.45	-1001.50	-1017.50	-1049.80
T1	540.00	540.00	540.00	540.00	540.00	540.00	540.00	540.00
T2	740.00	740.00	740.00	740.00	740.00	740.00	740.00	740.00
ΔT	200.00	200.00	200.00	200.00	200.00	200.00	200.00	200.00
c (km/h)	**-15.5**	**-16.3**	**-16.7**	**-17.1**	**-17.5**	**-18.0**	**-18.3**	**-18.9**

Table 3. The wave spread speed from the trajectory (own editing)

COMPARING THE ANALYSIS RESULTS OF THE THREE METHODS

In this chapter I compared the results obtained from the three difference methods. The diagram below **Fig.13** shows the three curves. It can be seen that the first method is definitely different from the other two measuring methods. It is seen too, that it has got a minimum of 40km/h traffic speed. It can also be seen too that 20km/h and 70km/h has the same value. Meanwhile the other curves show that the wave speed direct proportion with the traffic speed.

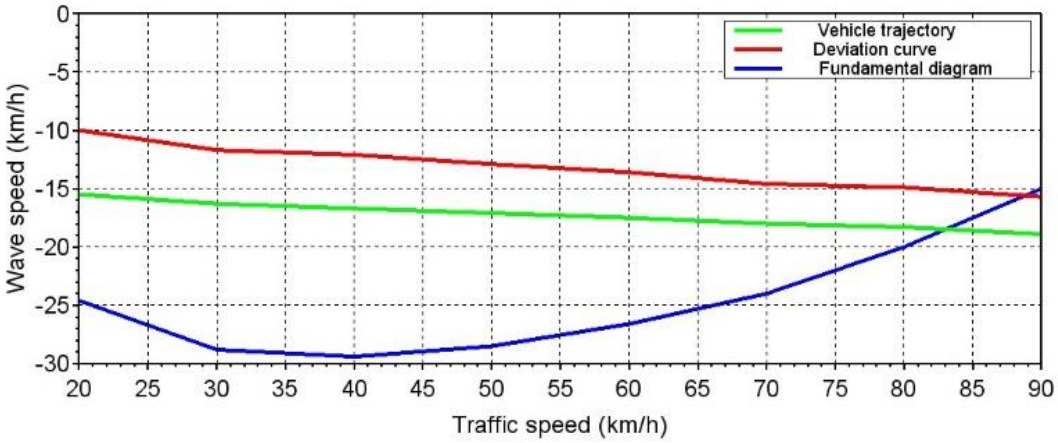


Fig. 13 The wave spread speed function as the traffic speed (own editing)

I identified that the speed difference is 5km/h between the vehicle trajectory and deviation curves. It means that the distance between two junctions for example 100m and the wave speed at the one 10km/h and 15km/h the other one then the wave arrives at junction 14 seconds earlier according to vehicle trajectory. Both curves are linear characteristic and mildly increase the absolute value. The wave speed extends in this case from 10 to 20km/h.

CONCLUSION

It turns out from the analysis that the oscillation can be shown from the measured traffic volume. I identified in this analysis that oscillation formation and propagation can be shown from the different place measured traffic volume. I regard the Vehicle Trajectory method the more reliable.

The curve from the fundamental diagram is definitely different from the others. There is a significant difference between the vehicle trajectory and deviation curve. Why the fundamental diagram is different from the other diagrams? I think to be that in the case a fundamental diagram, where the traffic is considered to be homogenous. The further examinations may shed light on this issue.

Another research opportunity is to analyse the territorial dispersion of the vehicles at a given road section. My next examination is how to mitigate the traffic wave with signal lamp.

REFERENCES

[1] TÓTH B.: *Állomások és állomásközök zavarának gráfelméleti alapú vizsgálata a magyarországi vasúthálózaton,* Hadmérnök XII. 4. (2017) p. 52-66.

[2] HORVÁTH, A.: *A kritikus infrastruktúra védelem, mint kritikus infrastruktúra* In: HORVÁTH, A. (szerk.): *Fejezetek a kritikus infrastruktúra védelméből*; Magyar Hadtudományi Társaság, Budapest, 2013., p. 167-190. (ISBN 978-963-08-6926-3)

[3] R. HERMAN.: *Theory of Traffic Flow*, American Elsevier Publishing Co., New York, 1961.

[4] F. A. HAIGHT.: *Mathematical Theories of Traffic Flow*, Academic Press, New York, 1963.

[5] D. L. GERLOUGH, AND D. G. CAPELLE.: *An Introduction to Traffic Flow Theory*, Highway Research Board, Spec. Rep. 79, National Academy of Sciences, Wash., D. C., 1964.

[6] G. OROSZ, R. EDDIE WILSON, G. STÉPÁN.: *Traffic Jams:dynamics and control*, Philosophical Transactions: Mathematical, Physical and Engineering Sciences, Vol.: 368, pp. 4455-4479, 2010.

[7] H. GREENBERG.: *An Analysis of Traffic Flow*, Operation Research, Vol. 7, No. 1, pp. 79-85, 1959.

[8] P. TAMÁS, S. FAZEKAS.:*Determination of vehicle density of inputs and outputs and model validation for the analysis of network traffic processes*, Peryodica Polytechnica , pp. 53-61, 2014.

[9] M.J. LIGHTHILL, G.B. WHITHAM.: *On kinematic waves a theory of traffic flow on long crowded roads*, Proceedings of the Royal Society of London, Series A, Mathematical and Physical Sciences, Vol.: 229, pp. 317-345 1955.

[10] L. A. PIPES.: *Wave theories of traffic flow*, Department of Engineering Univeryity of California, Los Angeles, California

[11] L. A. PIPES.: *Car following models and the fundamental diagram of road traffic*, Transportation Research, Vol. 1, pp. 21-29., 1967. Los Angeles, California

[12] M. MAUCH, M. J. CASSIDY.: *Freeway traffic oscillations: observations and predictions*, University of California, Berkeley, California, USA

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

ВОЙСКОВЫЕ ФОРТИФИКАЦИОННЫЕ СООРУЖЕНИЯ ДЛЯ ПУНКТОВ УПРАВЛЕНИЯ

FORTIFICATIONS OF MILITARY COMMAND POSTS

HORVÁTH Tibor

(ORCID: 0000-0003-4742-847X)

horvathtibor@uni-nke.hu

Absztrakt

В начале 1980-х годов продолжились работы по созданию быстровозводимых и быстроизвлекаемых сооружений для пунктов управления. В беседах с известным инженером-фортификатором Н. С. Маштаковым были расмотрены принципальные вопросы извлечения сооружений из-под грунта. Стало ясно, что принятые ранее схемы трансформации остова извлекаемых блоков сооружений «ПАКЕТ» и «БУНКЕР Б» нуждаются в совершенствовании.

Kulcsszavak: *пункт управления, фортификатор, бункер*

Abstract

In the early 1980s, work continued on the creation of fast-erecting and quickly retrievable structures for control posts. In conversations with the well-known engineer-faculty, N. S. Mashtakov, the principal issues of extracting structures from under the ground were examined. It became clear that the previously adopted schemes for transforming the skeleton of the recoverable blocks of the „PACKET" and „BUNKER B" facilities need to be improved.

Keywords: *control posts, fortifications, bunker*

A kézirat benyújtásának dátuma (Date of the submission): 2018.07.13.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.28.

ВВЕДЕНИЕ

В начале 1980-х годов продолжилисъ работы по созданию быстровозводимых и быстроизвлекаемых сооружений для пунктов управления. В беседах с известным инженером-фортификатором Н. С. Маштаковым были расмотрены принципальные вопросы извлечения сооружений из-под грунта. Стало ясно, что принятые ранее схемы трансформации остова извлекаемых блоков сооружений «ПАКЕТ» и «БУНКЕР Б» нуждаются в совершенствовании.

Оснавные пути совершенствования схем трансформации виделись в исключении процессов (подъёма) массы грунта над сооружением, трения покоя, разрушения остаточной связности грута и прилипаемости (глина, суглинок) несущей конструкции. С учётом накопленного научного задела и результатов экспериментальных исследований были уточнены оснавные положения теории давления грунта при извлечении сооружений различной формы поперечного сечения, силы сопротивления, возникающие при извлечении, и намечены способы быстрого извлечения.

Принципиально был определен так называемый «технический облик», который подразумевал форму (внешний вид, форма поперечного сечения несущей конструкции и др.) и содержение (функционирование, сборность, извлечение, транспортирование и др.) сооружений блочного и контейнерного типа.

Главное, требовалось определиться с размерами извлекаемых блоков и контейнеров. Вот здесь и появился так наываемый «параметрический ряд» в сооружении, включающий блоки входа, технические блоки и блоки оснавного помещения. В качестве параметра (размерного модуля) был определен размер 110 см, все остальные размеры принимались кратными по отношению к нему. Эти параметры обеспечивали соблюдение оснавных требований к сооружению по размещению и нормальной работе, нормированию нагрузок при расчёте несущей конструкции, извлечении, транспортабельности и др. Правильность и обоснованность принятых параметров были очевидными. Интересно, что оснавные размеры съёмных кузовов автомобнлей, независимо разработанные 21 НИИИ, в целом совпадали с размерами параметрического ряда фортификационных сооружений для Пунктов Управления (ПУ).

Оставалось совсем «немного» - исключить оснавные негативные факторы: непосредственное давление массы грунта обсыпки на сооружение (блок, контейнер), трение покоя и силы связности т прилипаемости грунта при извлечении. Для решения этих вопросов пришлось тщательно проанализировать схемы трансформации существующих Войсковых Фортификационных Сооружений (ВФС) и способы их извлечения, учитывая каждый фактор.

В результате остановились на следующих принципиальных механизмах исключениях (уменьшения) влияния сил сопротивления при извлечении сооружения:

- — полное (частичное – 2/3 толщины грунтовой обсыпки) удаление грунта с покрытия сооружения землеройным средством или гибкими полотнищами;
- — создание свободного объёма для сброса в него грунтовой обсыпки;
- — отжим стенок извлекаемго блока (без грунтовой обсыпки на нём) на грунт в пазухах котлована для формирования свободной плоскости отрыва;
- — введение в конструкцию дополнительных повротных стенок с механизмами скольжения, которые исключают трение грунта;
- — применение плоской линейной и угловой и при необходимости объёмной трансформации извлекаемой конструкции.

Для проверки принципиальных решений механизмов исключения (уменшения) влияния сил сопротивления при извлечении были определены оснавные типы быстроизвлекаемых сооружений:

— сборно-разборное быстроизвлекаемое сооружение арочной конструкции из крупной волнистой стали;
— быстроизвлекаемое сооружение блочного типа;
— сборно-разборное быстроизвлекаемое сооружение из волнистой стали комплекта КВС-У;
— сборно-разборное быстроизвлекаемое сооружение каркасно-тканевой конструкции;
— быстроизвлекаемое сооружение контейнего типа.

На первом этапе разработали и изготовили модели и макетные образцы быстроизвлекаемых сооружений с различными механизмами снижения сил сопротивления. Для исследований соорудили специальный полевой стенд исследований моделей в реальных грунтовых условиях и измерительный стенд для грунтового лотка с песком. С целью проверки кинематических схем построили масштабные модели с геометрическим подобием размеров фрагментов блоков быстроизвлекаемых конструкций и узлов, обеспечивающих их кинематику при извлечении.

Модель блока арочной конструкции из крупной волнистой стали состояла из неизменяемой (стационарной) и изменяемой (кинематической) частей. Извлечение предусматривало предварительное снятие грунтовой обсыпки с покрытия сооружения, последующее складывание кинематической части блоков и последвательное их извлечение. Однако результаты исследований, расчёты и анализ работоспособности кинематической схемы данной модели покозали, что она не имеет никаких преимуществ перед кинематической схемой извлечения сооружения «БУНКЕР Б». В связи с этим данное направления было закрыто.

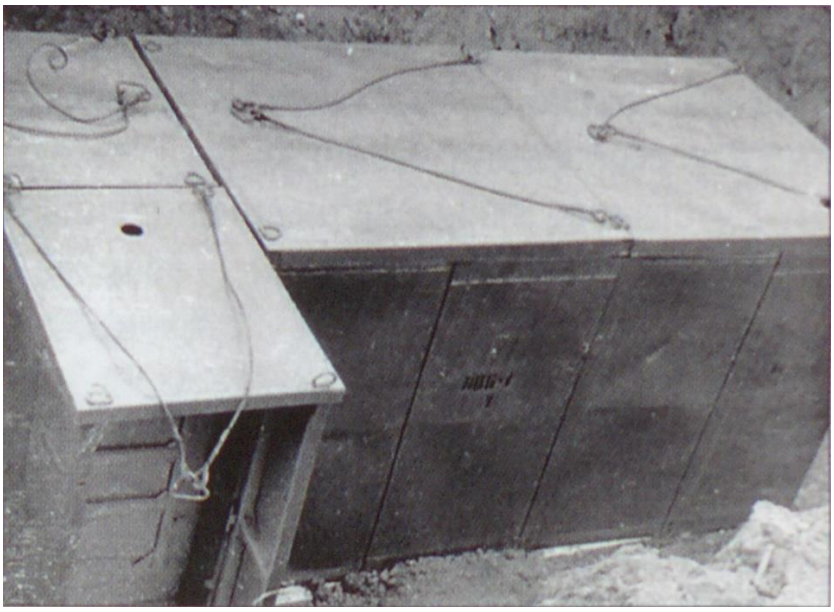
Принципиальная схема модели блока быстроизвлекаемого сооружения предусматривала стационарный объект (блок), кинематические элементы (панели), фиксируемые и постоянные свяи. По конструктивному решению и схеме извлечения блоки основного помещения и блоки входа сооружения приняли идентичными, за исключением размеров по ширине (пролету). Модель быстроизвлекаемого сооружения блочного типа изготовили в масштабе 1:4. Она состояла из двух моделирующих извлекаемых блоков оснавного помещения, каждый из которых включал поворотную панель пола, две повортные панели стен и поворотную панель перекрытия.

Заложенный принцип извлечения сооружения достаточно прост, если имеется (или создаётся) свободный пространственный объём для сбрасивания в него части грунта обсыпки с помощью поворотной панели перекрытия блока. Такой объём всегда имеется в виде примыкающей траншеи входа в сооружение, в связи с этим организуется порядок извлечения блоков сооружения. В первую очередь начиная с торцевого блока оснавного помещения, складывают элементы бытового оборудования, затем раскрепляют поворотную панель пола и переводят её внутрь блока, раскрепляют поворотные панели стен и закрывают проём блока, раскрепляют панель перекрытия с соседним блоком и так в каждом последующем блоке.

Следует учесть, что при возведении сооружения на поверхность грунтовой обсыпки выводятся тросы поворота панелей перекрытий блоков. После подготовки блоков к извлечению (начиная с первого блока входа) с помощью троса автокраном производят поворот панели, которая сбрасывает грунт в свободный объём, а затем извлекают блок входа. Так по очереди извлекают все блоки.

Исследования модели блоков оснавного помещения быстроизвлекаемого сооружения провели на полевом стенде в естественных грунтовых условиях. Результаты исследований показали перспективность конструкции и эффективность данного способа извлечения. Эксперементальные показатели усилий, необходимых при извлечении моделей, показали высокую сходимость с результатами теоретических расчётов (98%). Усилия, создаваемые на крановое оборудование при извлечении конструкции блока предложенным способом, обеспечивали надёжную и безопасную работу грузоподъёмного средства.

Эксперементальное быстроизвлекаемое сооружение блочного типа «КАМАЧ» предназначалось для защиты и работы групп управления КП тактического звена. Оснавные характеристики: рабочая площадь – 8,2 м^2, пролёт – 1,95 м, вес – до 4 т, транспортабельность – один комплект на автомобиле ЗиЛ-131, время возведения расчётом в составе 3 человек с использованием автокрана и экскаватора – 2-2,5 часов, время извлечения расчётом в составе 3 человек с помощью автокрана – 30-45 минут.



1. фото Эксперементальное быстроизвлекаемое сооружение блочного типа «КАМАЧ»[1]

С 1985 года эксперементальный образец сооружения блочного типа «КАМАЧ» проходил всесторонние испытания летом, осенью, зимой и весной, демонстрировался руководству и в целом получил положительную оценку. Однако постоянные изменения, вносимые в его конструкцию (в том числе кустарным образом) без согласования с разработчиками,привели к нарушению общих правил и требований по доводке образца до опытного и промышленного производства. Затем наступала пора «активной перестройки», которая кардинально изменила всё в стране. Эксперементальный образец сооружения блочного типа «КАМАЧ» был заброшен и почти 15 лет стоял и ржавел на площадке, пока его не сдали в металлом.

Вплоть до 1985 года исследовалась возможность модернизации сооружений КВС-У и ЛКТС, в том числе рассматривались различные направления и способы их извлечения. Остановились на способе объёмной трансформации сооружения из комплекта волнистой

[1] ВИА им. В. В. Куйбышева в Николо-Урюпино

стали, позаимствовав схему сборно-разборного двухпролётного эксперементального образца сооружения.

Оснавная идея заключалась в использовании упругости и податливости собранных на опорной раме двух арок из элементов ФВС за счёт введения в конструкцию одной арки быстроразборного стыковочного узла в верхней части рамы и шарнира в нижней её части. В итоге изготовили модель для проверки кинематики трансформации и поведения конструкции при давлении грунта в пазухах котлована на стенки сооружения. Исследования показали перпективность этого направления. На оснавании полученных данных изготовили полномасштабный экспериментальный фрагмент остова оснавного помещения и подготовили ТТЗ на ОКР по модернизации сооружения КВС-А.

Сооружение модернизированное фортификационное из элементов волнистой стали КВС-АМ предназначалось для зфщиты личного состава от средств поражения при оборудовании районов развертывания пунктов управления. Оснавные характеристики: рабочая площадь – 13,8 м^2, вместимость – 9 человек, время возведения расчётом в составе 7 человек с использованием автокрана и экскаватора – 5 часов, транспортабельность – один комплект на автомобиле ЗиЛ-131.

Сооружения КВС-АМ было выполнено сборно-разборным и включало остов и вход. Остов собирался из арок,установленных на опорную раму. Торцы остова закрывались торцовыми диафрагмами. Все арки опирались на раму и закреплялись на ней болтами. Торцевые диафрагмы соединались с рамой остова болтами. Между торцевыми диафрагмами снаружи остова по всей его длине с двух боковых сторон устанавливались продольные связи, предназначенные для повышения продольной устойчивости остоваи перераспределения нагрузки от торцовой диафрагмы на элементы всех арок.

Вход состоял из двух тамбуров и предтамбура. Тамбуры собирались из двух больших и двух малых криволинейных элементов волнистой стали.

Для получения сооружения большей площади и пролёта использовалось два комплекта, которые стыковались между собой рамами.

Таким образом, войска получили не трансформируемое быстроизвлекаемое двухпролётное сооружение, как это планировалось, а сборно-разборное, из волнистой стали, которое по эксплуатационным показателям не превосходило сооружение КВС-А. Единственным его преимуществом стала возможность создания двухпролётного сооружения из двух комплектов при их поперечной стыковке.

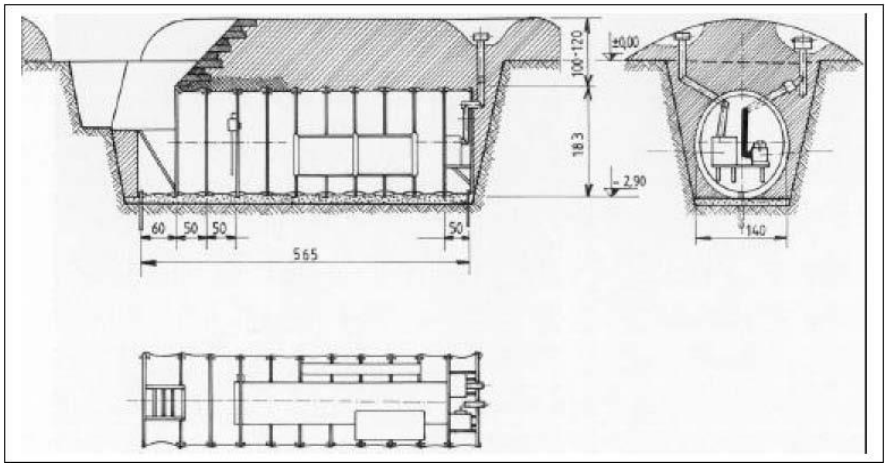
Другим направлением являлось создание сборно-разборного быстроизвлекаемого сооружения каркасно-тканевой конструкции. В качестве аналогов были приняты сооружения ЛКТС и ЛКС2. Принципиальным отличием новой конструкции стало введение в кольца остова конструкции угловых разъёмов и шарнира-дифференциала.

2. фото Сооружение из элементов волнистой стали КВС-А[2]

Кроме того, дополнительно к покрытию (его тоже видоизменили и выполнили в виде чихла) ввели два-три гибких (тканевых) покрытия для удаления грунта – наподобие конструкции грунтовых экранов. Провели теоретические исследования по определению усилий, необходимых для снятия максимальной толщины грунтовой обсыпки автомобилем и бронетранспортёром. Удалось определить размеры грунтовой обсыпки, которые можно удалить гибким покрытием с помощью автомобиля. Размеры снимаемой грунтовой обсыпки составили 45-60 см на длине 2,0-3,0 м. Извлечение сооружения проводилось за 35-40 минут: снятие грунтовой обсыпки (три слоя) занимало 20 минут, складывание остова сооружения и извлечение монтажной балкой с помощью автомобиля – 15 минут.

3. фото Сооружение каркасно-тканевой конструкции ЛКС3[3]

[2] ВИА им. В. В. Куйбышева в Николо-Урюпино
[3] ВИА им. В. В. Куйбышева в Николо-Урюпино



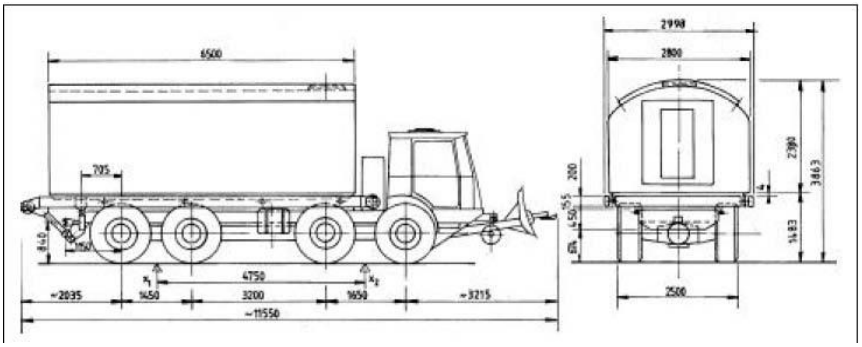
1. рис. Сооружение каркасно-тканевой конструкции ЛКС2

По результатам исследований было подготовлено ТТЗ на разработку быстроизвлекаемого каркасно-тканевого сооружения, в соответствии с которым ПФБ ИВ представило рабочую документацию. С этого момента начались коллизии: при обсуждении в НТК ИВ сотрудник, отвечающий за сопровождение проекта, не смог объяснить, для чего нужны угловые разъёмы, дифференциал и дополнительные полотнища. Затем из документации на опытный образец исключили ключевые элементы, обеспечивающие его быстрое извлечение. В конце концов, появилось сооружение ЛКС-3, которое по эксплуатационным характеристикам возведения и извлечения в целом не отличалось от прежнего ЛКС-2, изменился только вход.

Каркасно-тканевое сооружение ЛКС-3, принятое на снабжение войск в 1986 году, предназначалось для защиты, работы и отдыха личного состава на пунктах управления тактического звена. Оно включало оснавное помещение и вход. Оснавные характеристики: полезня площадь – 2,9 м^2, вместимость – 4-6 человек, масса: 400 кг, время возведения расчётом из 4 человек с отрывкой котлована ПЗМ-2 – 3-4 часа. Но в связи с распадом СССР сооружение не выпускалось и не поставлялось в войска.

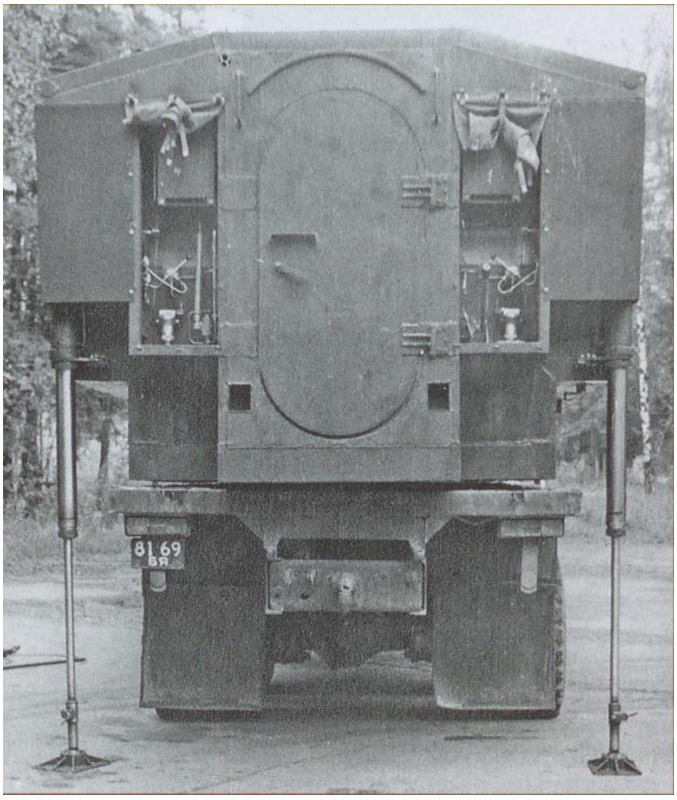
В начале 1980-х годов велось и создание съёмного защитного контейнера СЗК. Данное сооружение (по сути, аналог чехословацкого сооружения «ВЕСТА-Ц») представляло собой контейнер полигональной формы полной заводской готовности с встроенным оборудованием, системой жизнеобеспечения, гидравлической системой выглубления и мултилифтом для натаскивания на платформу базового автомобиля.

Для проведения всесторонних исследований изготовили модель СЗК, которая прошла испытания. Затем изготовили два варианта экспериментальных образцов сооружения СЗК – с гидравлической системой подъёма и без неё.



2. рис. Чехословацкое сооружение «ВЕСТА-Ц

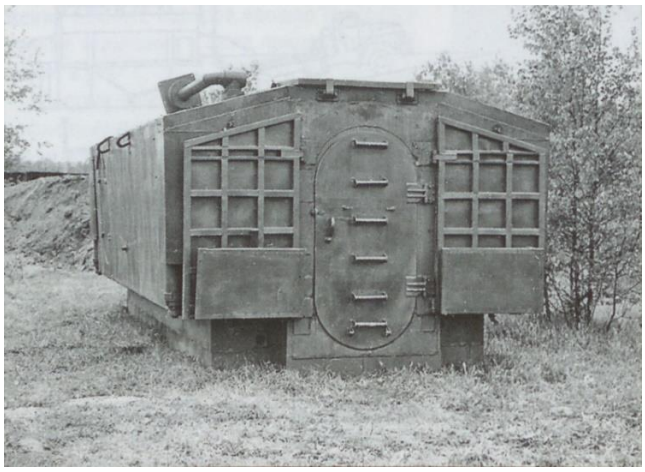
Оснавные характеристики: длина – 6 м, ширина – 3,15 м, высота – 2,3 м, полезня площадь – 14 м^2, вместимость – 10 человек, масса: до 6 т, время на возведение (извлечение) расчётом в составе 3 человек, экскаватора и крана – 1,5-2,0 (1,0) часа.



4. фото Сооружение СЗК с гидравлической системой подъёма[4]

Экспериментальное сооружение СЗК предназначалось для защиты, работы и отдыха оперативного состава на пунктах управления. Оно состояло из рабочего помещения и входа, конструктивно выполненного в виде остова с защитно- герметической дверью, двух тамбуров, расположенных внутри остова сооружения, и шарнирно прикрепленного к остову предтамбура. Допускалось стыковать такие сооружения друг с другом как в продольном, так и в поперечном направлениях. Экспериментальные образцы СЗК совместно с защищенной машиной «РЕДУТ» принимали участие в учениях, успешно демонстрировались на показах, но их постигла та же печальная участь.

[4] ВИА им. В. В. Куйбышева в Николо-Урюпино



5. фото Сооружение СЗК[5]

В 1988 году было подготовлено ТТЗ на разработку опытного модульного сооружения полной завадской готовности «ЛИФТЕР». Модульное фортификационное сооружение контейнерного типа «ЛИФТЕР» предназначалось для защиты, работы и отдыха личного состава на пунктах управления. «ЛИФТЕР», в отличие от сборно-разборных сооружений, представлял собой модуль полной заводской готовности. Оснавные характеристики: длина – 6,54 м, ширина – 2,4 м, высота – 2,4 м, полезня площадь – 10,6 м^2, вместимость – 8 человек, время на возведение расчётом в составе 3 человек с применение экскаватора и автокрана – 3,0 часа, транспортабельность на КамАЗ-53212 – один комплект.

Сооружение «ЛИФТЕР» состояло из рабочего помещения и входа, выполненного в виде остова с защитно- герметической дверью, двух тамбуров, расположенных внутри остова сооружения, и предтамбура, шарнирно прикрепленного к остову. Оно оборудовалось средствами отопления, вентиляции и освещения. В рабочем положении в нём размещалось бытовое оборудование для работы и отдыха личного состава. Извлечение сооружения из-под грунтовой обсыпки обеспечивалось традиционным способом – удалением с покрытия грунтовой обсыпки землеройным средством и удалением грунта из пазухи котлована по полупериметру контейнера.

Сооружение «ЛИФТЕР» прошло Государственные испытания и было принято на снабжение войск, но не выпускалось – началась перестройка.

ВМЕСТО ЗАКЛЮЧЕНИЯ

Прошло более 20 лет, как в армиях блока стран-участников НАТО появились и нашли своё место сооружения контейнерного типа. В СССР 1972. году создали перспективное быстроизвлекаемое сооружение контейнерного типа «ВЕСТА-Ц». При этом все новые наработки по техническим решениям эксперементальных и опытных быстроизвлекаемых сооружений, которые описаны высше, были защищены авторскими свидетельствами. В результате мы сегодня имеем только бумагу (чертежи, протоколы, акты), а также ржавые и заброшенные модели и образцы.

Новое время, новые технологии (нанотехнологии) и материалы, иозможности промышленной базы и передовые взгляды на фортификацию вписываются в стройную

[5] ВИА им. В. В. Куйбышева в Николо-Урюпино

систему Концепции обеспечения безопасности России, и перемены к лучшему в развитии ВФС для ПУ уже происходят.

ЛИТЕРАТУРА

[1] HORVÁTH T, PADÁNYI J: Műszaki eszközök a béketámogató műveletekben és a fejlesztés lehetőségei II. KATONAI LOGISZTIKA 15:(1) pp. 68-86. (2007)

[2] HORVÁTH T, PADÁNYI J: Műszaki eszközök a béketámogató műveletekben és a fejlesztés lehetőségei I. rész KATONAI LOGISZTIKA 2006:(4) pp. 96-130. (2006)

[3] HORVÁTH T: A személyi állomány védelmét biztosító erődítési építmények fejlődésének vizsgálata és a továbbfejlesztés lehetséges irányai. Doktori PhD értekezés; ZMNE, Budapest, 2003. 137 p.

[4] PADÁNYI J, HORVÁTH T: Úkoly zenistu pri budováni ochrannych staveb a provádeni stavební cinnosti v mirovych silách SBORNÍK VOJENSKÉ AKADEMIE V BRNE RADA B: TECHNICKE A PRIRODNI VEDY 1: pp. 103-110. (2001)

[5] HORVÁTH T: A védőképesség növelésének lehetőségei az erődítés-álcázás területén Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2000. 126 p.

[6] HORVÁTH T: Óvóhelyek tervezésének, méretezésének jogi alapjai NEMZETVÉDELMI EGYETEMI KÖZLEMÉNYEK 2. évf:(1) pp. 113-118. (1998)

[7] HORVÁTH T: A KFU óvóhely MŰSZAKI KATONAI KÖZLÖNY 7:(3) pp. 49-52. (1997)

[8] HORVÁTH T, WANCZEL G: Erődítési mintakert Csobánkán MŰSZAKI KATONAI KÖZLÖNY 6:(1) pp. 51-54. (1996)

[9] HORVÁTH T, WANCZEL G: Csapaterődítés Szentendre: Kossuth Lajos Katonai Főiskola, 1995. 44 p.

[10] Б. В. ВАРЕНЫШЕВ, К. Н. ДУБИНИН, И. П. МУДРАГЕЙ: Военно-инженерная подготовка. Воениздат, 1982.

[11] Е. С. КОЛИБЕРНОВ, В. И. КОРНЕВ, А. А. СОСКОВ: Инженерное обеспечение боя. Воениздат, 1984.

[12] Sz. A. ANANICS–P. K. BUZNYIK–A. I. SZUHAREV: Fortifikácia. Voennoe Izdatyelsztvo. ¹3/89735p. Moszkva, 1984.

A KATONAI VEZETÉSI PONTOK CSAPATERŐDÍTÉSI ÉPÍTMÉNYEI

Absztrakt

Az 1980-as évek elején folytatódott a munka gyorsan felépíthető és gyorsan bontható szerkezetek létrehozása a katonai (csapat) vezetési pontok számára. A jól ismert erődítményépítő hadmérnökkel, N. S. Mashtakoval folytatott beszélgetések során megvizsgálták a föld alatti szerkezetek kiemelésének, illetve vissza bontásának fő kérdéseit, problémakörét. Nyilvánvalóvá vált, hogy javítani kell a „PACKET" és a „BUNKER B" létesítmények hasznosítható blokkjainak vázát átalakító korábban elfogadott rendszereket.

Kulcsszavak: *vezetési pont, erődítési építmény, bunker*

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

FACTORS ENDANGERING HIGHLY PROTECTED SHELTERS AND THEIR PERSONNEL

A NAGY VÉDŐKÉPESSÉGŰ ÓVÓHELYEKET ÉS A BENNÜK TARTÓZKODÓKAT VESZÉLYEZTETŐ HATÁSOK

SZABÓ, Balázs

ORCID ID: 0000-0003-4860-6784

szabobalazs1980@gmail.com

Abstract

The determination of the requirements of designing, constructing and operating highly protected facilities may seem to be a simple task. But often, because of the possible impacts, it is difficult to determine them. Even the constructor cannot accurately specify the requirements and needs to the designers. It can be stated that this is a complicated and complex task requiring a high level of professional knowledge and experience. One needs to know the threatening impacts and the endangering factors in their entirety; they need to be aligned with the most unfavorable national defense policy expected in the long run, and one must be able to implement them. Knowing all this, one needs to determine the level of protection, so that risks can be minimized. These facilities should be integrated into the operational plans. Unfortunately, probability calculations are often not performed because of their complexity.

Keywords: *protected facility, specially fortified facility, endangering factors, risk factors, design requirements, protection capacity*

Absztrakt

Nagy védőképességű védett létesítmények tervezéséhez, kivitelezéséhez és üzemeltetéséhez a követelmények meghatározása egyszerű feladatnak tűnhet. De gyakran előfordul, hogy a nehezen meghatározható hatások miatt az építtető sem tudja pontosan megadni a követelményeket és az igényeket a tervezők számára. Kijelenthető, hogy bonyolult és komplex feladat, mely magas szintű szakmai tudást és tapasztalatot kíván. A veszélyeztető hatásokat és tényezőket maradéktalanul ismerni kell, össze kell hangolni a hosszútávon várható legkedvezőtlenebb nemzeti védelmi politikával és tudni kell azt alkalmazni. Ezek tudatában kell a védelmi szintet kialakítani. Így kockázatokat minimalizálni lehet. Ezeket az üzemeltetési tervekbe is be kell építeni. Sajnos a valószínűségi számításokat bonyolult voltuk miatt gyakran nem végzik el.

Kulcsszavak: *védett létesítmény, speciális erődítési létesítmény, veszélyeztető hatások, veszélyeztető tényezők, kockázati tényezők, tervezési követelmények, védőképesség*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.27.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.17.

ANTECEDENTS

Protected facilities are structures where, beyond ensuring physical protection and living conditions, also providing high-level working conditions and communication are basic tasks. [1] They have the functions, often separately or conjointly, of a command post and a shelter. They are built largely as state investments, so they fall within the scope of state fortification. They are also called as specially fortified facilities in the Hungarian terminology.[1] These facilities are generally shelters with physical protection capacity Class III according to the Hungarian classification[2] [3] [2; p.15.], but in special cases, they may have different protection capacities. The vast majority of the highly protected facilities[4] are located underground. They have significant advantages in camouflaging, especially in concealing (see at the end of this paper at the topic of camouflaging).

Such specially fortified facilities are located in many places in Hungary, the smaller part of which is still maintained by various state organizations. [3; pp.5-6.]

When designing such facilities it is difficult to determine to what effects they should be sized and prepared. It often happens that, due to the impacts that are difficult to determine, even the constructor cannot accurately specify the requirements and needs to the designers.

In Hungary, no required design requirement has ever been mandatory in relation to these facilities: designers used the no longer valid Technical Guidelines and other hard-to-access old recommendations for designing shelters.

In this paper, I have collected the factors that may jeopardize the specially fortified facilities, especially those that may affect Hungarian facilities. I have tried to present examples of all the factors and specific hazards, endangering the structures and the personnel inside. Along with the possible hazard sources, I have demonstrated some practical examples of specific incidents.

The appearance of the "Scalpel" operational theory and the continuous development of offensive weapons have further increased the demand that our fortified facilities our fortified facilities should ensure adequate protection, designed to an acceptable risk level, primarily for the personnel and the communication equipment, however, their implementation should stay in the framework of reasonable economy. [4]

RISK FACTORS AND THEIR GROUPING

Apart from the designers of specially fortified facilities people may easily have an impression that these facilities should only be sized against the impacts of a small number of offensive weapons. I have shown that the entirety of the jeopardizing impacts is much more complex. I have endeavored to collect the endangering impacts (and their real risks) with as much detail as possible. Knowing them, one can be prepared efficiently and economically against them.

[1] Terminology originating from the translation of Russian literature.

[2] Shelters are classified in five classes in the Principles of Engineering in Hungary as per the frontal pressure of the shock wave: Class I shelters must resist a value of 2.0 MPa, Class II shelters 1.0 MPa, Class III shelters 0.5 MPa, Class IV shelters 0.1 MPa and Class V shelters 0.03 MPa.

[3] In certain literatures, Class I shelters are to be designed to resist more than 1 MPa load without upper limit.

[4] In this paper, I call the facilities with high protection capacity, which, regarding their physical protection capacities, can be classified as Class III, and as far as their engineering systems, they are equipped not only with means capable of sheltering from the outside air, but also capable of regenerating air.

OFFENSIVE WEAPONS	**By type**	conventional
		nuclear
		special (e.g., generating electromagnetic impulse (EMI) or neutron weapon)
	By location of impact site	air
		ground
		underground
		underwater
	By location of launch site	remotely launched
		onsite external
		onsite internal
	By destructive impact	generating shock wave (and suction effect)
		generating electromagnetic impulse
		generating light and/or heat
		generating radiation
		generating toxic gases
		aerosol (generating incendiary or explosive gases)
		Contact-destroying impact
HUMAN FACTORS	defining incorrect and incomplete criteria	
	incorrect and wrong design	
	incorrect and wrong construction	
	unskillfulness and inability of operating personnel	
	unauthorized physical intrusion (organized attack of combatant units or accidental intrusion by an alien or the appearance of the fleeing civilian population or terrorist attack)	
	revenge, sabotage	
	bribery, industrial espionage, extortion	
	disregarding confidentiality, releasing critical information, missing encryption and required rules, non-compliance thereof	
	violation of rules and indiscipline	
	unauthorized intrusion into the control system	
	lack of documentation for the operation	
	improper or poor maintenance	
	psychic exhaustion of the personnel inside	
LACK OF LIVING CONDITIONS	lack of oxygen (enrichment of carbon dioxide)	
	lack of water	
	lack of food	
	lack of fuel	
	overheating	
	lack of healthcare conditions (e.g., lack of medical care, instruments, medicine, disinfectant)	
NATURAL IMPACTS	earthquake	
	flood, tsunami	
	lightning	
	wild fire	
	geological and hydrogeological changes	
OTHER IMPACTS	industrial or chemical disaster	

	operational disruption
	internal fire
	internal explosion (e.g., an equipment or machine)
	ever accelerating technical development
	lack of camouflaging (concealment, pretense, deception, demonstration)
	changes in the national defense policy and the willingness of the current government to allocate financial means
	lack of external and/or internal communication

Figure 1: Summary of endangering factors in a table format [5]

DETAILED DEMONSTRATION AND ANALYSIS OF RISK FACTORS

Grouping of offensive weapons by type

Conventional offensive weapons contain explosives, which, during explosion, are transformed into gases, so that their volume grows to multifold in a short time, thus they perform work. The high temperature and pressure gas, located concentrated, suddenly begins to expand. This creates a shock wave in the ambient medium (later, a minor intensity suction effect). [6] Although the temporal feature differs from the thrust wave to the shock wave created by an atomic bomb, they are just as dangerous as the latter. From the magnitude of the warhead (TNT equivalent mass)[5], calculating from the energy released, the value of the pressure on the dimensional structures of the facility to be fortified can be defined. Conventional weapons, even though they are still used nowadays in great numbers, yet they cannot produce the greatest impact, but nuclear weapons.

Nuclear weapons appeared in 1945. Their destructive power is much greater than that of conventional offensive weapons. Their shock wave effect on the specially fortified facilities is similar to those of conventional weapons, but they also have other, high intensity effects. In the case of aerial or ground explosion, as far as the order of their arrival, electromagnetic impulse is the first of the effects on the facility to be protected. The following are light and heat radiation. The third one is the thrust wave, the next one is the initial, then the secondary radiation. (In the case of underground explosion, there is a significant difference between them and some of the effects will be lost.) In a very short period (practically zero time), a large amount of energy is released that warms up suddenly the surrounding medium and the high temperature materials; during their thermal expansion, they produce a similar shock wave as conventional weapons.

[5] TNT equivalent is a data compared to the amount of energy released at the explosion of 1 kg of trinitrotoluene explosive.

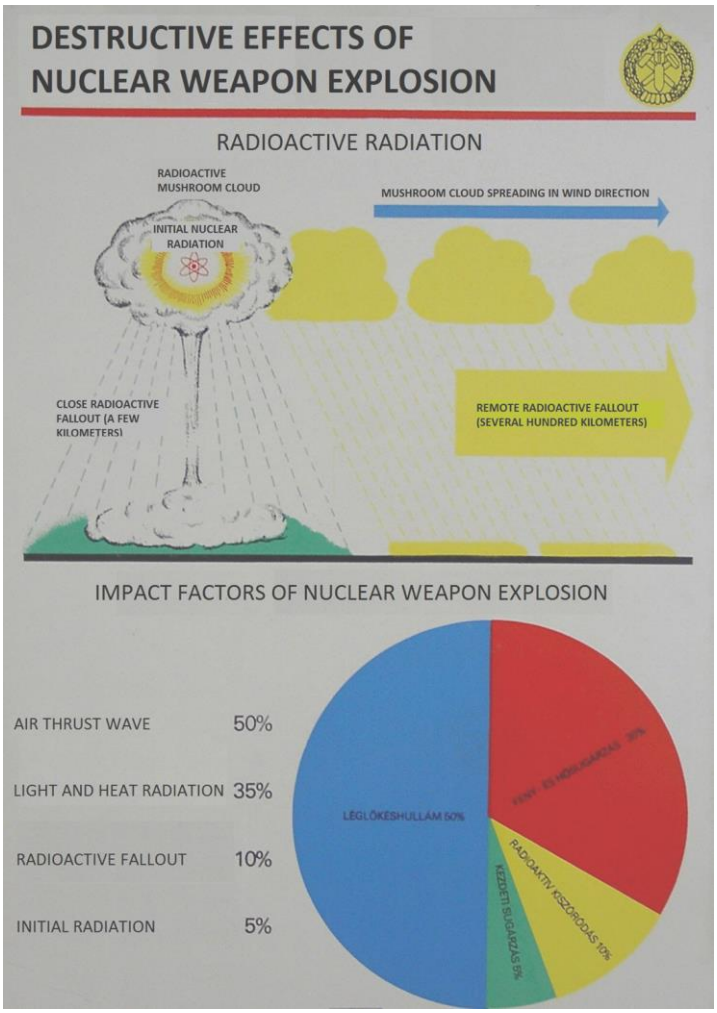


Figure 2: Destructive effects of a nuclear weapon explosion [7]

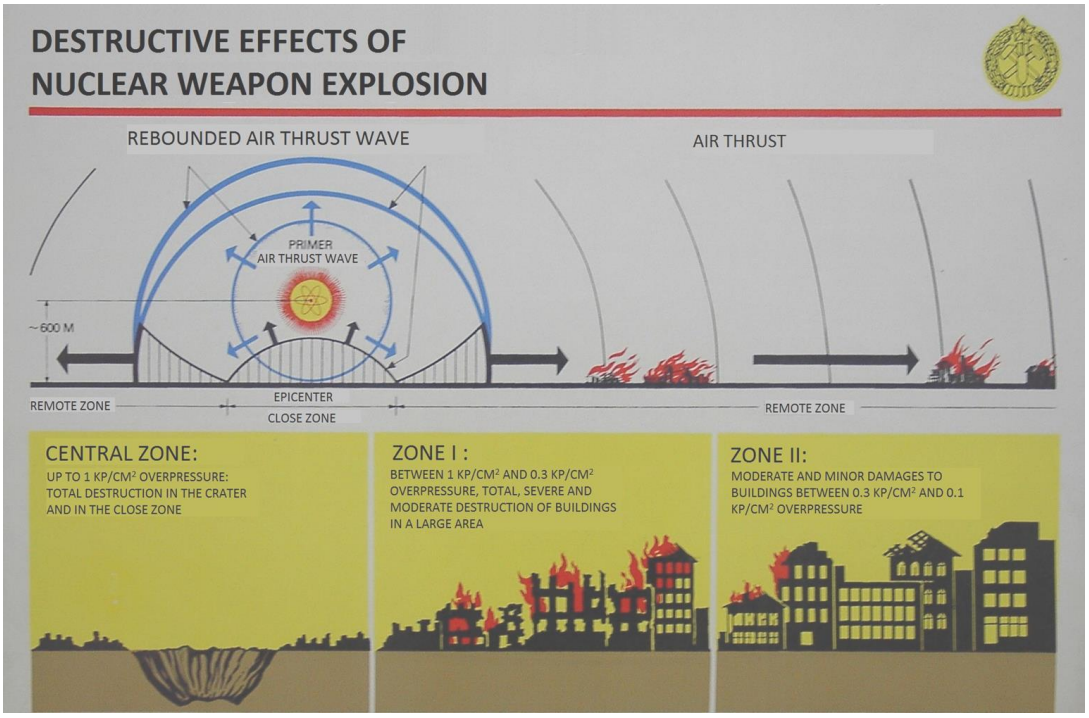


Figure 3: Destructive effects of a nuclear weapon explosion [7]

Here, too, there is a suction effect with a lower intensity and occurring later during the shock wave that occurs at the return of displaced fluid to its original (or nearly original) place. The radiation is very harmful to the organism, so, it has to be protected against it. Electromagnetic impulse (EMI) protection is inevitably necessary for electrical current in the instruments and devices, since without it, the effect may be fatal. Electrical devices must be protected even when they are off (current-free) as they are caused by EMI, high voltage is generated and they are deteriorated. Besides these weapons, nowadays, there are a number of other special weapons.

Special offensive weapons strengthen or amplify the secondary effects observed at other weapons. Such is EMI. A similar one is the neutron weapon, but with them, very detrimental effects are witnessed in organisms. It ionizes water molecules with which the cells constituting the human body are no longer capable of biological functions.

Grouping of offensive weapons by the location of impact

In the event of an *aerial explosion*, the explosion occurs at an altitude of over 300 meters above the surface. The shockwave is spread in the air (gas), then some of it passes to the solid surface and the other part is reflected. Underground protected facilities are endangered by air pressure (shock waves) generated by surface connections, as well as by induced shock waves spreading in the solid, infinite half-space[6] as well. The explosion may also occur lower which is called a surface explosion.

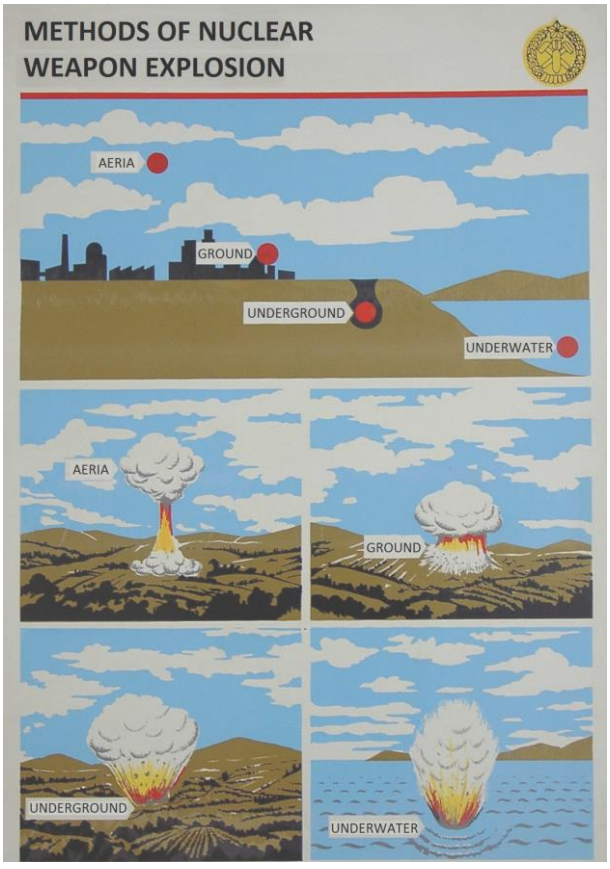


Figure 4: Modes of nuclear weapon explosion by location [7]

[6] The infinite solid half-space is the ground mass under the surface, above which air (and not soil) is located.

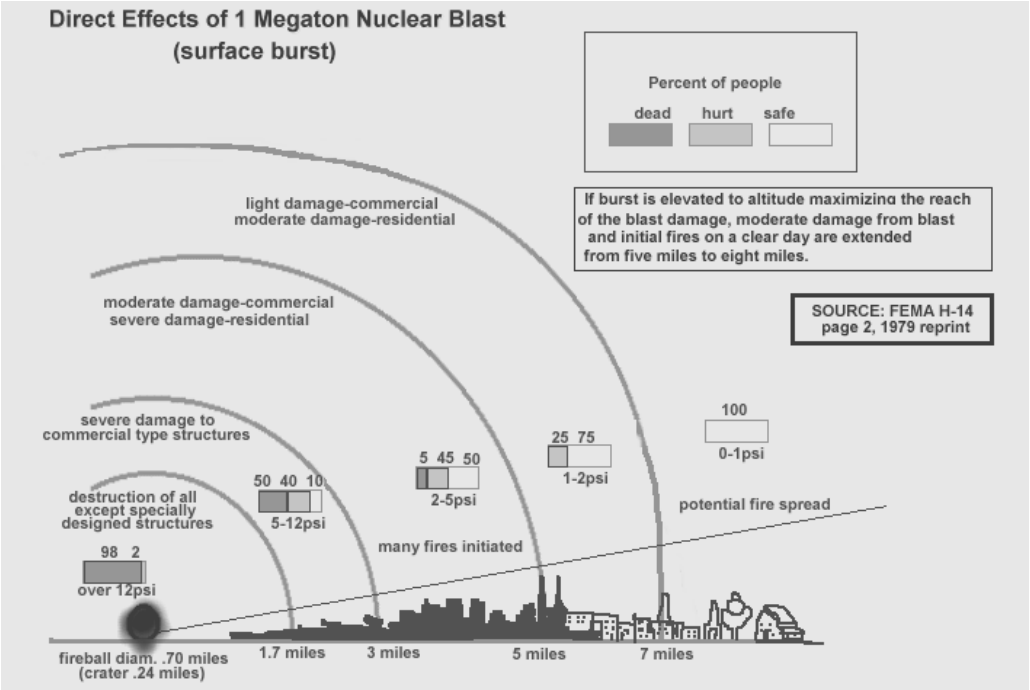


Figure 5: Immediate impacts of the surface explosion of a 1-megaton nuclear bomb [8]

In the case of *ground explosion*, the explosion occurs at a maximum height of 300 meters from the surface. The pressure wave is spread in the air (gas), then some of it passes to the solid surface and the other part is reflected back. Underground protected facilities are endangered by air pressure (shock waves) arising at surface connections, or shock waves induced and spreading in the solid, infinite half-space. This causes less physical impact than the aerial and underground explosions. The explosion can occur even lower.

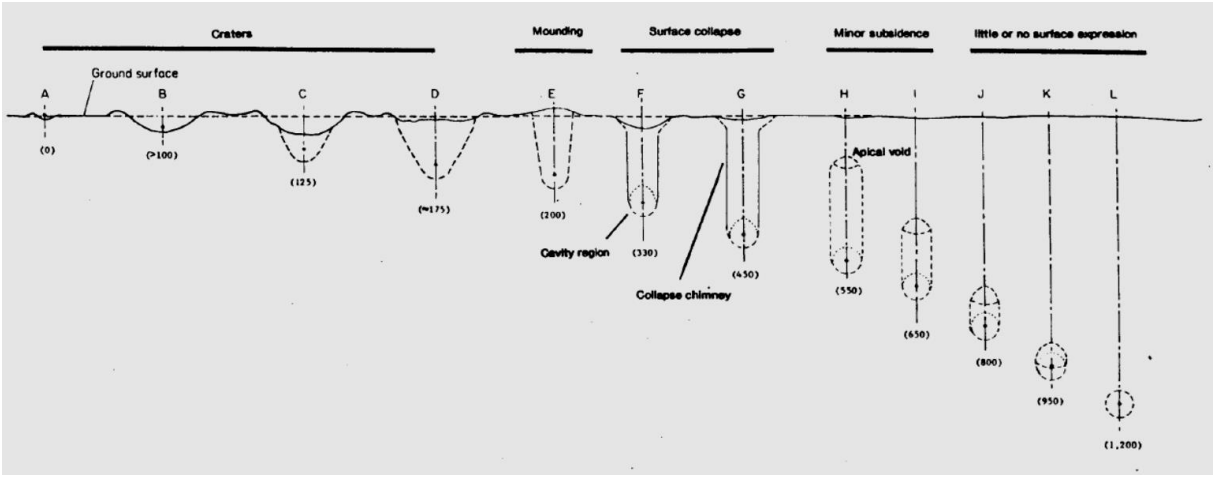


Figure 6: Crater formation depending on the burial depth in solid rock in the Nevada Test Area [9]

In case of *underground explosions*, as it is called, there is a detonation point (hypocentrum) located beneath the surface. It is usually possible that the carrier delivers the offensive weapon under the ground. Such devices have been in place for a long time and are able to penetrate even to a great depth. The near-surface explosion of high-load charges takes place partially suppressed, therefore, rejection and fallback occur. If the explosion happens deep, the rejection is complete and sinking and a crater is formed on the surface. If it occurs at very low depths, a lasting effect will not be visible on the surface. The effect on underground objects is very

dangerous despite the fact that in solids (soils) damping is relatively high but the detonation point may fall close to the facility. In some cases, the medium may behave as a non-solid (or liquid).

Offensive weapons, coming close to the protected facility at a vertical impact angle and then trying to penetrate into the ground under an oblique angle below the facility and create a delayed explosion are particularly dangerous. [5]

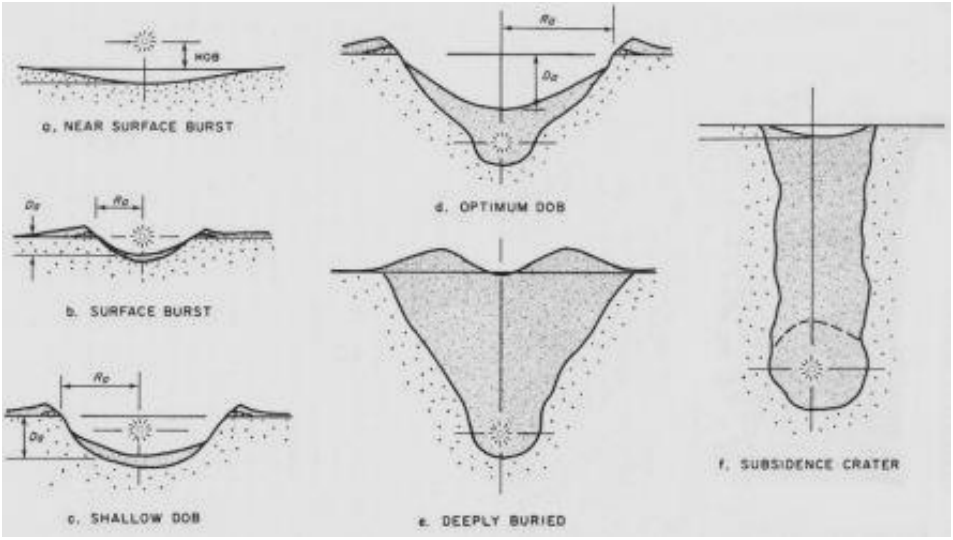


Figure 7: Crater formation depending on the position of the explosion [9]

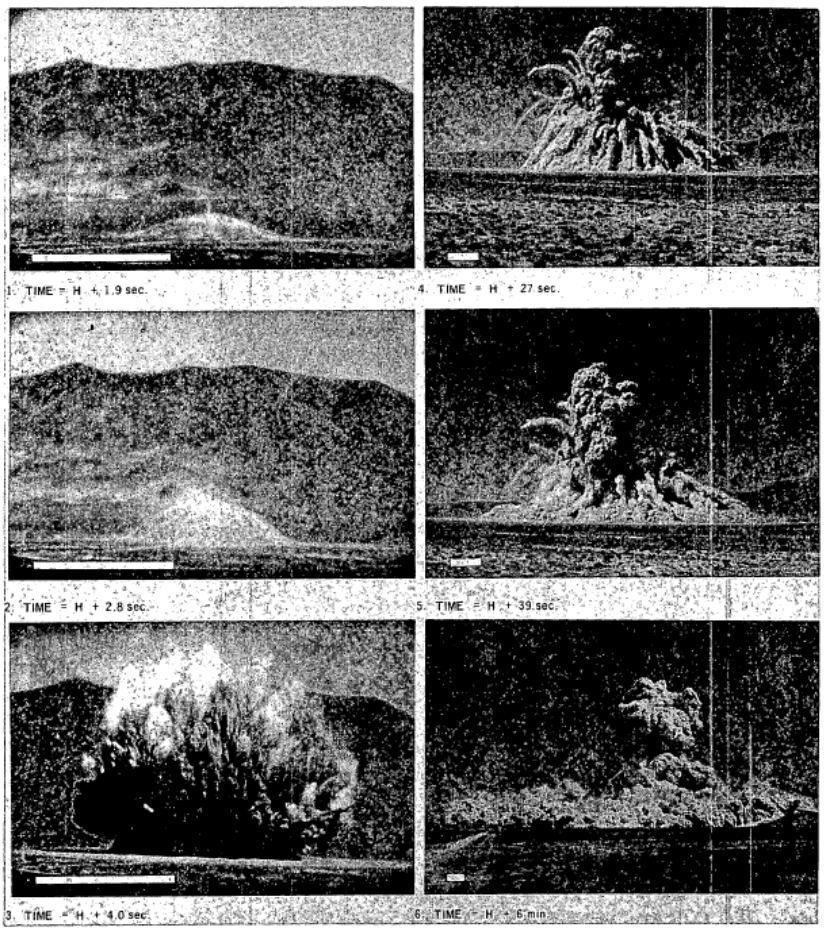


Figure 8: Pictures of the Sedan atomic bomb (104 kt) at the time of the explosion near the surface [10; p.10.]

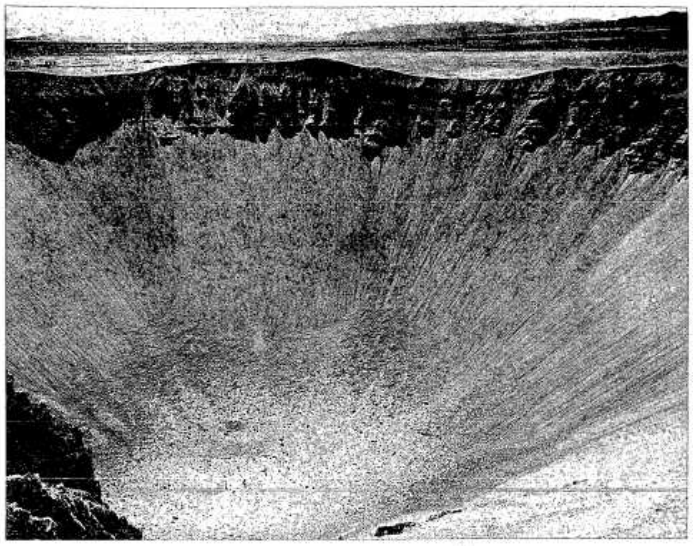


Figure 9: A crater with a 384-meter diameter and 100-meter depth on the Nevada Test Area created by the Sedan atomic bomb (104 kt) at an explosion near the surface [10; p.22.]

Explosions can take place even *underwater*, but since such facilities are not built underwater, I will not go into details in this article.

Grouping of offensive weapons by the location of launch site

Remote launching today is the most used delivery method against specially fortified facilities. Accordingly, it is common to see that its accuracy is also very high. 1-meter accuracy is not uncommon in the warfare of developed nations.[7]. They are quite dangerous, as they can be effectively used for attacking surface facilities of the enemy. Furthermore, the delivery means of so called bunker-destroying bombs that penetrate into a great depth also belong to these types. Due to technologies, only a handful of developed nations possess them, where the money needed for their development is available. Depending on their launch position, the weapons may be close launched ones.

Onsite weapons externally launched but with internal impact are offensive weapons launched from a medium distance (in visibility). Their magnitude is generally smaller than that of remote ones, but there may be exceptions, for example, if a facility is built near a coastline, it can be a warship's guns[8] or weapons more accurate at smaller distances, or when long-range weapons cannot reach their targets because of terrain obstacles. These weapons may, in some cases, be internal launched weapon[9] as well.

Onsite weapons internally launched may be the most dangerous ones in some cases, as we face an internal explosion. A great destructive effect can be achieved with them. At this time, the intruding or input charge launched from a distance will cause an internal explosion. Generally, it involves large-scale damage, blockage of escape routes, smoke and fire. These cases originate from the so-called asymmetric warfare, instead of symmetrical warfare, and pose a problem to the safety of protected facilities.

Grouping of offensive weapons by their destructive effects

The supporting structure designer should design the protected facilities against *offensive weapons creating shock wave (and suction effect)* against a support structure. During the

[7] For instance, the TOMAHAWK guided missile system in service at US Army.

[8] For instance, in the case of a facility in Yemen, designed and constructed by Hungarian engineers and constructors, respectively, which was attached quite soon after the handover

[9] An internally launched weapon, delivered into the building and exploding there.

detonation, very large front-pressure waves arise (deformation thrust at obstacles) in the surrounding environment. The delimiting structures of facilities are generated by tensions, to which they must respond. After the pressure wave, also a so-called suction effect can take place, with a lower intensity than the former. In addition to the shock wave, other special effects may also occur.

Figure 10: Impacts caused by explosion [6]

Weapons generating electromagnetic impulse (EMI) amplify the targeted electromagnetic radiation of nuclear weapons. Every advanced army lays a great emphasis on its development. They do not pose a threat to living organisms, but they permanently ruin electrical devices. [3; pp. 82-86.] The most effective protection is the protective layer or the Faraday cage against them.[10] This can be tackled by special means (e.g. by sparking).[11] [1]The point is that they are capable of detecting very high (even greater than solar) intensity light emitted by a device and then creating an electrically-free, so-called, zero mode in the entire facility. If this is not available, full sheltering must be used for protection and, at the same time, with adequate protective layers. There are types of weapons that are also dangerous to living organisms.

Nowadays, *weapons emitting toxic gases*, including asymmetric warfare, can be one of the most effective tools against specially fortified facilities. Weapons that emit colorless, odorless poisonous gases placed at external surface contact points (such as air intakes) can pose a significant risk. If the system does not detect and the filters for not performing their task, it may be fatal to those inside. This weapon can be produced in a simple way, at a low cost. The most dangerous are the colorless, odorless gases.

Aerosol weapons (releasing igniting and explosive gases) can be produced at a low cost, just as easily and quickly as toxic gases. They can also be delivered at the surface contact points. They pose a similarly high risk to those inside as toxic gases. Of course, in general, they are also colorless and odorless. By forming a suitable explosive mixture with air, being igniting, the can result in complete internal destruction. The most effective protection against them is the so-called sparking. At the air intake points, after detection (or continuously) sparking must be carried out, which, before suction, ignites and combusts such mixtures. Weapons that emit such gases can endanger not only living organisms, but the built-in instruments or devices and machines inside them.

The group of *contact destructive weapons* include weapons that can effectively destroy a local target. Specially fortified facilities always have external, surface appearances and structures. They can be effectively attacked with contact destructive weapons. They may be delivered in several ways.

[10] Faraday cage: Part of space surrounded by a metallic mesh to eliminate the electromagnetic effect, into which the outer electric force field does not penetrate ("shielding") due to the protective effect of the mesh. This can explain, for example, that in buildings made of reinforced concrete structure, there is usually no field intensity for mobile phones to function.

[11] Based the verbal comments by Dr. Horváth, Tibor.

Human factors

One of the most common issues that emerge from the first steps in design is the *definition of an incorrect, incomplete system of requirements*. Unfortunately, in Hungary as well, it often happened that the investor was unable to provide adequate data. Many people do not even think, but even during the design of a specially fortified facility, the criteria set by an investor or by professionals commissioned by it, generally, should contain quite a complex set of information, deliberation and probability calculation. If they are determined incorrectly by the designer, the facility may not provide adequate protection against certain effects. Conversely, the construction and the operation of a facility will be uneconomical. The problem is not simple, because the offensive weapons of the future have to be ascertained, their nature, duration and the effects of an attack should be forecast. Unfortunately, in Hungary as well, it often happens that an investor is unable to provide adequate data. There is a common case that, incorrectly, risks are only investigated at the time of construction and not for the duration of expected lifetime. Additional conditions are required to create facilities.

The professional and high-level design of these facilities can only be carried out by highly trained engineers with special knowledge.[12] In summary, if it is missing, it is called *incorrect and wrong design*. For example, details, seemingly small, should be taken into account by the designer like the proper attachment of fixtures. If this does not happen, the shock wave on the facility may cause acceleration to these objects, which, during their displacement, may cause even mass casualties or serious injuries to the personnel inside. For example, a raised floor designed and constructed in some of the premises of the Air Command and Control Center of the Hungarian Defense Forces (HDF) in Veszprém. Its short but dense pillars, in case of a shock wave, may cause serious injury to the persons inside as a result of tripping. Today, designing or transforming, modernizing a new protected facility would be a serious concern, as professionals with such experience have already retired or died. There has not been any training of designers of these special impacts for decades in Hungary. In addition to designing, implementation can entail risks as well.

Incorrect and wrong construction can also be a risk factor. Although the technical solutions of these facilities have been implemented and checked by technical inspectors according to much stricter rules than the average. Still, some solutions were made to different (lower) standards, for example, due to the incorrect selection of materials and technology. They can be such that have only become known during construction, or others that may cause issues in the long run. To maintain these facilities, regulations and procedures different from the conventional ones are required.

[12] See the designer team of such facilities built in the past: for example, a former designer team of the Road and Railways Designing Office (UVATERV), designer company, which designed a part of the Hungarian facilities, including the reconstruction of the KAGRA facility under the Buda Castle, or the specially qualified engineers of the HDF Building Designer Institute (ÉPTI Kft.).

Figure 11: Tunnel lining wall incorrectly constructed (and consequently, deteriorated insulation) in a KAGRA (Kamioka Gravitational Wave Detector) facility in Budapest[13]

In specially fortified facilities, quite complex and complicated mechanical systems operate. Therefore, the *lack of qualifications and the inability of the operating personnel* are unacceptable either. Maintenance workers and operator specialists, used to normal buildings, are not able to operate such facilities. Generally, this job requires the learning of special methods and time. In theory, appropriate specialists should be selected to perform these tasks, which used to happen earlier in Hungary. (Typically and intelligibly, reliability was very important in these jobs.)[14] The task of the operating personnel is to maintain the facility and assets contained therein, to provide its operability and to carry out planned preventive maintenance. If an operator cannot make decisions quickly and efficiently, it can seriously jeopardize the personnel inside and even the entire building. A no longer classified facility in Budapest today is a good example; a small electric fire broke out, to lead away the large smoke generated from which, a member of the operating personnel made a wrong decision and opened a wrong shut-off door, and thus circulated the smoke back, creating an even worse situation for the staff inside.[15] Regular retraining and national security vetting of the operational personnel are also required.

The access control in these facilities is quite strict, done under highly classified rules, therefore, *unauthorized physical intrusion* should be prevented in any case. This group includes organized attack of combatant units, accidental intrusion by an alien, the appearance of the fleeing civilian population or terrorist attack. In these facilities, during access control, after the preliminary check, the identity of a person is checked; the number and type of objects to be taken inside is restricted, otherwise, in case of an unauthorized intrusion, the operators and the personnel inside would be severely endangered. Although it is usually difficult to implement at such facilities, it still has great dangers. There are several facilities in Europe, which, due to their location in great depths would be difficult to threaten efficiently with offensive weapons, however, after intruding, significant damage could be caused to them. Thus, an installation can be easily made fully non-operational. To be able to intrude, of course, its location, design and physical parameters of the facility, of course, should be well known, that means intelligence

[13] Photo by the author in 2015.

[14] Based on stories told by the operational personnel of some of such facilities still operating.

[15] Verbal comments by Steyer, Ferenc on the events at the shelter at Budapest, Uri utca 72. (former National and Budapest Load Distribution Center).

should work at a high level. Because people's minds and actions are sometimes difficult to calculate, efforts must be made to prepare for the following threatening effects. This risk factor can be avoided by the professional design of external protection defense lines. Generally, they are physical obstacles, monitoring, warning and alert systems or the combination thereof. [11; pp. 67-71.]

Though quite rare, *revenge and sabotage* are also possible risk factors. It is the entirety of acts in the case of the detriment of one or several people that may lead to an act threatening the safety and security of the facility. Though quite rare, revenge and sabotage are also potential risk factors. It is the entirety of acts in the case of the detriment of one or more people who may lead to an act threatening the safety and security of the facility. It may happen by disclosing information or in damaging. Sabotage differs from revenge to an extent that it does not usually occur because of its own detriment, but due to external effect (intimidation, political motivation). It is so rare that it has records in Hungary, although the perpetrator would have had to face serious sanctions.

Bribery, industrial espionage and extortion are similar to the above, but there is an external motivation for influence or financial support. This is also a small risk factor due to vetted persons. However, there were several examples of industrial espionage already in Hungary. There was an event when the chief mechanical engineer of a large designing institute defected Hungary and revealed the parameters of a very important facility to the host country's counter intelligence.[16] In order to avoid such and similar cases, only people with security vetting were admitted to the specially fortified facilities in Hungary, monitored and for more than half a year. With them, such risk factors could be minimized.

In Hungary (contrary to the practice of some other nations), during all political regimes, there was a common position that specially fortified facilities should be protected by classifying them. The main reason for this comes from their function. In addition, one of the goals is to completely hide the data before the enemy, or in peacetime and in special legal order, to avoid the significant exhaustion of the physical personnel in keeping the population away from the facility. (A note by the author, if there were enough shelter capacity in Hungary, such a risk would not emerge.) As a result of reconnaissance and gathering intelligence by other nations, due to frequent superficial confidentiality initiatives, they are quite aware of such facilities. One good example is that, in Hungary, the British intelligence had reliable and detailed information on the so-called P50 facility (named KAGRA today), significantly upgraded and reconstructed in 1951 and 1952, already during its construction. Their findings were released during the Hungarian night program of the BBC Radio broadcast in Hungary.[17] Therefore, secrecy and encryption should have priority and considerable attention. Another typical example is the defectors, who were found by alien intelligence agencies and much information was gathered from them. A good example is the defection of the already mentioned chief engineer György Straub from UVATERV in 1966, where, besides many others, the largest and most secure facilities were designed.[18] In addition, civil servant Kálmán Mészáros, defected in 1979, who, as a driver, knew about a Budapest facility. Counterintelligence service collected operational data on him that allegedly had been contacted by the US intelligence agencies and then he revealed all the data he knew. [12]

A facility, on which foreign services have little information is very rare, so, the exact location of the facility was almost always and is quite well known. It is common that these facilities, due to cost reduction, utilize and expand already existing facilities. For example, the location

[16] Verbal comments by engineer Dr. Müller, Miklós (BME, Department of Geotechnology), also confirmed by historian Ungváry, Krisztián in connection with one of the former chief designer engineer of designer company UVATERV.

[17] Based on the notes taken during the enlargement of the then Facility P50 under the Buda Castle. (Stored and safeguarded: KAGRA design storage room T3f1)

[18] Verbal information by engineer Dr. Müller, Miklós (BME)

of the largest protected command post of the Federal Republic of Germany (FRG) was known by the Soviet Union, since the precise list of underground facilities of the Third Reich is complete, with the exact site locations being available to them. Since the protected command and control center of FRG was built utilizing and expanding such a facility, the enemy was able to locate it all the way. [13] There are some countries (mostly Scandinavian countries) where the location of protected facilities and even other important data are openly accessible to anyone. In these countries, due to the local culture and based on the large number of residential shelters, it is understandable. Classification before World War II, during the Horthy period, was merely the vetting and control of designers, construction contractors and workers and by having to sign a declaration. During the Cold War, this was taken much more seriously. At this time, design of such facilities took place in confined spaces within closed offices. The participants would work in intimidation and under pressure. In the post-communist regime period, not even the specialists knew how to deal with this information: new legislation was waiting to be adopted for a long time. Nowadays, several facilities have already been declassified. Knowing the past, this was wrong, as they still are likely to be needed. If needed to build new ones, neither time nor resources could not be ensured, because to design and construct them would take considerable time and/or money. A decision should be made now and not when it would be too late. This can be ensured through the correct national security policy.

Figure 12: The construction of the largest protected command post of the Federal Republic of Germany in the 1970s [14]

Although it is not typical and represents a low level of risk compared to others, it is worth mentioning *violation of rules and indiscipline*. Operational personnel working in specially fortified facilities have strict operational safety and protection regulations. In some cases (mainly in the deployment period), their violation may entail risks. For example, failure to perform planned preventive maintenance (TMK), the commissioning of certain machines and devices can be questioned. For example, inappropriate handling of radioactive materials kept for chemical protection devices can cause significant health problems.

Unauthorized intrusion into the control system is perhaps less threatening. It happens from the fact that facilities still operating in Hungary are outdated at a level that their control systems, even if they wanted to, could not be linked up to the system's external security telemonitoring system (e.g., the Internet). Another reason that *unauthorized remote cyber intrusion* does not represent a risk, is because the facilities are provided with independent internal building operational management. However, some of the cyber attacks do not require internet connectivity, and malicious codes can be transmitted with the help of an intermediary system -

consciously or negligently, the electronic environment serving operation becomes vulnerable as well. This attack may target the microcoding of the internal control of some systems and devices (firmware). The exposure of facilities to cyber attack is not necessarily based on the existence of the most up-to-date computing devices.

Today, there is a basic requirement for a building operational management and control system to be complex, "intelligent" and independent. It could be a serious threat to a new facility if there were a living external relationship with the outside world. In case a professional hacker intrudes, they can take your entire system under control, or cause serious damages deliberately. If such a facility were upgraded, the building operations management system should not be connected to external communication, and one should set up protection against an internal attack.

The *lack of documentation for the operation* is a non-typical error source. Deficiencies in the documentation that are described in detail in the documentation for the operators are revealed over time and need to be replaced. They can be bridged with improvisation by appropriate operating engineers and specialists. In the long term, improvement and supplementation may take place. It poses a risk if the facility is forced into a live operation immediately after its handover and there is no experience and time required for operation. nfortunately, in Hungary, after a rapid construction of such facilities, frequent belated decisions on the construction occurred in great numbers.[19]

In today's environment in Hungary, one of the risk factors inherent in most of the dangers is *improper or poor maintenance*. Among our facilities, especially during World War II and the Cold War, the danger of closing most of them had been raised already. In most cases, they do not have a function. That is why the political leadership treats them as a “stepchild”. Sometimes they see ideology in an old system, though this is a misconception, since all democratic nations had built similar ones as well. There are no resources to maintain (and renovate) them. The main reason is that financial expenditures will not be visible and, therefore, cannot be used for campaign goals. Because their professional closure that would comfort the environment protection experts, would generally absorb much larger amounts of money than their many decades of operation, they are maintained at a basic level.[20] The closure of one of the high-security facilities a few years ago in Hungary would have cost as much as its operation, on the present very low technical level, for approx. 300 years. Of course, this would be a time, besides desirable operation and maintenance, "only" approx. 30 years. Not even mentioning the fact that the amounts invested so far and the existing asset value would be lost for the nation at termination. It is clear that closure is not profitable. Even in this case, its good security policy of a nation would be decisive.

Underground protected facilities, for obvious reasons, can only provide a very confined living space for the personnel inside, especially after longer stays, the *psychic exhaustion and disruption of the staff inside* may happen even in large numbers. Though its appearance and treatment can significantly be extended today with medication, it still has a major source of danger, since the recognition and handling of perpetrators as dangerous individuals is complicated. Even before the problem is detected, it can trigger an action (for example, the unauthorized opening of a shutoff door) that could endanger the lives of the entire staff inside.

[19] For instance, the World War II period, when they was not enough time to complete some facilities like in the Buda Castle.

[20] For instance, based on the cost estimation of the proper occlusion of the largest highly protected facility in Hungary.

Figure 13: Protective door corroded due to the absence of maintenance in the KAGRA facility[21]

Living conditions

In specially fortified facilities, a basic requirement is that one should be able to shelter from the outside world for a shorter or longer time. The basic living conditions must be ensured for those inside. For humans, the condition "consumed" in the largest quantities and thus diminishing generally in the shortest time is air (mainly the oxygen within it). Therefore, one of the most serious risk factors is the *lack of adequate oxygen*. Under 16.25% of the oxygen content of the air, significant fatigue and the risk of fainting prevails, while at 14%, life is at risk. Filters, ventilation and air conditioning equipment and oxygen reserves can ensure these facilities the required air supply and composition. The systems must be equipped with carbon dioxide absorbers as well. In one facility in Hungary, during a deployment exercise, the oxygen content of the air decreased to a value that one could not even light a match.

Figure 14: Oxygen bottles in an ex KAGRA command post[22]

[21] Photo by the author in 2015.
[22] Photo by the author in 2011.

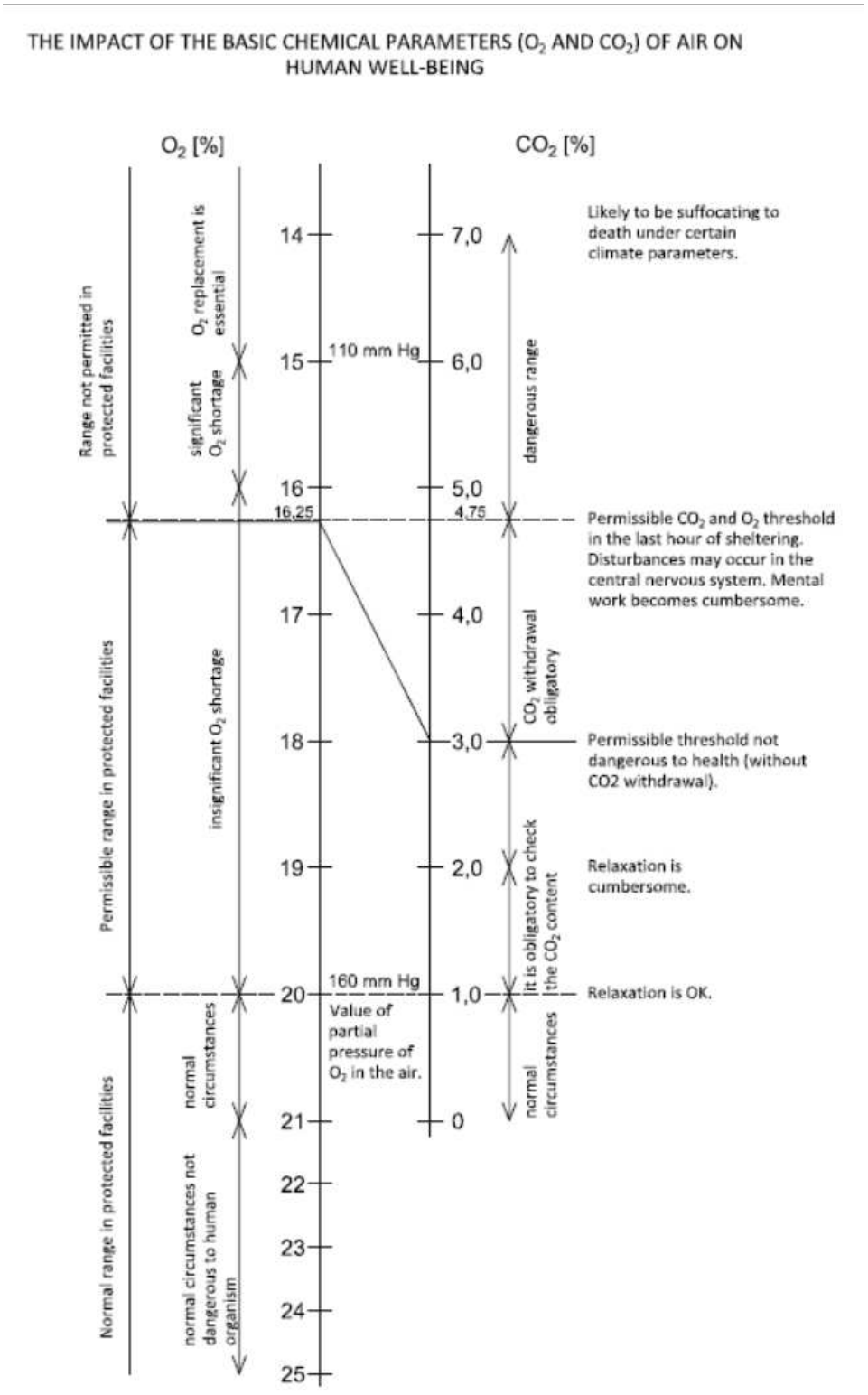


Figure 15: The effect of the content of oxygen and carbon dioxide of the air on the well-being of humans[23]

For humans, after air, drinking water is the most necessary living precondition. So, the next life condition risk factor is the lack of drinking water. Generally, survival time due to the lack of drinking water can be measured in days. In such facilities, water is not only needed for drinking, cooking or washing (including the operation of WCs), but also to operate machines

[23] Made by the author based on the document received from the operators of the KAGRA facility. A credit goes to them.

and equipment. Not even mentioning the water supply of medical points (or hospital detachments).[24] Several machines cannot operate for extended periods of time without cooling water. Generally, refrigerators and air conditioners also require a large amount of industrial water. As a result, in facilities with higher protection capacity, own water sources are at hand or they large enclosed and protected reservoir.[25]

Figure 16: Reinforced concrete drinking water container in the Hospital in the Rock in Budapest[26]

An obvious condition to be provided to humans is *food* in facilities suitable for long-term stay. In World War II, at numerous shelters, masses (mainly infants, babies) died of starvation not due to other effects but simply because of the lack of food. In these facilities, there is a need to accumulate long shelf life foods in larger quantities.

Specially fortified facilities, in any case, have at least two independent (one main and one backup) power supplies. Generally, the primary one is the external power supply, while the backup source is the internal power supply that is ensured, for simplicity, usually with diesel power generators. Without energy, the most basic systems (for example), ventilation systems would not be operational. Therefore, the *lack of fuel* can cause serious disruption. During World War II, the Capital's Surgical Hospital (nowadays called Hospital in the Rock) under the Buda Castle, due to the lack of a backup power generator (diesel) induced a very serious situation. Out of the two built-in machinery groups, one was taken away by the intruding Soviet troops. With this, the hospital could not satisfy its most basic needs and the quality of overheated internal air quickly became critical.

Since power generators are able to operate exclusively with fuel (and lubricating oil), they need to be looked after. Fuel (diesel oil) is generally provided from storage units in a protected location for different time periods.

[24] In WW II, in the Capital's Surgical Emergency Hospital, under the Buda Castle, nowadays called the Hospital in the Rock), lack of water created a serious situation. There was not enough of it even for drinking, not to mention other basic tasks. Therefore, a hydrological engineering building and a long pipeline was constructed during the cold war at one of the Danube bank water outtake plant.

[25] For instance, in the KAGRA F-4 facility and in the Hospital in the Rock.

[26] Photo by the author in 2003.

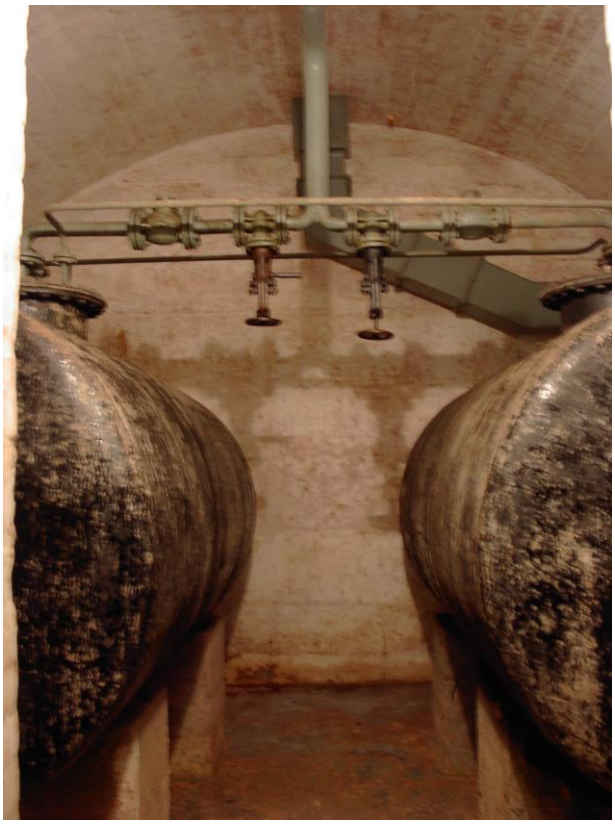


Figure 17: Fuel tanks in the Hospital in the Rock in Budapest[27]

Figure 18: Power generator in the Budapest metro line [15]

From the aspect of operation, one of the most critical issues is *overheating*. For most facilities, there is a significant problem despite the fact that in Hungary, a constant temperature (about 11°C) around the annual mean temperature can be measured. In the case of specially fortified facilities operating for a long time, or previously equipped with heating, a heat shield (heat coat) has formed in the rock environment from internal waste heat over the decades, which kept the indoor temperature of the facilities at very high. So, after the deployment, the internal temperature may rise rapidly to the permissible and tolerable level. This caused serious

[27] Photo by the author in 2003.

problems for several facilities. One of them was at a government shelter[28] and nowadays, in metro line M3 in Budapest, it is a considerable problem[29]. There can be an effective protection that in the maintenance (pre-deployment) period special care is dedicated in these facilities to keep the internal temperature below 16-18°C if possible. This can be ensured by switching off the internal consumers and/or with constant cooling.

Since protected facilities are generally in use in non-peacetime, the likelihood is great that non-healthy (injured, wounded) personnel would use them. Adequate *healthcare conditions* are to be ensured for the personnel inside. For example, the lack of medical care, medical instruments, medicine, disinfectants can develop a serious internal situation. For example, a simple influenza rapidly spreading in such enclosed spaces can paralyze the entire operation of the facility. It is imperative to form a hermetic separator room. Additionally, it is important to address the issues of temporary storage and handling, dispatch of biological contaminants and corpses.

Natural impacts

Earthquakes have a lesser detrimental impact, as the facilities are also safe against shockwaves from significant explosions, so they can withstand earthquakes with very similar efficiency. There is no facility in Hungary constructed on a system of internal absorbers, the protection of only some built-in devices is solved in this, in certain places. In contrast, in the case of protected facilities built in an environment that is seismologically more active and geologically unstable, this can be an important factor.

Floods and tsunamis are also less dangerous because the facilities were or are built in generally non-floodplain locations. If necessary though, the shutoff doors (if shut) will fully withstand the water pressure due to the load. For instance, one good example is the protected command post, the F-4 facility, underneath the Inner City in Pest, built for MDP, in the middle of the 1950s. [16] Tsunami in Hungary is absolutely excluded.

Lightning is also less dangerous because these facilities are protected against electromagnetic impulses, including lightning, as they are usually located underground, so the protection is enhanced.

The natural formation of *wild fires* is possible in rare cases (due to fierce, long-term, large spatial lightning or volcanic eruptions), but in our case, we understand extensive long-term and high-temperature fires after an atomic bomb explosion or the ignition by other bombs inducing high temperatures in large areas. They are characterized by extremely low oxygen levels, strong suction and toxic gases. According to the design specifications, one should calculate with a 48-hour duration and a 2000-degree Centigrade gaseous temperature. Of course, the use of external air intakes is not recommended during this period. If it becomes necessary, however, a significant reduction in the temperature of the gas, cleaning and filtration may become necessary as well. It is extremely dangerous, because a significant part of facilities in Hungary is built on an easily combustible, densely forested area.

Where appropriate, due to *geological and hydrogeological changes* or due to changes in other human activities (e.g. deforestation, quarries, etc.), the solidity indicators of the supporting rocks may change, soil slides may occur and the water output of the inner wells may dwindle. This is a lesser risk because the existing facilities are located in enclosed areas, so, in principle no harmful deforestation or destruction may occur.

[28] In the 90s, in Warehouse IV of MoD (nowadays called KAGRA), a restricted government session with a small number of attendees was held; the facility overheated itself in a short time despite mechanical cooling.

[29] The Budapest metro line M3 nowadays, due to its normal operational heat release would already have too high temperatures even before deployment. The author's own observation during a sector test in 2016.

Other impacts

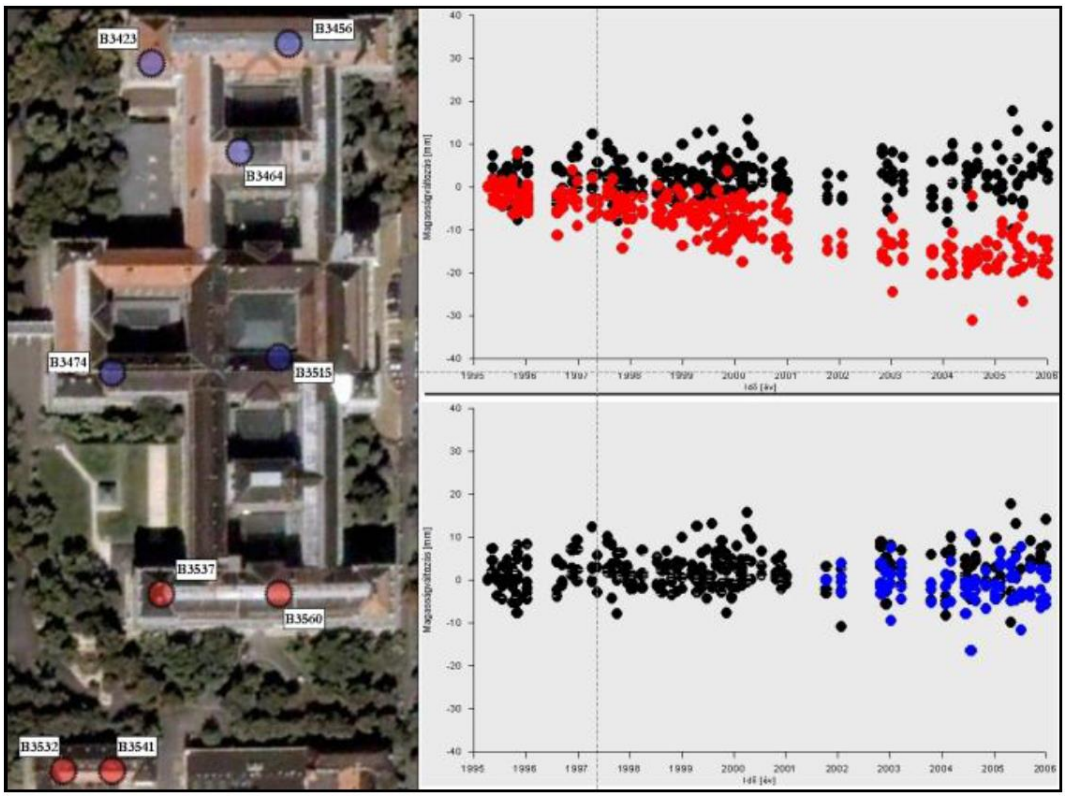
Because of the advanced industrial production by mankind, a protected facility may be built near a chemical or industrial plant. It is also possible that it is located further away, but in case a large *industrial or chemical disaster*, it becomes involved. This is possible, for example, due to the eventual failure of two Slovak nuclear power plants near the Hungarian border. In such a case, the devices built in against other effects (filtering and ventilation systems, locking ability, etc.) would provide sufficient protection in general.

Perhaps one of the most damaging effects are posed by *internal fires*. This is because these facilities always consist of narrow and confined rooms. Their (emergency) exit corridors are usually hundreds of meters long. The smoke emerging as the side effect of fires can cause very significant problems. A good example is the fire tricking even professional firefighters, equipped with oxygen cylinders, through corridors under the labyrinthine basement of the Budapest University of Technology and Economics (taking death tolls), broken out in 2006.

Generally, *operational disruption* is a system process based on a domino effect, resulting from some sort of anomaly. Nowadays, it poses an increasing risk because electronic control systems (building operational management systems) are more and more complicated and the interaction of some systems is not always known satisfactorily. By testing, practicing and simulating, the effects can be significantly reduced.

In specially fortified facilities, there are numerous hazardous devices, machines or equipment in service such as switchboards, batteries, diesel power generators, fuel tanks, oxygen bottles, compressed air containers, etc. Improper handling of them can cause an internal explosion as well. Complying with the rules, risks can be minimized. In fact, the use of conventional explosives in a confined is not a negligible factor besides heat and the shock wave of the explosion, neither is the resulting lack of oxygen and the toxic, choking effect of the residual gunpowder.

The *ever-accelerating technical development* is a major threat to a well-camouflaged, protected facility. This is a very good example of a new technology, the so-called satellite radar interferometry technology. Its essence is that some satellites, since the end of 1992, continuously emit radar signals and measure their reflected data. Signals can be reflected from any solid and large objects (building, pavement, ground). Satellites emit radar signals to all the points of the Earth (except the seas, oceans) with very high density, in an unprecedented resolution (up to 500-1000 points/km^2). The measurement is so accurate that it detect an approx. 0.1 mm/year vertical movement. No field measurements are required. The results of the measurements have been saved retrospectively for decades, and some of them can be retrieved for civilians and researchers as well. [17] [18; pp.3-9.] Obviously, it is possible to write automatic registration and signaling programs for these sets of data that monitor and indicate the major field movements for the human analysis service. As a protected facility, almost all built with mining technology, with the surface collapsing, it is almost impossible to conceal a new (or built since the early 90's) underground facility.



119: The timelines of sprinkle points are marked with black, located in the central and northern part of Building K of BUTE. Marked with grey are the timelines of the sprinkle points of the southern part and the immediate neighboring buildings. In the lower figure, marked with grey, you can find the data for the same after the reinforcement works of the base [18; p.8.]

Over the past decades, the efficiency, capabilities and capacities of reconnaissance have increased tremendously. Especially due to the widespread use of technical detection, there are far greater opportunities inherent in what the contemporary concealment and disguise of these facilities would provide. It can be stated that similar facilities in the world are generally well-known by foreign intelligence services and by the local population as well. This is partly so, as nowadays, with the rapid development of the technical level of these facilities, camouflaging solutions of these facilities have not at all been kept up-to-date. Therefore, the *lack of camouflaging* is one of the greatest risk factors. Today, due to the precision and the details of visual or satellite reconnaissance, a surface construction cannot be concealed. An underground construction would always have a surface "footprint".

Changes in the national defense policy and the willingness of the current government to allocate financial means is the factor that nowadays mostly determines the present and the future of such and similar facilities. Leaders (of current national governments) do not take into account that domestic or international environment and the national defense policy [19; pp. 113-118.] [30] can radically change in much less time than the lifetime of such a facility, or even the design or construction time. So, there is a need to create, maintain, operate, close, or dispose of these facilities to meet the current circumstances, to avoid the worst outcome. Nowadays, Hungary does not have an enemy concept; therefore, most of these facilities were abandoned or left entirely to decay in the past decades. In other (Western European) countries, where the extent of external threats is similar or perhaps even more favorable, these facilities are still maintained and operated at a high level. The situation in Hungary is well characterized by the fact that some years ago, politicians had brought up the closure of one of the highly protected facilities, which could have served as shelter for them in a classified period. This "idea" was

[30] An earlier article on the relationship between national defense policy and shelters.

not implemented just because the proper closure (occlusion) of the facility would have cost a huge sum.

Communication nowadays in all the fields is essential. There is a need to keep in touch with the rest of the world. Much of this work is exposed to data traffic inward and outward. As these facilities are generally large in size, communication between the internal departments is also important for security reasons. As a result, the *lack of external and/or internal communication* may be a cardinal issue. The following figure shows an older communications center.

Figure 20: Communications center of command post D0 (code name Istanbul) in the former Yugoslavia (nowadays Bosnia-Herzegovina) [20]

RECOMMENDATIONS ON THE PROTECTION AGAINST ENDANGERING FACTORS

Protection against offensive weapons is paramount with these. One may and should protected against them with a suitable thickness of protective layer and masonry as well as doors and windows. It is possible to protect against high dynamic effects with so-called absorbers[31].
Against EMI, it is possible to protect with proper structural thickness, steel lining and multilayer construction.

The threatening effects and factors need to be known to establish and maintain specially fortified facilities, which are necessary for the correct establishment of requirements. Their analysis and risk assessment must be carried out before the design phase.

During the design and construction, only the highest qualified, experienced and certified engineers can be employed. Training must be continually maintained. Design faults can be screened by employing design controllers.

Training of the operating personnel is just as well needed as the one of designers.

Against physical intrusion, protection can usually be ensured by complex, intrusion-protected solutions. There are countless devices to protect against unauthorized intrusion. They can be physical, optical, visual, electronic solutions. Other special solutions used are infra-red cameras, motion detectors and gas-tight protection doors. In some places, a very simple method is used: the sand in the vicinity of fences is raked in a special pattern, in which the footprints of an intruder become visible.

[31] Absorbers are energy absorbing and energy conversion devices. With their use, the physical impacts on structures can be moderated. For example, springs to which diesel engine groups are mounted.

Preventing malicious data acquisition is nowadays a very difficult and complex task. For example, when constructing a new facility, much attention should be paid to the fact that mobile phones at the workers, well-known by foreign intelligence, should be made inoperative before any meeting, especially when traveling to the site, as mobile telephone operators in foreign hands can easily obtain important information with these devices.[32]

The psychic exhaustion of the personnel inside can be prevented through more livable and friendlier interiors (for instance calming, warm-colored walls[33], recreation rooms with dead windows covered with curtains[34], etc.), with proper behavior and monitoring network and sabotage-proof structure design (for instance delimitation).

Of course, when constructing new building operational management systems, it is not advisable to connect them to external networks. It is advisable to create a physically completely separate network and to provide access only from the internal dispatcher room.

The biggest challenge is fighting the ever-accelerating detection and intelligence techniques. For example, against satellite radar interferometry one can protect with dense vegetation cover, as signals are not reflected to satellites.

Fuel (energy) can nowadays be produced with advanced technology, in other ways (e.g. from geothermal sources, thermal water, etc.), but they are not yet widespread systems, and since the construction of a new facility is not on the agenda, no such systems are built.

SUMMARY

From the above it turned out that, from design to operation, the definition of requirements is a very complicated and complex task at such a facility. They should be incorporated into operational plans as well. Thus, risks can be minimized. The probability of occurrence of the above effects should always be determined individually. One should be aware of the need to develop a level of protection. Unfortunately, due to the complexity of probability calculation, it is often not done. One can prepare them for an effect at one time, relatively easily and effectively, but the coexistence of two or more unfavorable factors can result in a very high risk level. For example, the appearances of a serious construction failure and an offensive weapon triggering shockwave. Or the simultaneous extortion and the introduction of toxic gases at any surface connection point.

Protected facilities should be dimensioned and designed to face a number of risk factors, requiring very special expertise. Recent and present politics regarded them as almost "unnecessary". Future natural and political challenges recognized, however, the necessity of these facilities. The present and future utilization of the existing ones are dealt with by some specialists on research level as well. [21; pp.296-310.] Ferenc Kovács and János Szalai could be mentioned as such examples.

Overall, it can be stated that protected facilities deserve more attention within the defense/protection sphere; and the exploration of endangering factors is the basis of any further activity.

[32] Dr. Horváth, Tibor called my attention to it, special thanks to him.

[33] Guidance by Potucsek, Iván during the reconstruction of the HDF Air Command and Control Center in Veszprém.

[34] An example of such settings is the recreation room of the Kingsway underground telephone switchboard center under London City.

REFERENCES

[1] TÓTH, R.: Based on the lecture (Doctoral School of Military Engineering, National University of Public Service).

[2] HORVÁTH, T., WANCZEL, G.: Csapaterődítés, "Kossuth Lajos" Military Academy, Higher education textbook, Szentendre, 1995.

[3] SZALAI, J.: A speciális erődítési létesítmények alkalmazása és szerepe az új biztonsági kihívások tükrében, PhD dissertation. 2010. Budapest

[4] KOVÁCS, F.: Állandó rendeltetésű védett létesítmények tervezésének folyamata és alapelvei a hagyományos fegyverek hatásaival szemben a NATO ajánlása alapján, study 2. (2002)

[5] KOVÁCS, F.: Állami és katonai védett létesítmények létrehozása és fenntartása (Doctoral School of Military Engineering, National University of Public Service). (PPT presentation)

[6] KOVÁCS, Z.: Katonai kritikus infrastruktúra fizikai védelme. (Doctoral School of Military Engineering, National University of Public Service) lecture 3, slide 9, NUPS lecture notes (ppt).

[7] Early civil protection tutorial board (MN PV).

[8] FLEETWOOD, R.: rafleet@aol.com, http://members. aol.com/blast.htm.

[9] www.nuclearweaponarchive.org (Downloaded: 26 September 2016)

[10] NORDYKE, M. D. – WILLIAMSON, M. M.: U.S. Army Corps of Engineers: The Seden Event Lawrence Radiation Laboratory, University of California, Livermore, California, 1965. (www.osti.com) (Downloaded: 29 October 2007)

[11] PÁSZTOR P.: A speciális erődítési (védett) létesítmények béke időszaki alkalmazásának lehetőségei, Kard és Toll 2004/1.

[12] http://www.titkosbudapest.hu/hirek/a-varbunker/154 (Downloaded: 26 September 2016)

[13] JAMRIK, L.: Üresen kong a világ legnagyobb atombiztos kormányóvóhelye (www.falanszter.hu) (Downloaded: 07 October 2011)

[14] Spiegel.de

[15] TÓTH R.: A METRÓ kettős rendeltetését biztosító műszaki megoldások és speciális berendezések, lecture notes (ppt).

[16] SZABÓ, B.: Rákosi titkos bunkere. Sziklakórház Kiadó. 2013.

[17] http://www.sgo.fomi.hu/InSAR/

[18] GRENERCZY-VIRÁG-FREY-OBERLE: *Budapest műholdas mozgástérképe: a PSInSAR/ASMI technika hazai bevezetése és ellenőrzése*, Geodézia és kartográfia 2008/11.

[19] HORVÁTH, T.: Óvóhelyek tervezésének, méretezésének jogi alapjai, *National Defense University Communication,* year 2. (1) 1998.

[20] The secret of the former Yugoslavia 280 meters under the ground. (www.falanszter.hu) (Downloaded: 12 January 2018)

[21] KOVÁCS F. – SZALAI J.: Speciális erődítési létesítmények hasznosítása az új biztonsági kihívásoknak megfelelően. Hadmérnök: year VI, No. 1 – March 2011.

[22] HORVÁTH, T.: *A személyi állomány védelmét biztosító erődítési építmények fejlődésének vizsgálata és a további fejlesztés lehetséges irányai. PhD dissertation*, Budapest 2002.

[23] HORVÁTH, T.: A védőképesség növelésének lehetőségei az erődítés-álcázás területén. *Higher education textbook*, ZMNE 2000.

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

ATOMERŐMŰ GENERÁCIÓK FEJLŐDÉSÉNEK VONZATAI

DEVELOPMENTAL CONSEQUENCES OF ATOMIC POWER PLANT GENERATIONS

ANTAL Zoltán; KÁTAI-URBÁN Lajos; VASS Gyula

(ORCID: 0000-0001-9373-3454); (ORCID: 0000-0002-9035-2450);
(ORCID: 0000-0002-1845-2027);

antalzmax@gmail.com; lajos.katai@uni-nke.hu; gyula.vass@katved.gov.hu

Absztrakt

Az első atomerőművek kifejlesztésétől napjainkig több évtized telt el. A nukleáris láncreakció biztonságos szabályozása és felhasználása mára már mindennapos feladattá egyszerűsödött, köszönhetően a több évtizedes, különböző típusú atomerőművek üzemeltetési tapasztalatainak. A cikkben bemutatásra kerülnek a leglényegesebb szempontok, amiben az egyes atomerőművek különböznek egymástól, az évtizedek alatt bekövetkezett technológiai változtatások, melyeket ma már generációkba sorolunk és szót ejtünk a jövő nukleáris energiahordozóiról is. Mindezek feltételeiről, összefüggéseiről és egymáshoz való viszonyukról végül levonhatjuk majd azt a konzekvenciát, hogy a nukleáris energiát felhasználó üzemek előtt még sok fejlődési szakasz áll, tekintve azt, hogy a technológia előrehaladása mindig újabb megvalósítható lehetőségeket kínál az emberiség tudósainak.

Kulcsszavak: *atomerőmű, reaktor, nukleáris, fúzió*

Abstract

Several decades have passed since the appearance of the first atomic power plants. Safe regulation an utilization of the nuclear chain-reaction has become by now an everyday task, due to the decades-long operational experience of different types of atomic power plants, The most important aspects of differences among the types of atomic power plants are to be presented in this thesis, along with the technological changes and developments of these past decades (hence the expression "generations of atomic power plants" has been used validly) and the nuclear energy sources of the future will be touched upon as well. Eventually a consequence may be drawn, based on the conditions and correlations of all the above, that there are a lot of developmental possibilities and new periods to come in the future for power plants using nuclear energy- due to the fact that technological advancement will continuously provide options for humanity and its scientists to improve and realize the potentials hidden in this resource.

Keywords: *nuclear power plant,reactor, nuclear, fusion*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.10.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.11.

BEVEZETÉS

Az elmúlt évtizedekben a villamos energia felhasználása olyan rohamos mértékben növekedett a technológia és számítástechnika fejlődésének köszönhetően, hogy a közeljövőben az igények kielégítéséhez tudatos tervezésen alapuló, megnövelt hatásfokú energiatermelőkre lesz szükség, amelyek alkalmazása nem jár együtt a környezeti károk növekedésével. Az emberek fajlagos energiaigénye napról napra nő, így a technológiai fejlődés és hatásfoknövelés elengedhetetlen szegmense a villamos energiatermelésnek. Az optimális cél tehát olyan korszerűen hatékony energiatermelő technológiák megalkotása, amelyek káros környezeti hatása és kockázati tényezője alacsony. A kezdeti nukleáris reaktor üzemeltetés veszélyes és kiforratlan technológiájához képest a jelenlegi energiatermelést tekintetbe véve ma az atomenergia felhasználása áll a legközelebb az optimális igények kielégítéshez. [1] A jelenleg alkalmazott aktív és passzív biztonsági rendszerek már olyan fejlett megoldásokat tartalmaznak, amelyek alkalmazása mellett az atomerőművekről megállapítható, hogy üzemük során nincs káros hatásuk, és nem okozzák a környezet károsodását.

A világban termelt villamos energia 12%-át adják az atomerőművek. [2] A jelenleg üzemelő erőművek azonban működési élettartamuk végéhez közelednek. A cikkben a létező atomreaktorok típusainak és működésük jellemzésével kívánom bemutatni, hogy a II. világháború után miként fejlődött az atomenergia felhasználása, melynek eredményeként az újonnan épülő erőművek már felhasználják az elmúlt évtizedek tapasztalatait, továbbá miként tesznek eleget a jelenlegi biztonsági kritériumoknak. Az épülő 3 és 3+ generációs atomerőművek bemutatásával alátámasztom az azokat megelőző technológiák fejlesztett alkalmazásainak hasznosságát és előrevetítem a jövő generációi számára kifejlesztésre váró, egyenlőre még elméleti stádiumban lévő atomerőművek típusait.

REAKTORTÍPUSOK

Minden erőműnek hasonló az elektromos energiatermelési alapelve, a különbség az atomerőművek esetében az, hogy a folyamathoz szükséges hőt nukleáris energia felhasználásával állítják elő. Manapság az atomerőművek fejlődésének szakaszait generációkba szokás sorolni, melyek között nincs egyértelmű határvonal, ugyanakkor egymásból kiinduló átmeneteket figyelhetünk meg bennük. [3] A generációkon belüli csoportosítás alapjául a nukleáris láncreakció szabályozására és a keletkező hő elvezetésére hivatott közeg különböző megoldásai szolgálnak, hiszen az atomreaktorokban három alapvető biztonsági feltételt kell teljesíteni annak érdekében, hogy káros hatás mentes energiatermelés valósulhasson meg: [3]

- a nukleáris láncreakció hatékony szabályozása;
- a termelt energia és hő megfelelő elszállítása;
- a radioaktív anyagok kikerülésének megakadályozása.

Az atomerőművek esetében a moderátor, a neutronelnyelő- és a hűtőközeg a nukleáris láncreakció és energiatermelés szempontjából a legfontosabb paraméterek. Amint az ismert, az atomreaktorban nukleáris láncreakció játszódik le, ahol a maghasadás során egy neutron befogadó izotóp több neutront termel. A neutrontermelés energiatermeléssel jár együtt, azaz például 1 db Urán 235 izotóp elhasadásakor kb. 200 MeV szabadul fel. ($1\ \text{MeV}=1.6\ 10^{-13}$ Joule) [4]

A földön egyetlen olyan természetesen előforduló izotóp van, amely neutron hatására könnyedén képes elhasadni és újabb neutronokat termelni, ez az ^{235}U -ös tömegszámú izotópja. Neutronbefogással további három olyan izotóp állítható elő, mely atomreaktorokban

felhasználható. Az ^{238}U-ból plutónium 239 és 241-es izotópja, valamint a tórium 232-es izotópjából ^{233}U izotóp. [5]

A reakció állandó szinten tartását és stabil működését szabályozni kell valamint annak leállítását is meg kell tudni valósítani. A maghasadás során keletkező többlet neutron elnyeletésével csökkenteni lehet a maghasadások számát, vagyis a neutronelnyelő anyag mennyiségének módosításával szabályozni a láncreakciót. Neutron elnyelő hatása van a bór 10-es tömegszámú izotópjának, a kadmiumnak, a gadolíniumnak, diszpróziumnak vagy az erbiumnak. A szaknyelv ezt a szabályzott keretek között fenntartott láncreakciót kritikus állapotnak nevezi. A maghasadási reakció elérésére és fenntartására azonban nem elegendő a neutronelnyelő közeg alkalmazása. Az Urán 238-as izotópja (továbbiakban ^{238}U) a természetben előforduló urán 99.3%-át teszi ki és csak 0.7%- a Urán 235 (továbbiakban ^{235}U). Az ^{238}U hasadás nélkül befogja és megállítja az előző maghasadás során keletkező nagy energiájú neutronokat, így a benne lévő hasadóképes ^{235}U izotóp reakció esélye kicsi. A hasadási láncreakció fenntartására éppen ezért két megoldást alkalmaznak. [6]

Az első, hogy a keletkező gyors neutronokat lelassítják, amihez neutronlassító anyagokat használnak fel, ezek a moderátorok. Ezen anyagok atommagjával ütközve a neutron lelassul, úgynevezett termikus neutron keletkezik, ami nagyobb valószínűséggel hoz létre újabb maghasadást. Ilyen moderátor anyagok például a könnyű- és nehézvíz vagy a grafit. A könnyűvíz esetén a maghasadás létrejöttének érdekében az ^{235}U-öt 0.71%-ról 2-5%-ra dúsítják, hogy így növeljék a termikus neutronok által létrehozott maghasadás lehetőségét, mivel a hidrogén kis mértékben elnyeli a termikus neutronokat. Nehézvíz és grafit moderátor esetében a láncreakció természetes uránnal is megvalósulhat. [6] [7]

A második lehetőség a neutron lassítás helyett az ^{235}U nagy mértékű dúsítása és egy reaktoron belül nagyobb mennyiség felhalmozása. Ebben az esetben viszont az ^{238}U neutronelnyelése során új hasadó anyag, nevezetesen plutónium keletkezik. Ezt a folyamatot tenyésztésnek hívják, az ilyen típusú reaktorokat pedig gyorsreaktornak.

Az első nukleáris energiatermelést célzó reaktorok feltalálásától napjainkig ezen elvek alapján fejlődtek az atomerőművek. [6] [7]

Termikus reaktorok

A termikus reaktorokban a már említett önfenntartó maghasadást lassú, azaz termikus neutronok tartják fenn a moderátorok segítségével. A maghasadások során a nagy mennyiségű keletkező hőt el kell vezetni. Grafit moderátor esetében a hűtéslevezetés történhet szén-dioxid vagy héliumgáz felhasználásával. Könnyű- és nehézvíz esetében a hűtőközeg lehet maga a moderátor vagy kialakítható külön hűtővízrendszer is. [8]

Folyadék moderátorú reaktorok

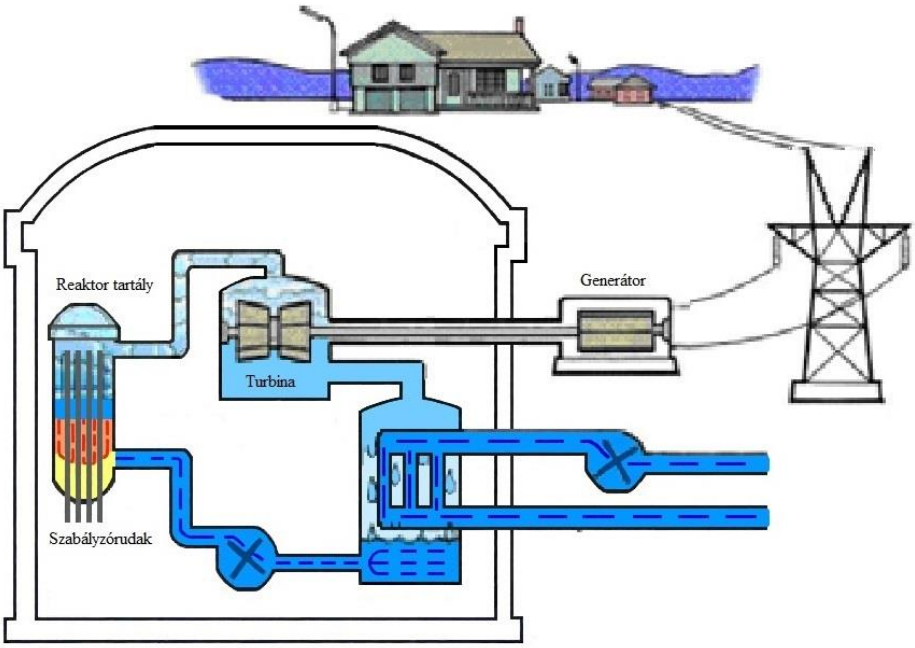
A könnyűvízzel moderált reaktorok esetében, ahol a moderátor és a hűtőközeg is víz, a meghasadásos hőtermelés következménye, hogy a reaktorban túlhevülés esetén a víz forrni kezd, ami által csökken a moderátor a reaktorban és így a neutronlassító képessége is csökken. A keletkező gyors neutronok maghasadás nélkül befogódnak az uránban.

Kétféle könnyűvizes reaktortípus került kifejlesztésre, a nyomott vizes és a forralóvizes reaktorok, melyek között az alapvető különbség a primer és szekunderkör valamint az őket körülvevő konténment kialakításában van. A konténment bevezetéséről később, a 2. generációs erőműveknél ejtünk még szót.

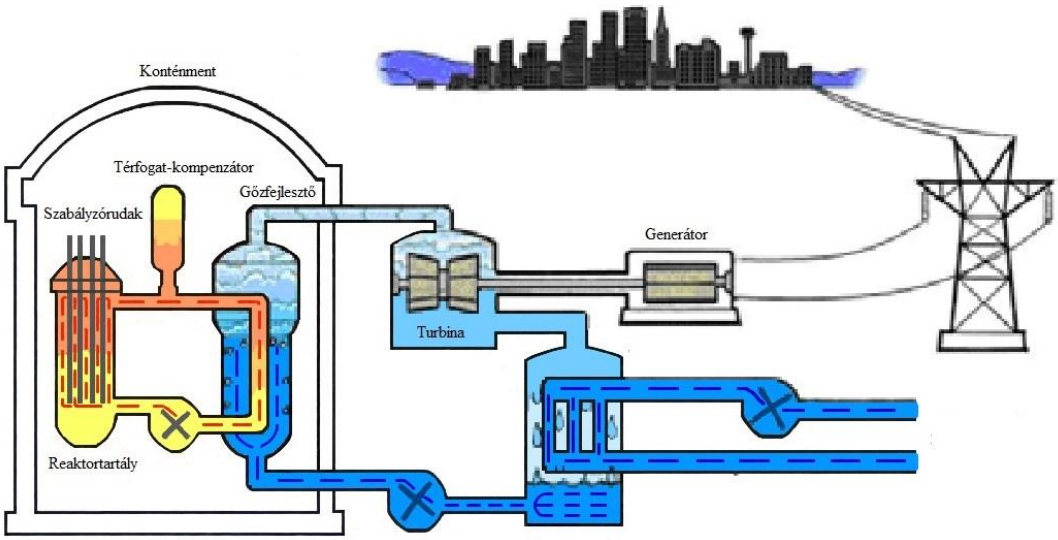
A nyomottvizes atomreaktor moderátora és hűtőközege könnyűvíz, üzemanyaga pedig alacsony dúsítású urán. Jellemzője, hogy a primerkörben, azaz az aktív zónában felszabaduló hőt egy hőcserélőn át adja át a szekunder körnek, ahonnan elforrással a turbinák meghajtásához használatos gőz keletkezik. A primer és szekunder vízkör megkülönböztetése azért fontos, mert egymástól fizikailag elhatárolt, eltérő nyomású hűtővízkörről van szó, így a

konténment a primerköri részeket veszi csak körbe, mivel az a szekunderköri vízzel nincs közvetlen kapcsolatban. A primerköri vizet itt magas nyomáson tartják, hogy az magas hőmérsékleten se forrjon el, azonban a gőzfejlesztők csövei által visszahűl és egy körfolyamat révén visszajut a reaktorba. A radioaktív anyagok így a primerkörben maradnak.

A forralóvizes reaktorok egykörösek, azaz a reaktor aktív zónáján áthaladva a víz elforr és azt leválasztva telített gőz kerül a turbinákra. Ebben az esetben a szekunder kör, vagyis a turbinák is a konténmenten belülre kerülnek, hiszen a turbinákra is az enyhén radioaktív hűtőközeg kerül.

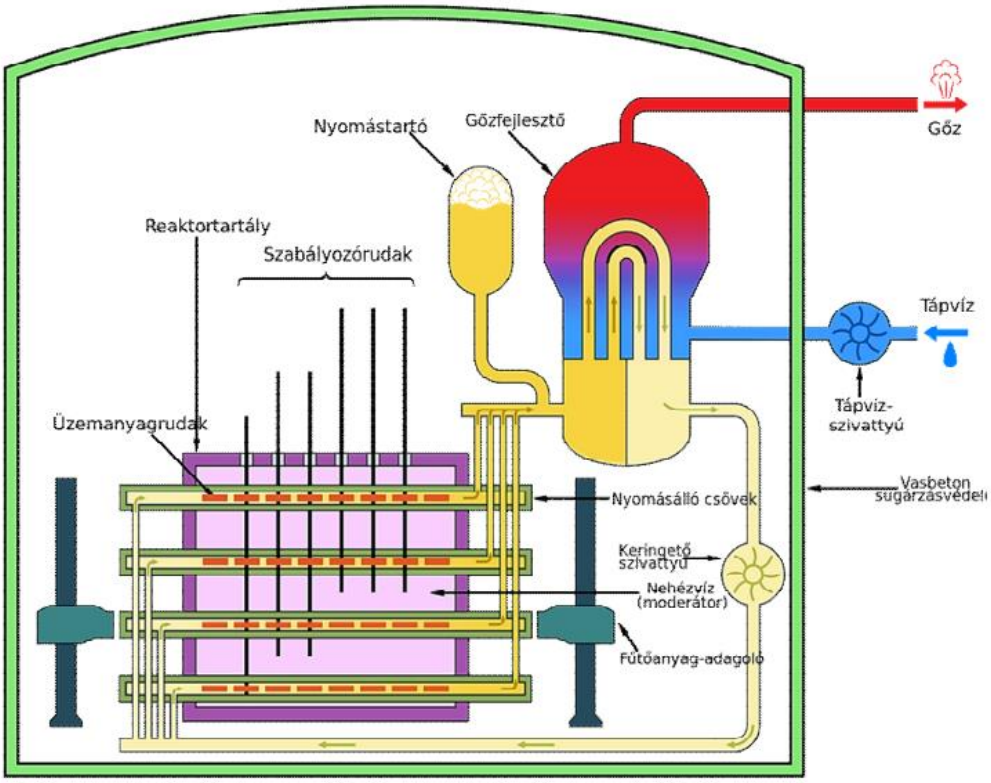


1. ábra Forralóvizes reaktor
Forrás: http://watt-logic.com/2017/12/06/abwr/



2. ábra Nyomott vizes reaktor
Forrás: http://watt-logic.com/2017/12/06/abwr/

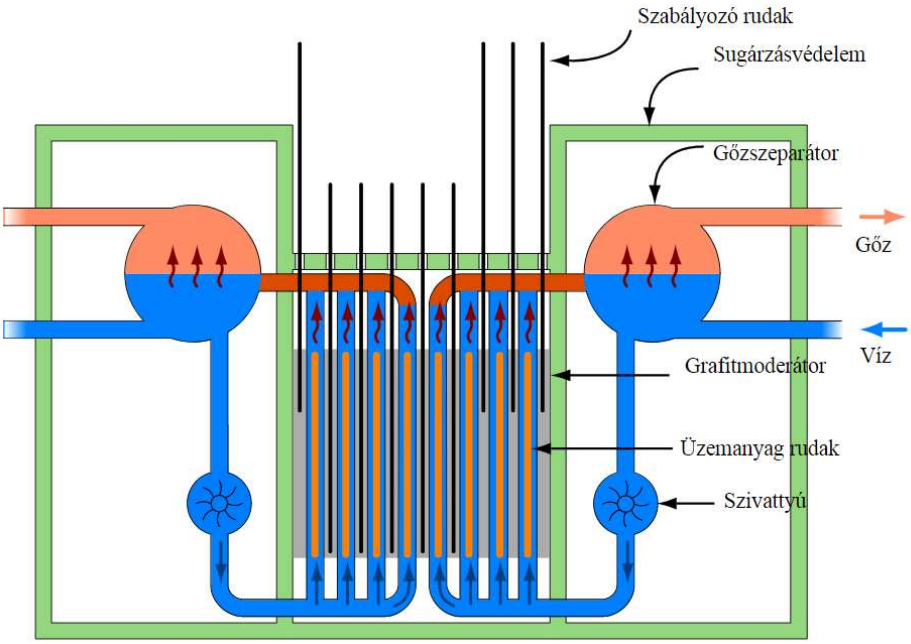
A nehézvízzel moderált reaktorok esetében a hűtőközeg könnyűvíz, a moderátora pedig nehézvíz. Az üzemanyaga lehet természetes vagy enyhén dúsított urán, mivel a nehézvíz nem nyeli el a neutronokat. Ezeknél a reaktoroknál nincs szükség a friss üzemanyag feltöltéshez a leállásra, mert az üzemanyag nyomásálló csövekben van, nem tartályokban és ezek egyesével, folyamatos működés mellett is felnyithatók. [5] [6] [8]



3. ábra Nehézvíz reaktor
Forrás: RADNÓTI K., KIRÁLY M.: Az atomenergiáról egyszerűen: az atomerőművek működése, típusaik és jövőjük. *Nukleon*, VIII 177 (2015). 1-13.oldal

Szilárd moderátorú reaktorok

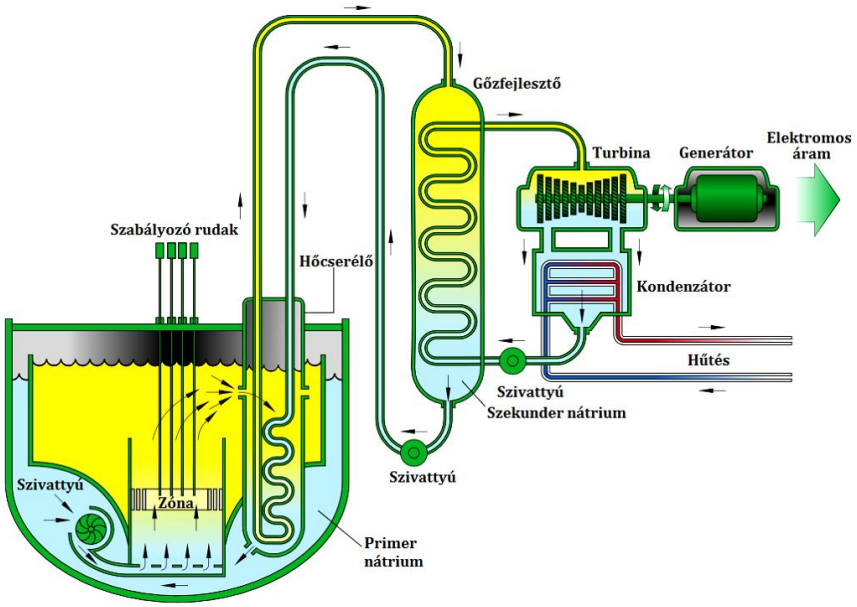
A grafit moderátoros erőművek esetében a hűtőközeg lehet gáz (szén-dioxid, hélium) vagy lehet könnyűvíz. A reaktor előnye, hogy természetes uránnal is működtethető, de a gazdaságosság szempontjából enyhén dúsított uránt használnak. Ugyanakkor a könnyűvíz hűtésű reaktornál túlhevülés esetén a neutronelnyelő hűtővíz elforrhat, ami a grafit moderátor megmaradásával a láncreakció és a hőtermelés folytatódását eredményezi és a reaktor megszaladásához vezethet, mint a csernobili atomerőmű baleset esetében. [5] [6] [8]



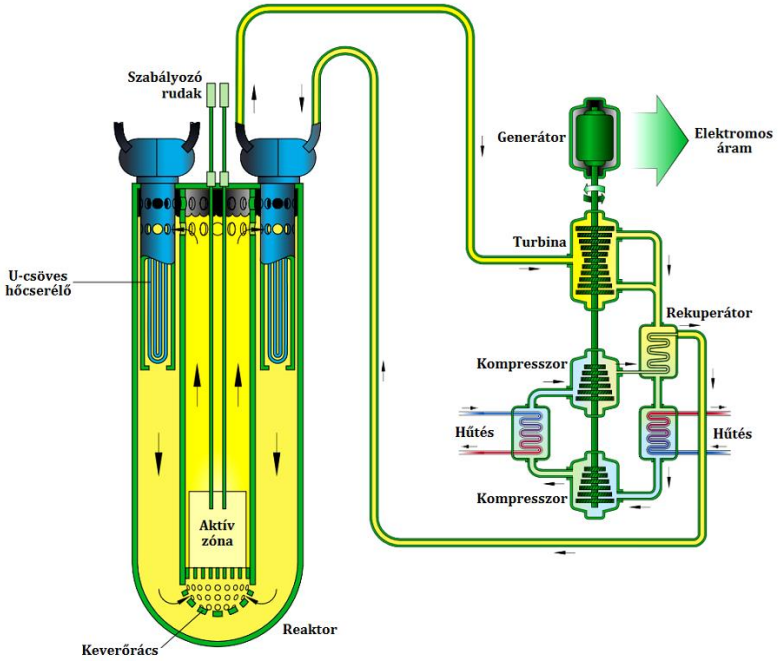
4. ábra Grafit moderátoros reaktor
Forrás: http://www.bnra.bg/en/useful/reactor-types/rbmk.gif

Gyors reaktorok

A gyorsreaktorokban nincs moderátor, itt az aktív zónában a neutronok nem lassulnak le. Nagy dúsítású uránnal vagy plutóniummal működnek, ami származhat már kiégett nukleáris üzemanyagokból vagy leszerelt atomtöltetekből. A gyorsreaktorok feladata a villamos energia termelésén felül újabb hasadó anyagok termelése. Ebből következik, hogy a gyors reaktorok egyben tenyésztő reaktorok is. A reaktorok intenzív hűtését úgy kell megoldani, hogy a hűtőközeg ne lassítsa le a neutronokat, ezért erre a célra folyékony fémet alkalmaznak, nátriumot vagy ólmot. [5] [6] [7] [8]



5. ábra Nátriumhűtésű gyorsreaktor
Forrás: RADNÓTI K., KIRÁLY M.: Az atomenergiáról egyszerűen: az atomerőművek működése, típusaik és jövőjük. *Nukleon*, VIII 177 (2015). 1-13.oldal



6. ábra Ólomhűtésű gyorsreaktor
Forrás: RADNÓTI K., KIRÁLY M.: Az atomenergiáról egyszerűen: az atomerőművek működése, típusaik és jövőjük. *Nukleon*, VIII 177 (2015). 1-13.oldal

Tenyésztőreaktorok

A tenyésztő reaktorok lényege, hogy a termelődő hasadó anyagok aránya az elhasznált hasadó anyagénál nagyobb legyen. Erre azért is szükség van, mert az ^{235}U nem megújuló energiahordozó, és bár jelentős készlettel rendelkezünk, 50-100 év múlva elfogyhat. Az uránon és a belőle neutronbefogadással ~~keletkeztethető~~ előállítható plutóniumon felül még a tórium neutronbefogadással átalakuló izotópja, a ^{232}Th alkalmas a maghasadás láncreakciójának fenntartására. A tenyésztőreaktorok javarészt még fejlesztés alatt állnak és jelenleg még nem vesznek részt aktívan a villamos energia termelésében, de az atomerőművek üzemanyaga, mint nem megújuló, véges energiaforrás szempontjából kis számuk ellenére egyre nagyobb jelentőséget kapnak. [5] [6] [7] [8]

ATOMERŐMŰ GENERÁCIÓK

1. generáció

A II. világháború után minden olyan nukleáris kezdeményezést, amely az atomenergia békés felhasználását tűzte ki célul az első generációnak tekinthető. A tudósok az ötvenes évek előtt is a békés atomenergia-termelés beindításának alapjait kívánták lefektetni, de a háború és az atombomba felhasználása elodázta a nukleáris energia kiaknázásának lehetőségeit.

Aztán az USA 1951-ben üzembe helyezte az első, nátrium-kálium hűtésű kísérleti szaporító gyorsreaktort, mely ugyan már villamos áramot is termelt, de ez inkább csak a reaktorcsarnok világítására volt elegendő. Fontosabb tulajdonsága volt, hogy a Urán 238-ból állított elő Plutónium 239-et, az atombomba úgynevezett alapanyagát. [5]

Az első hálózatra kapcsolt atomerőművet 1954-ben állították üzembe Obnyinszkiben, Moszkvától 110 kilométerre. Ez egy grafit moderátoros, vízhűtésű, egy reaktorblokkos erőmű volt. [5]

Anglia 1953-ban állította üzembe az első, hivatalosan is kereskedelmi célú atomerőművét Windscale-ben, melyet maga II. Erzsébet királynő nyitott meg, azonban 1957-ben leégett. Ebben az évben állították üzembe Magnox atomerőművüket, mely szintén plutónium termelésére alkalmas széndioxid hűtésű, grafit moderátoros erőmű volt.[7]

Az USA 1957-ben állította üzembe a Shippingport könnyűvizes atomerőművet, mely még katonai célokra plutóniumot termelt, viszont 60 MW teljesítményével villamos energiát táplált be a hálózatba. [5] [7] [9]

2. generáció

A napjainkban használt reaktorok többsége ilyen, de tervezett élettartamuk, mint már említésre került, hamarosan lejár. Az első generációs, kezdetleges hibákból sok tanulságot levontak, ennek eredményeként a 70-es évektől épített, vagyis második generációs erőművek biztonságnövelő átalakítások alkalmazásával kerültek megépítésre. Az egyik legfontosabb újítás a nyomásálló burkolat alkalmazása volt, mely a baleseti helyzetekben megakadályozza a radioaktív anyagok kijutását a szabadba. Ez az úgynevezett konténment. Ezek a reaktorok már általános célú nukleáris erőművek lettek, amelyek feladata kizárólagosan a villamos energiatermelés. A jelenleg üzemelő paksi atomerőmű négy blokkja is a második generációs reaktorok közé tartozik, ugyanakkor az évek során több teljesítmény és biztonságnövelő fejlesztésen estek át, ahogyan a technológia fejlődése azt lehetővé tette. [5] [7] [9]

3. generáció

A jelenleg és az elkövetkezendőkben épülő atomerőműveket szokás a harmadik generációba sorolni, ezek más néven az evolúciós erőművek. Ezek lényege, hogy a második generációs erőművek működtetése során szerzett tapasztalatokat felhasználva kibővített és továbbfejlesztett technológiai megoldásokkal valamint a jelenlegi reaktortípusok gazdasági és biztonsági optimalizálása továbbá az ezekből gyűjtött tapasztalatok felhasználása által építik meg az új erőműveket. A működtetésben megnövelt hatásfokon, magasabb üzemanyag hasznosítással és fejlett dúsítási eljárásokkal együtt valósítanak meg az eddiginél jóval hatékonyabb és hosszabb, akár 60 éves üzemidőt. [5] [7] [9]

Az Aktív és passzív biztonsági rendszerek kialakítása jelentős fejlődésen ment át, köszönhetően a technológia és számítástechnika fejlődésének, valamint a sajnálatos balesetekből levont mértékadó tapasztalatoknak köszönhetően. [10]

A harmadik generációs atomerőművek fejlesztésének eredményeként jöttek létre a következő reaktortípusok: [6] [7] [8] [9] [10]

- EPR (European Pressurized Reactor) – egy olyan nyomottvizes hatásfoknövelt reaktor, melynek a konténmentje acéllal erősített duplafalú betonbunker. A zónaolvadás esetére a reaktor alatt egy zónaolvadék felfogó rendszer kialakítására került sor. Az újításokhoz hozzátartoznak a legkorszerűbb jelző és mérőműszerek beépítése is. A hűtőrendszere négy független rendszerből áll, amelyek a reaktor leállítása után is működőképesek maradnak 1-3 évig.
- AES 2006 (VVER 1200) – Újfajta, orosz fejlesztésű, továbbfejlesztett vízhűtéses, vízmoderátoros nyomottvizes reaktor. Erről a típusról részletesebben szó esik még a cikkben, mivel a Paks II beruházás során a meglévő atomerőmű mellé ilyen rektorokkal szerelt erőmű kivitelezése a cél.
- AP-1000 Westinghouse – Az amerikaiak által tervezett harmadik generációs atomerőmű, ahol a biztonsági rendszerek többleti felhalmozása lehetővé teszi a

balesetek esetére, hogy a reaktor emberi beavatkozás nélkül is biztosítsa 72 órán keresztül a reaktor hűtését és az aktivitás környezetbe ~~kerülésétkerülésének~~ megakadályozását. Ebben a továbbfejlesztett nyomottvizes reaktorban a pihentető medence a VVER új típusához hasonlóan a konténmenten belülre került.

4. generáció

A negyedik generációs atomerőműveket innovációs erőműveknek is szokás nevezni, hiszen olyan új megoldásokat és fejlesztéseket vetít előre, melyek az eddigi atomerőművek működését alapvetően más mechanizmusra tervezik. Ilyen például a fúziós erőművek megvalósításának lehetősége valamint minden olyan elméleti nukleáris reaktor dizájn, amely tervei, kutatásai, fejlesztései még folyamatban vannak. A negyedik generációs erőművek feltétele, hogy megfeleljenek a megnövelt biztonsági követelményeknek úgy, hogy a nukleáris hulladék minimalizálása és újrahasznosítása mellett az üzemanyag cellák érzékenységének kezelése is megvalósuljon. [5] [6] [11]

A negyedik generációs erőművek fejlesztése a következő típusok irányába indult el: [9]

Termikus reaktorok fajtái:

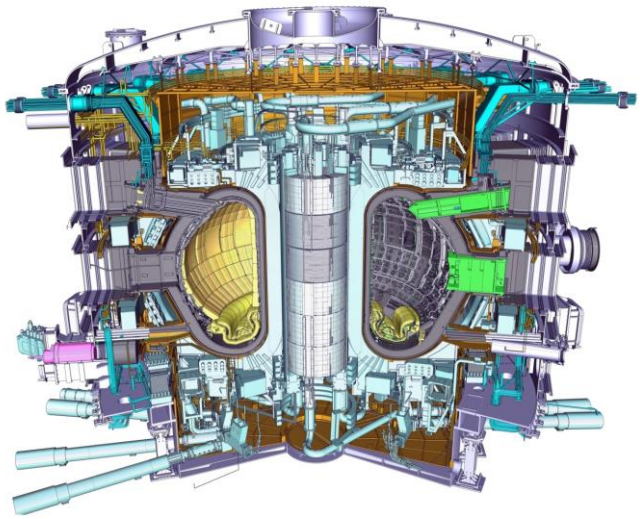
- Nagyon nagy hőmérsékletű reaktor (VHTR – Very HighTemperature Reactor);
- Szuperkritikus vízhűtéses reaktor (SCWR – Supercritical Watercooled Reactor);
- Olvadéksó reaktor (MSR – Molten Salt Reactor).

Gyors reaktorok fajtái:

- Gázhűtéses gyors reaktor (GFR – Gas-cooled Fast Reactor);
- Nátriumhűtéses gyors reaktor (SFR – Sodium-cooled Fast Reactor);
- Ólomhűtéses gyors reaktor (LFR – Lead-cooled Fast Reactor).

FÚZIÓS REAKTOROK

Deutérium és trícium hevítésével és azok tórusz formájú reaktorában mágneses térrel körpályára kényszerített ionjainak reakciója, amely révén plazmaállapot valósul meg valamint a neutronon felül hélium keletkezik. A reaktor falát vízzel hűtik és a hűtésből keletkező víz hajtja meg a turbinákat. [3] [8] [12] [13]



7. ábra Nemzetközi Kísérleti Termonukleáris Reaktor – Tokamak
Forrás: https://cpb-us-e1.wpmucdn.com/sites.psu.edu/dist/8/38131/files/2016/04/ITER.jpg

A PAKSI ATOMERŐMŰ

A Paksi Atomerőmű 1976-ban alakult, és 4 darab VVER 440/213 típusú nyomottvizes reaktort tartalmaz, melyek beépített teljesítménye 1850 MW. A négy blokk a világ élvonalába tartozik, mivel évek óta az első 25 legbiztonságosabb blokkja között szerepelnek. Ez az erőmű adja az ország energiatermelésének több mint 50 %-át. [14]

A reaktorok üzemanyaga urán-dioxid (UO_2), amelyből egy reaktorban 42 tonnányi mennyiséget helyeznek el. Az urándioxidból 9 mm magas, 7,6 mm átmérőjű hengeres pasztillákat préselnek, melyeket egy cirkónium-nióbium ötvözetből készült, 2,5 m hosszú, 9 mm külső átmérőjű csőbe helyeznek, amelyet feltöltenek héliumgázzal, és ezután hermetikusan lezárnak. A burkolat megakadályozza a hasadványok kikerülését a hűtővízbe. Az üzemanyag tabletta és a burkolat együtt jelentik a fűtőelem pálcát. Mivel a több tízezer fűtőelem pálca egyenkénti mozgatása, cseréje gyakorlatilag megoldhatatlan lenne, a fűtőelemeket kötegekbe, úgynevezett kazettákba foglalják. A fűtőelem kazetták hatszög keresztmetszetűek, és egyenként 126 fűtőelemet tartalmaznak. A nyomottvizes reaktorok közül csak a VVER-ek kazettája hatszöges, a többié négyzet keresztmetszetű. A kazettákban lévő UO_2 üzemanyag dúsítása 3,5-4,8 % között van, de egy kazettában rendszerint csak azonos dúsítású fűtőelemek vannak. A kazetták 14,4 cm laptávolságúak. Az aktív zónában összesen 349 kazetta fér el, ebből az üzemanyagkötegek száma 312.[4]

A VVER-440 típusban a láncreakció szabályozásához a fűtőelem kötegekkel azonos méretű abszorbens (bóracélból készült) kazettákat használnak, amelyek felülről lógnak be az aktív zónába. A reaktorban összesen 37 ilyen szabályozó és biztonságvédelmi rúd van, amelyek közül üzem közben 30 állandóan kihúzott állapotban, és az aktív zóna fölött helyezkedik el. Ezek a biztonságvédelmi rudak, amelyekkel a reaktor 10-12 másodperc alatt bármikor biztonságosan leállítható. A maradék 7 elnyelő kazettával az üzem közbeni teljesítmény-szabályozást végzik, de természetesen ezek is ellátnak biztonságvédelmi funkciót. A szabályozókazetták aljához egy-egy fűtőelem kazettát kapcsolnak, így a kihúzott abszorbensek helyén is üzemanyag található.

A már elhasználódott üzemanyag kazettákat áthelyezik a reaktor melletti pihentető medencébe, ahol három évig víz alatt tárolják őket. Ekkor már nem folyik bennük nukleáris láncreakció, csupán a radioaktív bomlások eredményeznek kismértékű hőfejlődést. A vízben elnyelődik a radioaktív sugárzás, s egyben hűti a kazettákat is. Így a környezetet nem veszélyezteti a sugárzás. Három év alatt lecsökken a kazetták sugárzása és hőtermelése olyan mértékben, hogy szállíthatóvá válik. Innen a Kiégett Kazetták Átmeneti Tárolójába kerül, a Paksi Atomerőmű telephelyének szomszédságában létesített tárolóba. Itt minimálisan 50 évig tárolhatók a kazetták, mindaddig, amíg a lehetőségek szerint egy végleges nagyaktivitású tároló kialakításra nem kerül.

A VVER típusú reaktorok nyomottvizes rendszerűek, azaz a primer körben nagy nyomás fenntartásával biztosítják azt, hogy a hűtőközeg ne forrjon fel (a víz forráspontja 1 bar nyomáson 100°C, a primer körben uralkodó 123 bar nyomáson viszont már 297°C). A nyomás állandó értéken tartására szolgál a térfogatkompenzátor vagy nyomáskiegyenlítő és négy darab hidroakkumulátor blokkonként. Minden blokkhoz 1 db térfogatkompenzátor tartozik, amely az egyik hurok meleg ágához csatlakozik. A térfogatkompenzátor egy álló elrendezésű tartály, melynek alját az egyik hűtőkör meleg ágával, tetejét (szelepeken keresztül) az egyik hidegággal kötik össze. A tartályban 325°C-os, telített állapotú víz, és felette nitrogénpárna található.

A szekunder körben történik a reaktorban megtermelt hő átalakítása mozgási, majd villamos energiává. A gőzfejlesztőben lévő 222°C-os, 46 bar nyomású tápvizet a csövekben keringő 297°C-os primer köri víz 260°C-ra melegíti, és felforralja. A keletkező gőzből a vízcseppeket el kell távolítani, ugyanis a turbinalapátokat károsítják a vízcseppek. Erre szolgálnak a kilépő gőz útjába helyezett cseppleválasztók. Ezek olyan terelőlemezek,

amelyeken áthaladva a vízcseppek lecsapódnak, így a kilépő gőz nedvességtartalma már alacsonyabb, mint 0,25 %.

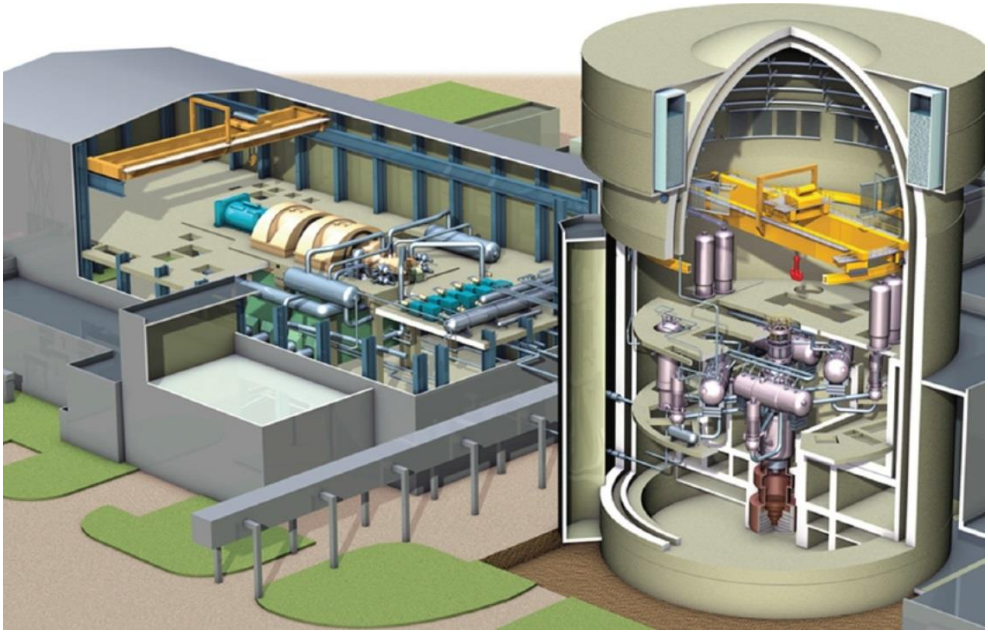
A gőzfejlesztőből kilépő, mintegy 450 t/h tömegáramú gőz a turbinára kerül, és meghajtja a turbina lapátjait. Egy adott blokkban lévő 6 gőzfejlesztőből 3 együtt táplál egy turbinát. A Paksi Atomerőműben 8 darab turbina és 8 darab 230 MW-os generátor van. A turbinában egy tengelyen helyezkedik el egy nagynyomású és két kisnyomású ház, valamint a generátor fogórésze. A turbina nagynyomású háza 7 fokozatú, azaz a gőz expanziója és munkavégzése 6 fokozatban történik. A nagynyomású turbinaházban a gőz hőmérséklete kb. 135°C-ra csökken, nedvességtartalma pedig 12 %-ra nő. Emiatt a kisnyomású házba való belépés előtt a csepplevalasztó és gőztúlhevítő berendezésbe kerül, ahol a turbinára káros vízcseppeket eltávolítják, és a telítési hőmérséklet fölé melegítik. A két kisnyomású ház 5-5 fokozatú.

A már munkát végzett gőz a kondenzátorba kerül, ahol a Dunából kivett hűtővíz áramlik. A hűtőcsöveken a gőz kb. 25°C-os hőmérsékleten lekondenzálódik. Minden turbinaegységhez két kondenzátor tartozik, amelyekben 0,035 bar nyomást (vákuumot) tartanak fenn. A turbinán a munkagőzt a gőzfejlesztő és a kondenzátor közti nyomáskülönbség hajtja át. A cseppfolyósodott munkaközeget különböző tisztító és előmelegítő berendezéseken keresztül a tápszivattyúk visszajuttatják a gőzfejlesztőbe. Az előmelegítésre az erőmű jobb hatásfoka miatt van szükség. Az előmelegítést a turbináról vett gőzzel végzik, melynek során a kondenzátorból kilépő 25°C hőmérsékletű víz 8 hőcserélőben végezetül 222°C hőmérsékletűre melegszik fel. A tápvíz ezen a hőmérsékleten lép be a gőzfejlesztőbe, ahol újra felmelegíti a primer köri víz hőenergiája. [3] [4] [6] [7] [15] [16]

A 3+ generációba tartozó VVER-1200 (AES-2006) reaktor

A VVER-1200-as reaktor orosz fejlesztésű, továbbfejlesztett vízhűtéses, vízmoderátoros nyomottvizes reaktor, melynek aktív és passzív biztonsági rendszerei a mai legmodernebb technológiákat alkalmazzák. Konténmentje két különálló részből áll, egy külső és egy belső burokból, melyek sajátos védelmi funkciókkal rendelkeznek. A külső burkolat 80 cm vastag és elbírja egy utasszállító becsapódását is, továbbá a konténment ellenáll a földrengésnek és nagynyomású lökéshullámoknak. A belső burkot belülről egy vastag acéllemez fedi, amit egy csőrácsháló is erősít. A megerősített belső burok ellenáll a nagy nyomásnak és a magas hőmérsékletnek. A konténmenten belül a sérült reaktorból származó gőz kondenzálására külön befecskendező rendszer lett kiépítve, valamint a pihentető medence is a konténmenten belül található, ami a hűtővízrendszer szükségszerű betáplálásban is részt vesz. A kiégett fűtőelemek átmeneti tárolójához tartozó 2000 m^3-es hűtővíz jelentős része alacsony- és magasnyomású rendszereken keresztül használható fel pótvízként. A magas nyomású rendszerek kis szivárgás esetén, az alacsony nyomású szivattyúk nagy elfolyásos csőtöréskor lépnek működésbe. A sérült reaktorból származó gőz kondenzálására külön befecskendező rendszer hivatott a Konténmenten belüli nyomás és hőmérsékletcsökkentésre. Ehhez a tartalék hűtővízrendszereket nitrogénnel helyezik nyomás alá, hogy megfelelő legyen a passzív befecskendezés a reaktorba. Az EPR-hez hasonlóan rendelkezik zónaolvadék csapdával ahol egy speciális anyaggal leállítják a láncreakciót és külön hűtőrendszer gondoskodik az olvadéktároló hűtéséről. Az aktív és passzív biztonsági rendszerek a primerköri csővezeték törése esetén is 72 órás hűtést biztosítanak a reaktornak. A hidrogénrobbanás megakadályozására a konténmenten belül hidrogén rekombinátorokat is alkalmaznak, amivel a belső, konténmentre belülről ható nagy nyomást lehet csökkenteni. A hidrogénrekombinátorok megakadályozzák a gőz és olvadt cirkónium reakciójaként felszabaduló hidrogénrobbanást úgy, hogy felgyorsítják a hidrogén-oxigén egyesülést, melynek eredményeként robbanóképes hidrogén elegy helyett víz keletkezik. A reaktorban a hűtővíz 160 bar nyomáson 328°C-os, amelyek a cirkónium fűtőanyag pálcákban lévő urán-dioxid pasztillákat hűtik és moderálják, maga a reaktor tartály pedig speciális

lengéscsillapítókra ültetett, 20 cm vastag falú, és négy gőzfejlesztőre van kivezetve. A reaktortartályban 163 kazettában darabonként 312 fűtőelem pálca található és 121 szabályozó rúd. A 3+ generációba tartozó VVER reaktornál a tervezett reaktorhűtés aktív és passzív rendszerek segítségével egyaránt megtörténhet, ahol a passzív rendszer üzemeltetése nem igényel villamos betáplálást vagy emberi beavatkozást. [17]



8. ábra VVER-1200-as reaktor vázlata
Forrás: http://static.ezermester.hu/Ezermester-online/2016/03/atoeromu%20paks2/1418055380.jpg

ATOMERŐMŰ GENERÁCIÓK FEJLŐDÉSÉNEK VONZATAI

Mindazt, amit ma generációknak hívunk az atomerőművek életében, igazán elválasztani egymástól nem tudjuk. A második generációs típusok nem egyszerre léptek a piacra, nem egy ország vagy egy tudós feltalálásából származnak. A II. világháborúban az atomenergia felhasználása egyértelműen ~~determinálta~~ előrevetítette a jövő fegyvere titulus mellett, hogy elképesztő kiaknázatlan területről van szó. Ahogy a tudomány fejlődött az évtizedek alatt, úgy lett egyre biztonságosabb a nukleáris energia felhasználása és az új lehetőségek kutatása. Minden egyes újítás és fejlesztés további lehetőségekkel kecsegtetett, melyeket sorra igyekeztek megvalósítani és a társadalom szolgálatába állítani. Éles generációs elhatárolásra talán a negyedik generációs erőművek megvalósításának esetében kerülhet sor vagy a jelenleg már működő, de még kísérleti stádiumban lévő nukleáris energiatermelési lehetőségek esetében, mint például a hidrogénfúzió. [18] A világban több tudós kutatócsoport épít úgynevezett tokamak berendezést, melynek a lényege, hogy a mágneses összetartású mágneses tekercsekkel toroidális kialakítású berendezésekben megvalósítják a plazmaállapotot, aminek az energiája felhasználásra kerül. [8] [13] [19] Az bizonyos, hogy minden egyes fejlesztés és kutatás hatással van az azt követőre és egymásra épülő rendszerként formálják már ma a holnap nukleáris energiafelhasználását.

FELHASZNÁLT IRODALOM

[1] *World Nuclear Industry Handbook*, Zagreb, Progressive Media International, 2016.

[2] *The World Nuclear Industry – Status Report 2017.* Paris: Mycle Schneider Consulting Project, 2017.

[3] BOGNÁR B., KÁTAI-URBÁN L., KOSSA Gy., KOZMA S., SZAKÁL B., VASS G.: *Iparbiztonságtan I. - Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához.* Budapest: Nemzeti Közszolgálati Egyetem, Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., 2013.

[4] *Atomerőmű Tűzoltóság, ATOMIX Kft. Tűzoltási és Kárelhárítási Szakágazat, Szakmai Ismeretek* Oktatási anyag, ATOMIX at-me-6.2.2.-11-v2: *Atomerőműves rendszerek*, 2012. 08. 01.

[5] RADNÓTI K., KIRÁLY M.: Az atomenergiáról egyszerűen: az atomerőművek működése, típusaik és jövőjük. *Nukleon*, VIII 177 (2015). 1-13.oldal.

[6] PÓR G.: *Atomenergetikai alapismeretek – Atomerőművek generációi.* Budapest: Edutus Főiskola, 2012. www.tankonyvtar.hu/hu/tartalom/tamop412A/2010-0017_61_atomenergetikai_alapismeretek/ch01s03.html (A letöltés dátuma: 2017. 10. 27.)

[7] CSOM GY.: Atomerőművek. Magyar Atomfórum Egyesület, Budapest 2004.

[8] HANUSOVSZKY L.: Atomreaktorok előadás http://atomfizika.elte.hu/magreszfiz/hanusovszkylivia_atomreaktorok.pdf (A letöltés dátuma: 2017.10.27.)1999. évi LXXVI. törvény a szerzői jogról

[9] RÁCZ E.: *Nukleáris Erőművek előadás sorozat, 6. előadás: Atomreaktorok generációi* http://uni-obuda.hu/users/racz.ervin/NE_n_1_Eloadas.pdf (A letöltés dátuma: 2017.10.27.)

[10] NÉMET B.: *Nukleáris energetika előadás sorozat, 7. előadás: Harmadik generációs atomerőművek, a paksi atomerőmű bővítése (Paks-II),* Pécs 2015. http://www.physics.ttk.pte.hu/pages/munkatarsak/nemetb/Nucl-En-7_PaksII.pdf (A letöltés dátuma: 2017.10.30.)

[11] *Nuclear Safety & Security - IAEA Safety Standards* http://www-ns.iaea.org/standards/ (A letöltés dátuma: 2017.10.27.)

[12] CACUCI, D. G.: *Handbook of Nuclear Engineering.* Springer Science+Business Media LLC, New York 2010.

[13] *Iter.org: What is a Tokamak*? https://www.iter.org/mach/Tokamak (A letöltés dátuma: 2017.10.26.)

[14] *Atomenergia info: Hazai és nemzetközi energetikai helyzetkép - Fokozódó hazai kiszolgáltatottság* http://atomenergiainfo.hu/magyar-atomenergetika/hazai-es-nemzetkozi-energetikai-helyzetkep (A letöltés dátuma: 2017.04.01.)

[15] *MVM Paksi Atomerőmű Zrt, Atomerőmű Tűzoltóság, ATOMIX Kft. Tűzoltási és Kárelhárítási Szakágazat, Szakmai Ismeretek Oktatási anyag*, ATOMIX at-me-6.2.2.-11-v2: Atomerőműves rendszerek, Paks 2012. 08. 01.

[16] *MVM PA Zrt. MSSZ 18. verzió* Az MVM Paksi Atomerőmű Zrt. *Munkahelyi Sugárvédelmi Szabályzata*, MSSZ_V18, érvényes: 2017.10.02-től

[17] *The VVER today: Evolution, Design, Safety – State Atomic Energy Corporation ROSATOM* http://www.rosatom.ru/upload/iblock/0be/0be1220af25741375138ecd1afb18743.pdf (A letöltés dátuma: 2018.03.03.)

[18] *Safety of Nuclear Power Reactors World Nuclear Association – Energy For Sustainable Development,* 2003. http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/safety-of-nuclear-power-reactors.aspx (A letöltés dátuma: 2017.10.30.)

[19] RÉFY D.: *„Mai fúziós kísérleti berendezések”*. Plazma magfúziós erőmű cikk (A letöltés dátuma: 2018.03.26.) http://magfuzio.hu/tanulmanyok/mai-fuzios-kiserleti-berendezesek/

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

ERDŐTŰZOLTÁS TÁMOGATÁSA MŰSZAKI MEGOLDÁSOKKAL

TECHNICAL METHODS SUPPORTING FOREST FIRE SUPPRESSION

BODNÁR László; KOMJÁTHY László

(ORCID: 0000-0001-9196-8030); (ORCID: 0000-0003-3167-692X)

bodnar.laszlo@uni-nke.hu; komjathy.laszlo@uni-nke.hu

Absztrakt

*Az erdőtüzek olyan elemi csapások, amelyek egyre jelentősebb kihívások elé állítják a hivatásos tűzoltóságokat. A globális éghajlatváltozás hatására hazai és nemzetközi szinten is megnövekedett az erdőtüzek átlagos száma. Az ilyen tűzesetek során nem csak súlyos károk,de jelentős tűzoltási költségek is keletkeznek, ezért erre a problémára mind a megelőző tűzvédelemnek, mind az aktív tűzoltásnak megoldásokat kellene találnia. A cikk az erdőtüzek oltását elősegítő műszaki megoldásokat mutat be hazai és nemzetközi példákon keresztül – elsősorban mesterséges víznyerőhelyek kialakításának lehetőségeit és módjait – amelyek bizonyos szempontból megelőző tevékenységként is értelmezhetők. A cikk eredményeként megfogalmazhatók olyan erdőtűzvédelmi módszerek, amelyek hatékony segítséget nyújthatnak mind a megelőző tűzvédelem tervezéséhez, mind a beavatkozói állományhatékonyabb tűzoltásához. Ennek segítségével a tűzoltás költségei csökkenthetők, amivel nemzetgazdasági szinten is jelentős megtakarítást le*het elérni.

Kulcsszavak: *erdőtűz, tűzmegelőzés, vegetáció, víznyerőhely*

Abstract

Forest fires are major challenges for the professional firefighters. As a result of global climate change, the average number of the forest fires has increased all over the world.These forest fires lead to significant damages and firefighting costs, so the problem needs a solution from the fire prevention and from the operation sector. This paper presents solutions of the two sectors through Hungarian and international examples. Hungarian and international technical solutions are presented to prevent forest fires and making the operation more effective, mainly in connection with the development of artificial water resources. As a result of the paper forest fire prevention methods can determine, which can effectively assist the intervening forces in the effective firefighting. By doing so, fire costs can be reduced, which means more savings to the economy.

Keywords*: forest fire, fire prevention, vegetation, water source*

A kézirat benyújtásának dátuma (Date of the submission): 2018.04.15
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.12.

BEVEZETÉS

A kiterjedt erdőtüzek olyan természeti katasztrófák, amelyek egyre jelentősebb szerepet kapnak a katasztrófavédelemben. Ennek oka, hogy a katasztrófa számos esetben nem csak az anyagi javakat pusztítja, de akár az emberi életet is veszélyeztetheti. Az erdőtüzek elleni küzdelem két irányból is megközelíthető. Az egyik, a megelőző tűzvédelem, a másik az aktív tűzoltás, vagy mentő tűzvédelem. A nagy kiterjedésű erdőtüzek során jelentős erdészeti kárral és magas oltási költséggel is számolni kell, amelyet számos hazai szakirodalom is feldolgozott.[1] [2] [3] Ezek alapján az erdőtűzoltás megelőzésére, illetve a hatékonyabb tűzoltás feltételeinek megteremtésére egyre nagyobb hangsúlyt célszerű fektetni. Felmerül a kérdés, hogy az erdőtüzek megelőzésének milyen módszerei vannak, és hogy ezek a módszerek mennyire nevezhetők hatékonynak. Emellett további kérdést vet fel az is, hogy a nemzetközi szinten már bevált megelőzési módszerek milyen formában kerültek már alkalmazásra, illetve, hogy azok megvalósítása célszerű lehet-e hazánkban is.

A szerzők célja, hogy bemutassák az erdőtűz megelőzéssel kapcsolatos hazai és nemzetközimegelőző tűzvédelmi megoldások oltást támogató műszaki lehetőségeit. A cikk a szerzők egy korábbi kutatómunkájának folytatása; abban az erdőtüzek tovább terjedésének megakadályozását elősegítő tűzpászták és erdő átalakításoklehetőségeivel foglalkoztak, most a tűzmegelőzést, oltást elősegítő műszaki megoldásokat mutatják be, elsősorban a mesterséges víznyerőhelyek létesítése kapcsán. A cikk módszertani háttere a témakört érintő legfontosabb hazai és a nemzetközi szakirodalom részletes tanulmányozása és elemzése. Emellett a szerzők hosszabb-rövidebb konzultációkat folytattak a téma szakértőivel, illetve megtekintettek egy olyan erdőtűzoltási gyakorlatot is, ahol a víznyerő helyek alkalmazásával lehetőségei kiemelt szerepet kaptak. A szerzők feltételezése alapján a mesterséges víznyerőhelyek létesítésével hatékonyabbá válhat a beavatkozók részéről történő tűzoltási tevékenység, amivel nemzetgazdasági szinten nagyobb megmentett értékkel és kevesebb tűzoltásra fordított kiadással számolhatunk.

ERDŐTŰZ MEGELŐZÉS MŰSZAKI MEGOLDÁSAI

Mivel az erdőtüzek kialakulását leginkább az adott országra jellemző éghajlat, valamint az emberi gondatlanság befolyásolja,[4] ezért elengedhetetlen a tűzmegelőzést segítő különböző intézkedések és megoldási lehetőségek előtérbe helyezése. Az erdőtűz megelőzést nem csak erdészeti, hanem műszaki oldalról is meg lehet közelíteni. A fejezet speciálisan német és magyar példákon keresztül igyekszik bemutatni a legjellemzőbb műszaki megoldásokat a megelőző tűzvédelem területén.

Mesterséges vízszerzési pontok

Az erdőtűzoltás egyik legnagyobb és legnehezebb logisztikai háttérfeladata az oltóanyag szállítása. Az erdő, mint vízhiányos terület jelentős mennyiségű oltóanyagot igényel. Az oltóanyag szállítása számos esetben igen nagy távolságból történik, ez pedig megnöveli a tűzoltás költségeit, de csökkenti a beavatkozás hatékonyságát. [3] Mivel az erdőtűzoltás alapvető oltóanyaga a víz, ezért rendkívül fontos, hogy a tűzoltás során megfelelő mennyiségű vízkészlet álljon rendelkezésre. A vízszállító fecskendők kapacitása kevés egy erdőtűz eloltásához. Ebben az esetben kerül sor vízszállításra. Ezt egy erdőben, mint vízhiányos területen igen nehéz megvalósítani. Ebben az esetben az erdőhöz közeli települések ún. tűzivíz tározói, vagy az erdőben található nyílt vízforrások nyújthatnak segítséget. Mivel a folyamatos ellátást biztosító összefüggő vízkészlet a tűzoltóságnak és az erdészetnek is érdeke, ezért nemzetközi szinten számos példát találunk arra, hogy (például Németországban) létrehoznak mesterséges oltóvíz nyerésre szolgáló vízellátási pontokat. A vízellátási

pontokkal szemben támasztott követelmények között szerepel az egyszerű és gyors megközelíthetőség, valamint a terület jól látható megjelölése is. [5]

A mesterséges vízszerzési helyek felállításával egyrészt csökkenthető a vízhiányos területek száma, másrészt a vízszállító fecskendők által megtett ingázási útvonal is lerövidül. Ha a vízszerzési pontot úgy alakítják ki, hogy a terület helikopterrel, vagy adott esetben tűzoltásra alkalmas merevszárnyú repülőgéppel is megközelíthető, abban az esetben a légi tűzoltás logisztikai háttérfeladatai is könnyebbé válnak, erre pedig már hazánkban is van igény.[6]

1 ábra Egy mesterséges víznyerőhely Németországban. Készítette: N. Kessner.

A mesterséges vízszerzési pontok is több kategóriába sorolhatók. A legáltalánosabbak ezek közül a mesterséges víztározók, amelyek jelentős vízkapacitással rendelkeznek. Természetesen megnevezhetők ezen felül egyéb vízszerzési pontok is. Ilyen lehet többek között egy mély, nagy vízhozamú kút, egy földalatti víztartály, vagy egy erdőbe bevezetett vízvezeték rendszer is. Ezek a megoldások elősegíthetik a vízhiány pótlását, viszont működőképességükről és karbantartásukról folyamatosan gondoskodni kell. [5]

Magyarországon a 41/2014. (IV.8) VM támogatási rendelet keretein belül erdővédelmi létesítmények létrehozására nyíltlehetőség, úgymint víznyerőhelyek kialakítása. [7] Erdőtüzek oltásnál fontos, hogy megfelelő mennyiségű oltóvíz álljon a tűzoltók rendelkezésére. Tekintettel arra, hogy az erdőben a tűzivíz vezetékes hálózatának kiépítése ökológiai és ökonómiai szempontból is korlátokba ütközhet, ezért abban az esetben, ha nincs megfelelő mennyiségű természetes nyílt vízforrás a nagykiterjedésű, összefüggő veszélyeztetett területen, szükséges lehet mesterséges víztározó kapacitások kialakítása. [7]

Víznyerőhelyek létesítése

A víznyerő helyek megtervezésénél az alábbi feltételeket kell figyelembe venni. A víznyerő helyet, mint erdészeti létesítményt engedélyeztetni kell az erdészeti hatóságnál, valamint a létesítéséhez építési engedély valamint vízjogi engedély is szükséges! Víznyerőhely létesítésre támogatás kizárólag a nagy, illetve a közepes mértékben erdőtűzveszélyes megyékben vehető igénybe úgy, mint:

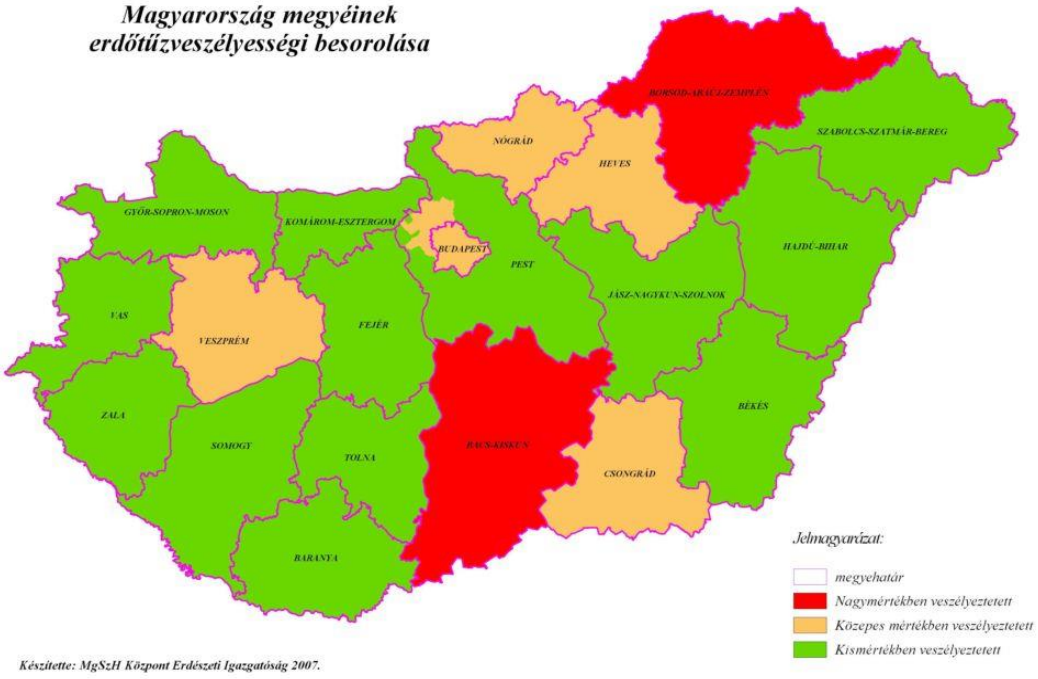
- Bács-Kiskun,
- Borsod-Abaúj-Zemplén,
- Veszprém,
- Heves,
- Nógrád,
- Csongrád,
- Budapest főváros,
- Pest megye agglomerációs része

Az erdőtűzvédelmi tervben fel kell tüntetni a létesítendő víznyerő hely pontos helyét, műszaki paramétereit, valamint a védendő terület lehatárolását és létesítés okát. Az erdőtűzvédelmi terv térképi mellékletén fel kell tüntetni a víznyerő hely által védett, térben közel összefüggő területet és fel kell sorolni az oda eső nagymértékben és közepes mértékben tűzveszélyes erdőrészleteket. A támogatási rendeletben megjelölt, az egyes víznyerő hely típusokhoz tartozó minimális védendő terület nagyságot a nagymértékben és közepes mértékben tűzveszélyes erdőrészleteknek kell elérni, de természetesen a védett területre eshetnek kismértékben tűzveszélyes erdőterületek is. Ezek viszont nem számítanak bele a minimálisan lefedendő területbe. Abban az esetben, ha több erdőgazdálkodó területére esik a védendő terület, az erdőgazdálkodóknak megállapodást kell kötniük a víznyerő hely használatáról. [7]

A természetes vízszerzési pontok nem minden esetben elegendőek vagy elérhetőek a tűzoltó erők számára, ezért szükség van mesterséges víztározók kialakítására. Ennek a megoldásnak a segítségével megoldódhat a tűzoltás egyik legsúlyosabb logisztikai problémája. A vízszerzési pontok kialakításánál érdemes még megjegyezni, hogy megvalósításuk esetén gondolni kell a hely megközelíthetőségére is. Fontos, hogy a terület megfelelő nagyságú legyen és egy tűzoltó fecskendő közlekedési igényeinek eleget tegyen. A szerzők 2017 tavaszán részt vettek egy erdőtűzoltási gyakorlaton, ahol hivatásos tűzoltók véleményét kérték ki a víznyerőhelyek létesítésével kapcsolatban. A konzultáció során a tűzoltók alátámasztották az erdőtüzek oltása során felmerülő logisztikai problémákat, illetve a vízhiány jelentőségét. A hatékonyabb tűzoltás érdekében támogatják a mesterséges víznyerőhelyek létesítését, azonban fontosnak tartják megemlíteni, hogy ezek elhelyezését célszerű lenne az adott erdőterület szélén, vagy tűzpászta közelében megvalósítani. Ennek oka, hogy ha a víztározók az erdőterület közepén kerülnek elhelyezésre, abban az esetben a vízszállító gépjárművel problémát jelentene a megközelítés, valamint a megfordulás sikeressége. Ez hátráltatná a tűzoltás hatékonyságát.

ERDŐTŰZVESZÉLY MAGYARORSZÁGON

A mesterséges víznyerőhelyek vizsgálata után, fontos bemutatni Magyarország erdőtűz veszélyeztetettségét, annak érdekében, hogy a megoldási lehetőség integrálására javaslatot lehessen tenni. Az Európai Unió a kötelezi a tagországokat, hogy közigazgatási területüket legalább megyei szinten is sorolják különböző tűzveszélyességi osztályokba. A besorolás tényezői közé tartozik az adott megye erdő és vegetáció típusa, az erdőtűz statisztikai adatok, illetve a jellemző időjárási tényezők. Magyarországon az erdőterületek tűzkockázati besorolását a katasztrófavédelem, valamint az erdészeti hatóság közösen végezte el. A besorolás elkészítésekor figyelembe lett véve az erdőgazdálkodók által készített erdőtervben feltűntetett faállományok különböző paraméterei is. Ahhoz, hogy egy jó minőségű tűzkockázati térkép elkészülhessen, kiemelten fontos tűzmegelőzési és tűzoltási aspektusból is értékelni az erdőterületen lévő biomasszát. Ez gyakran változatos képet mutathat, hiszen befolyással van rá az éghető biomassza mennyisége, alakja, nedvességtartalma, a terület domborzata, illetve a területre jellemző időjárási viszonyok is. A 2. számú ábra a hazaibiomassza tűzveszélyességi besorolását szemlélteti az egyes megyékben.



2. ábra Erdeink tűzveszélyességi besorolása megyénként.
Készítette: MGHSZ Központi Erdészeti Igazgatóság. Forrás: [8]

Látható hogy a legmagasabb, tehát a nagymértékben veszélyeztetett megyék közé tartozik, Borsod-Abaúj-Zemplén és Bács- Kiskun megye. Ezeken a területeken nagy intenzitású égés esetén – különösen az alföldi fenyőerdőkben – koronatűzzé is fejlődhetnek a talaj menti tüzek. A fent említett megyékben ezen felül az erdősültség is magas, ezért a szerzők javasolják elsősorban ebben a két megyében kivitelezni, vagy adott esetben tovább fejleszteni a fent említett megelőző tűzvédelmi módszert, hiszen a víznyerőhelyekhez hasonló műszaki megoldások mind hozzájárulhatnak a hatékonyabb tűzoltás megvalósításához. A megoldás nem csak az erdészeti, hanem a beavatkozói oldal kapcsán is hatékonyan működne, hiszen hatással lenne a tűzoltás vezetői döntéshozatalra [9] [10] valamint a beavatkozói biztonságra is. [11]

Bács-Kiskun megye kapcsán érdemes még megjegyezni, hogy a nagymértékben tűzveszélyes biomassza miatt az erdészet már megkezdte a tűzpászta rendszer kiépítését. Ez azért is fontos, mert a megyében korábban számos nagy kiterjedésű erdőtűz keletkezett, amelyek eloltása több napot vett igénybe. (Kunfehértó 2007, Bugac 2012) A 2012-es Bugaci ősborókás területén keletkezett vegetációtűzben a fokozottan védett természeti területen visszafordíthatatlan károk keletkeztek. Az ilyen és ehhez hasonló nagy kiterjedésű tűzesetek megelőzése érdekében kezdték meg a tűzpászta rendszer kiépítését, amely a jövőben elősegítheti az erdőtüzek megelőzésének egyes célkitűzéseinek megvalósulását.

Az erdőtüzek okainak megértése kiemelt jelentőségű az erdőtűzmegelőzési tevékenység, valamint a környezet és lakosság védelmi intézkedések megtervezésében. Hazánkban, az éghajlati sajátosságok valamint a biomassza összetétel miatta természetes úton keletkező erdőtüzek, aránya alig egy százalék. Ez a nyári időszakokban jellemző olyan zivatar esetén, amelynél nagyobb villámaktivitás tapasztalható csapadék nélkül, vagy elenyésző csapadékkal. Erre az időszakra már jellemző a vegetáció kizöldülése, így rendszerint aszályosabb években, az alföldi területen fordulnak elő ilyen típusú tüzek. Sajnos azonban a tüzek többsége emberi gondatlanság vagy szándékosság következménye. [8]

A tűzveszélyes időszakok előrejelzése, a tűz korai észlelése, a tűzoltási tevékenység támogatása informatikai rendszerekkel komplex feladat, amely több szakterület, a felelős szervezetek, a földhasználók átgondolt és folyamatos együttműködését igényli.

KÖVETKEZTETÉSEK

A cikk célja az erdőtűz megelőzéssel kapcsolatos hazai és nemzetközimegoldási lehetőségek bemutatása volt. A részletes szakirodalom tanulmányozás segítségével a szerzők bemutatták a tűzmegelőzést segítő műszaki megoldásokat különös tekintettel a mesterséges víznyerőhelyek létesítésére. Egyes ilyen műszaki és erdészeti megoldások Magyarországon még kevésbé elterjedtek, azonban alkalmazásuk nemzetközi szinten hatékonynak tekinthető, ezért a módszerek használatára és további támogatására tettek a szerzők javaslatot. A megoldási lehetőségek rendszeresítését elsősorban az erdőtüzek által nagymértékben veszélyeztetett megyékben javasolták kezdeni. A cikk megírásakor a szerzők azt feltételezték, hogy az egyes tűzmegelőzési megoldási lehetőségek alkalmazásával még hatékonyabbá válhat a beavatkozók részéről történő tűzoltási tevékenység, ez pedig nemzetgazdasági szinten jelentős megtakarítást eredményezhet. A vizsgálat minden esetben rávilágított a hatékonyabb tűzoltás vagy tűzmegelőzés megvalósításának lehetőségére. A vegyes típusú vegetáció ültetésével és a tűzpászta rendszer kialakításával csökken a tűz terjedési sebessége, ezáltal pedig hatékonyabban megvalósul a tűz körülhatárolása, lefeketítése majd eloltása. A mesterséges vízszerzési pontok létesítésével viszont lecsökkenthetők a tűzoltás során felmerülő logisztikai nehézségek, ami szintén hatékonyabb tűzoltást eredményezhet.

Összességében megállapítható, hogy hazánkban is vannak már hatékony tűzmegelőzési módszerek az erdőtüzek kapcsán, azonban nemzetközi szinten ezek a módszerek bizonyos esetben fejlettebbek, jobban ki vannak dolgozva. Ennek eredményeként fontos és hasznos ezeknek a megoldási lehetőségeknek az ismerete, hiszen a szerzők által végzett kutatás bebizonyította, hogy a legtöbb megoldási lehetőségalkalmazhatóMagyarországon is.

FELHASZNÁLT IRODALOM

[1] RESTÁS Á: *Alégi tűzoltáshatékonyságának közgazdasági megközelítése*. Repüléstudományi Közlemények,XXIV 2 (2012), 805-813. o.

[2] KÓS GY. KOMJÁTHY L: *Erdőtüzek helikopteres oltása*.Repüléstudományi közlemények, 24 2 (2012) 471- 482.o

[3] BODNÁR L: *Az erdőtüzek oltásának logisztikai problémái valós példák alapján*. Bolyai Szemle 24 4 (2015) 86-99.o

[4] RESTÁS Á: *The effects of global climate change on fire service: Human resource view*. Procedia Engineering, 211 (2018), pp. 1-7.

[5] KAULFUß S:*WaldbaulicheMaßnahmenzur Waldbrandvorbeugung.*

http://www.waldwissen.net/waldwirtschaft/schaden/brand/fva_waldbrand_wb4/index_DE letöltve: 2017.04.08.

[6] KOMJÁTHY L., KOZÁK A: *Helikopteres tűzoltás Szabolcs-Szatmár-Bereg megyében.* Magyar rendészet, XIII. különszám. (2013), 75.-83.o ISSN 1586-2895

[7] Tájékoztatóaz erdőterületeket érintő tűzkárok megelőzéséhez nyújtandó támogatás igénybevételének feltételeiről szóló 41/2014. (IV. 8.) VM rendelethezkapcsolódó erdőtűzmegelőzési és hatósági tudnivalókról.

[8] NAGY D: *Az erdőtüzek megelőzési és oltástechnológiai lehetőségeinek vizsgálata*; PhD értekezés, Nyugat-magyarországi Egyetem, Sopron, 2008.

[9] RESTÁS Á: *Pszichológia a tűz frontvonalában*. Védelem Tudomány, 1 3 (2016), 46-56.o

[10] RÁCZ S: *A tűzoltói beavatkozások súlyponti erőmegosztásának vizsgálata*. Hadmérnök. 12:(KÖFOP) pp. 92-107. (2017)

[11] PÁNTYA P: *Lehetőségek a katasztrófavédelmi, tűzoltói beavatkozó biztonság növelésére.* In: Pokorádi László: Műszaki Tudomány az Észak-kelet Magyarországi Régióban 2014., pp. 214-222., (ISBN:978-963-508-752-5)

HADMÉRNÖK

XII. Évfolyam 3. szám – 2018. szeptember

AZ IVÓVÍZKEZELÉSSEL KAPCSOLATOS PROBLÉMAKÖR HAZÁNKBAN

THE DIFFICULTY OF DRINKING WATER TREATMENT IN OUR COUNTRY

CSŐSZ László

(ORCID: 0000-0003-1662-5139)

csosz.laszlo@uni-nke.hu

Absztrakt

Ahogy az emberi szervezet jelentős részét a víz teszi ki, úgy Földünk felszínének közel háromnegyedét is víz borítja. A víz a földi élet, a természet, illetve az emberi társadalom számára is létfontosságú, nélkülözhetetlen természeti javak egyike. A társadalom egyik működési alapfeltétele a vízzel való gazdálkodás és annak biztosítása. A víz iránti igény a népesség növekedésével időről időre folyamatosan emelkedett. Becslések alapján a fejlett országok közel háromszor annyi vizet használnak, mint amennyit a természetes körforgás biztosítani képes. Emiatt fokozódó mértékben hasznosítják például a rétegvíz tartalékokat, ami a talajvíz szintjének nem kívánatos csökkenésével jár, de egyre nagyobb mértékben kell a vízhiányt szennyezett felszíni vizekből költséges tisztítással fedezni. Vajon hazánkban az ivóvíz-ellátó rendszer hozzá tud járulni hatékonyan a lakosság biztonságos ivóvízellátásához?

Kulcsszavak: *közművek, vízgazdálkodás, ivóvízkezelés, ivóvízszenyezés*

Abstract

As significant part of human organism is constituted by water, three-quarter of the surface of the Earth is covered also by water. Water is of vital importance for life on Earth, nature and human society, it is one of the essential natural goods. The basic condition of the operation of a society is water management and the assurance thereof. The demand for water has continuously increased from time to time with the increase of the population. Based on estimations the developed countries use almost three-times more water than the natural circulation is able to provide. Due to this for example layer water reserves are utilized to an increased extent, which contributes to the unwanted reduction of soil water level, however lack of water shall be covered with expensive cleaning of contaminated surface waters to a great extent. Can the drinking-water supply system in our country effectively contribute to the safe drinking-water supply of the population?

Keywords: *public utilities, water management, water treatment, piped water pollution*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.18.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.05.

BEVEZETÉS

A közműves vízellátás és csatornázás fejlődése során több tényező is volt, amely a vízi közművek fejlődésére ösztönző hatást gyakorolt. Annak ellenére, hogy a közműves vízellátás igénye igen régi, első nyomai már a Római Birodalomban is fellelhetőek voltak, hazánkban a közműves vízellátási és csatornázási munkákat csak az 1867. évi kiegyezést követő, felgyorsult kapitalista fejlődés indította el. [1] Az első víz- és csatornaművek szinte kizárólag a nagy történelmi múltú városokban épültek ki, mert a kapitalizmus térhódítása egyben az ásványi kincsekben is gazdag dunántúli és északi városok fejlődésének felgyorsulásával járt. Budapest mellett a Pécs, Szombathely, Sopron és Győr öregbítette kulturális, illetve közigazgatási pozícióját és kezdte meg vízi közművei kiépítését. A közművesítés iránti igényeket a polgárság életkörülményeinek, kulturális színvonalának a növekedése keltette fel, a reális kielégítési lehetőségeket viszont a települések beépítési módja határozta meg. A zárt beépítettségű, többszintes beépítésű városokban a víz- és csatornahálózat iránti igény sürgetőbb volt, mint a falusias vagy mezőgazdasági jellegű településeken. A természeti adottságok is befolyásolták a vezetékes vízellátás alakulását. A kedvező vízszerzési lehetőségek ösztönzően és előnyösen éreztették hatásukat, mivel csökkentették a szükséges költségeket, amelyeket jórészt a városi önkormányzatoknak kellett saját erőforrásukból előteremteniük. Ezt a viszonylag lassú és korlátozott fejlődést megállította az első világháború. Lényeges fejlődésről ezután nem beszélhetünk. A két világháború között alig épültek víz és csatornaművek. A vízellátás szervezete elszakadt az egységes vízügyi szolgálattól és „vándorolt" a különböző minisztériumok között. A második világháború harci cselekményei során számos város víz- és csatornaműve megrongálódott, tönkrement. A második világháborút követő helyreállítások után az ösztönző társadalmi és gazdasági tényezők hatására egyre növekvő ütemben indult meg a vízi közművek fejlődése. Az ezt követő időszakban a fejlesztéseket három jól elkülöníthető szakaszra oszthatjuk. [2] Az első a szocialista iparosítás, a nehézipar elsődleges fejlesztése által meghatározott fejlesztés (1948-1957), amely a városi vízművek kapacitásának növelését elsősorban a vízvezetéki hálózatról kielégítendő üzemi és szociális vízigények biztosításától tette függővé. A lakossági igények kielégítése főként a bányász- és munkástelepek, a régi hálózatoknak a munkások által lakott kerületekre való kiterjesztésével jutott érvényre. A második szakasz a már egységes vízügyi szolgálat keretében az életszínvonal, a lakáskultúra és az ipar összehangolt kielégítésének a megindítása, a vízigényeket a vízkészletekkel térben és időben összehangoló regionális elemek bevezetésével. Ez a tizenkét év (1958-1970) teremtette meg a további dinamikus fejlesztés alapjait képző szervezeti, műszaki és pénzügyi bázist. Ezen éveket nevezhetjük a magyar vízellátás és csatornázás eddigi legdinamikusabb korszakának. A harmadik szakaszra (1971-től napjainkig) a városokban a magas- és toronyépületekből kiképzett, melegvíz szolgáltatással és távfűtéssel ellátott új lakótelepek építésével megnövekedett vízigények, az ipar fokozódó kívánalmainak kielégítésére a vízművek fejlesztése, a közösségi vízművek tömeges építésének folytatása, a városi és üdülőhelyi közcsatornázás és a szennyvíztisztító telepek építési ütemének fokozódása jellemző.

VÍZGAZDÁLKODÁS

A vízgazdálkodás több szempont szerint osztható részekre, illetve szakterületekre. A leggyakrabban alkalmazott felosztás alapján két fő területet különböztetünk meg. Ez a két szakterület a területi vízgazdálkodás és a települési vízgazdálkodás. [3] A területi vízgazdálkodás fő feladata vizeink számbavétele, nyilvántartása, a hidrológiai folyamatok mérése, illetve a vizekkel való ésszerű és célszerű gazdálkodás megvalósítása. Emiatt hatósági szerepet is ellát. A területi vízgazdálkodás foglalkozik a vízkészletekkel, a vízgyűjtő gazdálkodás komplex feladatival, folyó- és tószabályozással, illetve ár- és belvízvédelemmel.

A települési vízgazdálkodási tevékenység érinti leginkább a társadalmat, hiszen az emberek otthona, munkahelye a településeken található. A települési vízgazdálkodás foglalkozik az ivó- és ipari vizek beszerzésével, a vízbázisok védelmével, üzemeltetésével és fenntartásával, a lakossági, ipari és a mezőgazdasági vízigények kielégítésével. Fő feladata a felhasználók számára folyamatosan megfelelő mennyiségű, minőségű víz biztosítása. Ennek érdekében gondoskodik a vizek beszerzéséről, megfelelő mértékű tisztításáról, elosztásáról, tárolásáról, a kapcsolódó rendszerek üzemeltetéséről, illetve fenntartásáról. Másik fő feladata a vízfelhasználás során keletkezett szennyvíz összegyűjtése, majd pedig azok leggyorsabb, legbiztonságosabb módon a tisztító telepre történő elvezetése, ahol pedig olyan mértékben kell megtisztítani, hogy az a környezetbe visszaereszthető legyen, hiszen előbb-utóbb ez a víz visszajut a vízbázisokba jut.

Települési vízgazdálkodás

A vízellátási folyamat első lépése magának a víznek a beszerzése. Azt a területet, amelyből vízellátási céllal tartósan, fenntartható módon a vízbeszerzés megvalósítható vízbázisnak nevezzük. [4] A vízbázisokba a vízhidrológiai folyamatok során jut el a víz. Vízbázisaink és a vízbeszerzési létesítmények is igen sokrétűek. Karsztvízbázisaink a Balaton északi partján és Kincsesbánya térségében Rákhegyen találhatóak. Legjelentősebb a nyirádi vízbázis, ahol nagy mélységű és nagy átmérőjű akna kutak segítségével termelik ki a vizet. A rétegvíz két vízzáró réteg között összegyűlt víztömeg, melyek különböző mélységben találhatóak, megcsapolásuk létesítményei a fúrt kutak. Hazánkban ezek a leggyakoribb vízbeszerzési művek. Akár karsztvízről, akár rétegvízről beszélünk mindkét esetben előtörhetnek forrásként. A források vízellátási célú hasznosítását forrásfoglalási művekkel valósítják meg. Ennek több módja lehetséges, de lényeg, hogy legtöbbször a fakadó vizeket valamilyen gyűjtőaknába terelik, majd szivattyú segítségével juttatják vagy a hálózatba, vagy ha szükséges, akkor a megfelelő víztisztító egységbe. Forrásaink többsége szintén a Balaton északi partján található, de a Mecsekben is üzemeltetnek forrásfoglalásokat. A karsztvíz és a rétegvíz mellett, használnak olyan vízbeszerzési műveket is, melyek partiszűrésű vizet szolgáltatnak, ilyen például az Ercsi térségében, a Duna partján található kútsor, valamint a Mohács szigeten üzemelő kútsorok. Partiszűrésű víz azon folyószakaszok mentén alakul ki, ahol a meder anyaga kellő vastagú homokos kavics, mely természetes szűrőként viselkedve szűri meg a folyó vizét. A felszín alatti vízbázisok mellett a legjelentősebb feszíni vízbázisunk a Balaton, amelyre hat darab vízművet telepítettek. A Balaton, mivel felszíni víz, rendkívül sérülékeny vízbázis és élőhely egyben.

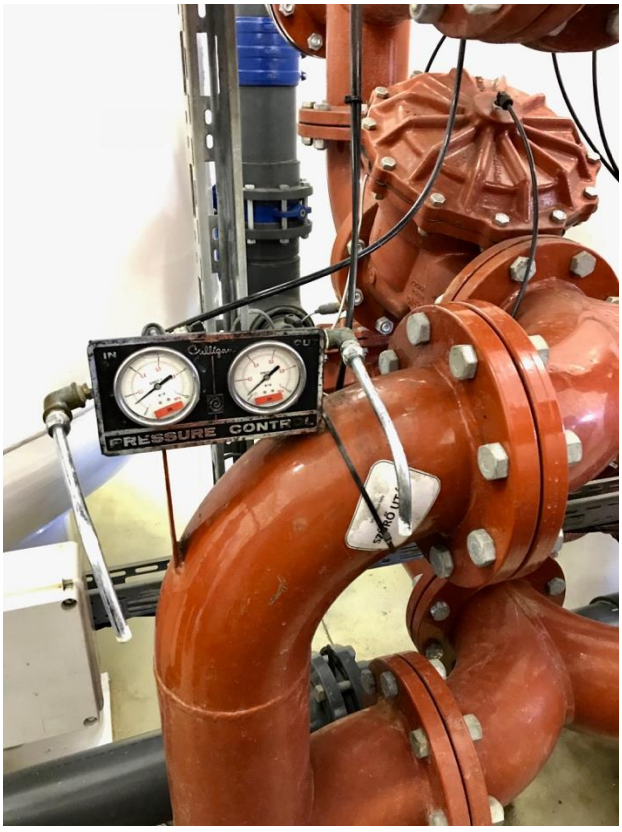
Az ivóvíz a legszigorúbban ellenőrzött élelmiszer. A vízbázisokból kitermelt vizeket különféle technológiák alkalmazásával teszik alkalmassá arra, hogy a fogyasztók számára a törvényben előírt minőségben kerüljenek. A vízből el kell távolítani a kórokozó mikroorganizmusokat, a mérgező anyagokat, a mikroszennyeződéseket, a zavarosságot okozó anyagokat, a szerves vegyületeket, valamint az íz- és a szagrontó anyagokat. Ahány vízbázis, annyi nyersvízminőség összetétel, annyiféle alkalmazandó technológia. A kiváló minőségű karsztvizeknél is kötelező a fertőtlenítés. Minden víztisztítási technológia alapfolyamatokból, illetve azok célszerű kombinációjából tevődik össze. Ilyen az oxidáció és a redukció, melyek célja, hogy valamely szennyezőt oldhatatlanná alakítsák, kevésbé toxikussá tegyék vagy fertőtlenítsék. Másik alapfolyamata a kémiai kicsapás, amely a vegyszeradagolással a szennyezőanyag oldhatatlanná alakítását jelenti. A következő ilyen folyamat az abszorpció, amely a gázok és oldott anyagok megkötése szilárd felületen. Leglátványosabbak a felszíni víztisztítás technológiái. A kitermelt víz az első technológiai lépcsőben levegőztetésnek van kitéve, melynek alapvető célja a vízben oldott gázok eltávolítása. A levegőztetés lehet surrantó, csatornás, csepegtetős vagy légbefúvásos. A következő lépés a derítés, amely két részből áll, a pelyhesítésből és az ülepítésből. Ezek célja a vízben lévő lebegő anyagok eltávolítása. A vízben

található anyagok a gravitáció hatására a tároló aljára ülepednek. Vannak azonban olyan kis méretű, szemmel alig látható lebegő anyagok melyek nem ülepednek le. A pelyhesítés során megfelelő mennyiségben derítő szereket adagolnak a vízhez, ami azt eredményezi, hogy ezek az apró anyagok összetapadnak, pelyheket képeznek, melyek már elég nagyok ahhoz, hogy saját tömegük miatt leülepedhessenek. A derítést követő lépés a szűrés. A szűrés történhet nyitott vagy zárt szűrőkön keresztül, célja a lebegőanyag tartalom további csökkentése. A szennyezőanyagok a szemcsékre tapadnak, a szemcsék közötti üregekben leülepednek. Szűrésnél a szemcsés közegen való áramlás hatására a víz elveszíti szilárdanyag tartalmát, a folyamat során csökken az időegység alatt átáramló vízmennyiség ezért meghatározott időközönként a szűrőket öblíteni kell. A szűrést követő, illetve minden technológia befejező lépése a fertőtlenítés. Feladata a vízben található mikroorganizmusok egyedszámának a csökkentése az érvényes előírásoknak megfelelő szintre, a kórokozó mikroorganizmus egyedszámnak nullának kell lennie, fontos, hogy az alkalmazott módszer kis mennyiségben legyen hatékony, de hatása hosszú távon a fogyasztó csapjáig érvényesüljön. A vízellátás következő művelete a víztermelés. Víztermelés alatt azokat a folyamatokat értjük, mely során a vízbázis kivett és előírt minőségűre tisztított fertőtlenített vizet, az elosztóvizet az útjára indítják. Szinte minden vízműtelepen található szolgálati medence, melyben a megtisztított víz tárolása történik. Ezekből a medencékből szivattyúk segítségével jut el a víz a különböző vízellátó rendszerekbe. Az immár ivóvízminőségű víz ezeken keresztül jut el a felhasználókhoz. A vezetékek funkciójuk szerint különböző anyagúak és átmérőjűek. Megkülönböztetünk például távvezetékeket, melyek több települést kötnek össze. A vízfelhasználás időbeni alakulása helytől, szokástól és egyéb körülményektől más és más. [5] A szivattyúzás és víztermelés azonban állandó. A fogyasztás és a szivattyúzás közti különbség kiegyenlítésére valók a tárolók. Ilyen tároló látható az 1. ábrán, amely a dombóvári vízműtelepen üzemel. Ha a vízfogyasztás nagyobb, mint amennyi a vízműből a hálózatba jut, akkor egy tároló ürül, hiszen a többlet vizet onnét kell pótolni. Ha a vízfogyasztás kisebb, mint amennyi víz a vízműből a hálózatba jut, akkor egy tároló töltődik. A tárolók ezen felül biztosítják a közel állandó hálózati nyomást is. A tárolók több szempont szerint csoportosíthatók. Egy hálózaton belül általában több tároló is található. Azok a gépházak, amelyekben a szivattyúk feladata a tárolók töltése, átemelő gépháznak, illetve átemelő szivattyúnak nevezzük. Vannak olyan nyomászónák, amelyek nem rendelkeznek tárolóval viszont az előírt nyomást itt is biztosítani szükséges. Ezt a feladatot látják el a nyomást fokozó gépházak. A nyomásfokozók beépített érzékelők segítségével elindulnak, ha a hálózati nyomás a meghatározott értékűre csökken, majd a megfelelő értékkor leállnak.

1. ábra A dombóvári vízműtelepen üzemelő tároló (Forrás: saját fotó)

A megfelelő minőségű és mennyiségű víz biztosítása egy összetett és bonyolult folyamat, melynek során különféle gépészeti és villamos berendezések segítségével üzemeltetik az e célt szolgáló létesítményeket. A folyamatelemek összehangolását a vízbeszerzés, tisztítás, elosztás és tárolás irányítását azok folyamatos ellenőrzését az üzemirányítás végzi. Üzemirányítás során ma már alapvetően távvezérléssel és távfelügyelettel dolgoznak a szakemberek. Az ilyen központokban napi 24 órás szolgálat folyik.

Nemzetközi és hazai viszonylatban egyaránt növekszik az igény a biztonságos ivóvíz iránt, ezért fontos, hogy az ivóvíz ne tartalmazzon egészségre káros mikroorganizmusokat, mérgező anyagokat, ugyan akkor az is lényeges szempont, hogy az ivóvíz tartalmazza a szervezet számára nélkülözhetetlen vegyületeket. Az emberiség számára a fertőzött víz szennyezettsége nagyságrendekkel nagyobb veszélyt jelent a levegő és a talaj szennyezettségével szemben. A vízgazdálkodást korszerű alapelvekre kell helyezni és a vízi közmű szolgáltatóknak az üzemeltetés biztonságára különös figyelmet kell fordítani. Ezzel egyidőben a laboratóriumoknak folyamatos és megbízható tájékoztatást kell adni a vízbázisok aktuális állapotáról, a működés biztonságosságáról és a víztisztítás hatásfokától. Mindezek alapján csak szigorú jogszabály által is rögzített minőségi ellenőrzés után mondható, hogy a víz alkalmas emberi fogyasztásra és felhasználásra. Az ellenőrzések gyakoriságát és spektrumát jogszabályok írják elő. Az akkreditált laborok végzik a fizikai, a kémiai, illetve a mikrobiológiai vizsgálatokat az ivóvíz hálózat számos mintavételi pontjáról vett mintákból. Ilyen mintavételi pont látható a 2. ábrán.



2. ábra Mintavételi pont a dombóvári vízműtelepen (Forrás: saját fotó)

A laborokban a minták a vonatkozó szabványoknak és előírásoknak megfelelő határidőn belül kerülnek feldolgozásra. A minőségellenőrzés egyik részét képezi az ivóvíz bakteriológiai vizsgálata, amely során speciális anyagok felhasználásával kimutatható azon baktériumok jelenléte, amelyek megbetegedést képesek okozni. Ezek a mikroorganizmusok természetes és

mesterséges úton egyaránt bejuthatnak az ivóvízbe. A minőségellenőrzés egy másik fontos része a fizikai és kémiai vizsgálatok elvégzése. Fizikai vízminősítés során a víz színváltozása, áttetszősége, a hőmérséklete, a lebegőanyagok szemcsemérete, valamint az áramlási viszonyok kerülnek megvizsgálásra. Kémiai vízminősítéssel a vizek vegyi összetétele kerül meghatározásra, vagyis az oldott anyagok mennyisége és minősége, valamint a lebegő és emulgeált anyagok minőségi és mennyiségi viszonyai. Ezen vizsgálat kiterjed többek között az oldott gázokra is.

SÉRÜLÉKENY VÍZBÁZISOK

Egyes gazdasági és társadalmi elemzések az ivóvíz kérdéskörét a jövő évtizedek vagy akár évszázadok fejlődésének egyik kulcstényezőjének tartják. [6] A vízbázisvédelem fogalma az utóbbi években a szakmai körökből egyre inkább bekerült a köztudatba. Ez leginkább annak köszönhető, hogy az ivóvízellátásra alkalmas vízkészletek jelentősége megnőtt szerte a világon. Bár a fogalom alatt nálunk sokan értik a vízkészletek általános értelemben vett védelmét, valójában ez a fogalom a vízkészletek egy szűkebb, meghatározott részének az általánosnál jóval fokozottabb védelmét jelenti.

A vízbázisvédelemnél két csoportot különböztethetünk meg a távlati vízbázisok csoportját és az üzemelő vízbázisok csoportját.

A távlati vízbázisok potenciális, jó vízadó adottságokkal rendelkező területek, amelyeken jelenleg még nem alakítottak ki víztermelő telepeket. Az ivóvízbázis-védelem célja az emberi tevékenységből származó szennyezések megelőzése, a természetes és jó vízminőség megőrzése. 1995-ben indult el az első kormányprogram az ivóvízellátást szolgáló sérülékeny környezetű üzemelő vízbázisok védelmére, védőterületek kijelölésére. [7] Az első vízbázisvédelmi célprogramok pedig 1997-ben indultak. Hazánkban a természeti adottságoknak megfelelően a közműves ivóvízellátás döntő mértékben, több mint 90 %-ban a felszín alatti vízkészletből történik. Ez az arány összhangban van az ENSZ Egészségügyi Világszervezete, a WHO önkormányzatok számára kiadott ajánlásával. Az ajánlás szerint, ahol erre lehetőség nyílik, a vízigényeket a felszín alatti vízkészletekből kell biztosítani, mivel ezek a vizek kevésbé érzékenyek a havária szerű szennyezésekre. Több nyugat-európai példa is van arra, hogy felszíni vizet, például folyóvizet előzetes tisztítás után mesterséges úton beszivárogtatnak a felszín alá, majd onnan termelik ki kutakkal mesterséges felszín alatti vízként. Nem hagyhatjuk figyelmen kívül, hogy a felszín alatti vízbázisok rehabilitációja egy szennyezést követően sokkal költségesebb és sokkal több időt vesz igénybe, mint a felszíni vizek esetében.

IVÓVIZEK ELSZENNYEZŐDÉSE

A felszíni vizek elszennyeződése mellett leginkább a felszín alatti vizek elszennyeződése jelenti a nagyobb veszélyt az ivóvízre. A vizet kitermelése, szállítása, illetve tárolása során is érhetik bakteriális fertőzések. A víz érintkezhet a levegővel, a levegőben lévő porokkal, vagy a csőtöréseknél föld kerülhet a vezetékbe. Ezért a vizet csírátlanítani, fertőtleníteni szükséges. A fertőtlenítés során olyan nagy mennyiségű fertőtlenítő anyagot kell adagolni, hogy a víz a fogyasztási pontokig csíramentes legyen. Háromféle fertőtlenítő anyag ismeretes, az UV, az ózon, illetve a klórgáz vizes oldata. [8] Ilyen UV fénnyel működő fertőtlenítő berendezés üzemel a dombóvári vízműtelepen is, amely a 3. ábrán látható.

3. ábra UV fertőtlenítő berendezés a dombóvári vízműtelepen (Forrás: saját fotó)

Az emberi tevékenységek akaratlanul is veszélyes és szennyező anyagokat juttatnak a felszín alatti vizekbe. Mivel egy vegyület gyakran hónapok vagy évek múlva jut a felszínről a talajvízbe, a víztartó rétegekben okozott kár talán csak évtizedek múlva derül ki. A világ számos részén csak most kezdik felfedezni azokat a szennyezéseket, amelyeket több évtizeddel ezelőtti szennyezések okoznak. Hazánkban erre az egyik legszemléletesebb példa az Abasáron 2013-ban bekövetkezett ivóvízszennyezés [9]. Abasár szomszédságában lévő Pipis-hegyen a ’80-as években bezárt ipari telep okozta a szennyezést. Az Abasárt ellátó kutak közelében anno működő diódagyárat nem a kellő körültekintéssel zárták be, környezettanulmányt nem készítettek a lehetséges szennyezésről. Az évek során a mérgező anyagok lassan leszivárogtak a talajban a vízbázisokig és elszennyezték azokat. Az abasári ivóvíz szerves vegyi anyaggal, halogénezett szénhidrogénnel szennyeződött el, és emberi fogyasztásra alkalmatlanná vált. A teljes ivóvíz hálózatot újra ki kellett építeni a területen. Az ivóvíz ellátásban egy másik jelentős probléma a jelentős nitráttartalom. Az 50-es évek óta a gazdák a többszörösére növelték a nitrogén tartalmú műtrágyák használatát a termelés növelése érdekében. A nagyobb mennyiségű anyagot azonban a növények nem tudják teljes mértékben felhasználni. A műtrágya egy jelentős része sokszor kárba vész, viszont a fel nem használt nitrát a vízzel keveredve keresztülszivárog a talajon a víztároló rétegbe.

KÖVETKEZTETÉSEK

Összességében elmondható, hogy hazánkban a vizek valóban jó minőségűek, a Duna például bőséges partiszűrésű vízzel lát el bennünket, illetve karszt- és rétegvizeink elegendőek és jó minőségűek. Vizeink csak „kisebb” utókezelésre szorulnak. Azonban a vízhiány, illetve a rossz minőségű ivóvíz számos olyan negatív kockázatot hordozhat magában, ami a hétköznapi, a lakosságközpontú felhasználhatóságát veszélyezteti. Ebből kifolyólag az ivóvizek használatát, illetve minőségi paramétereit és határértékeit, összhangban az Európai Uniós jogszabályokkal szükséges vizsgálni. Az ivóvíz analizáló laboratóriumok pedig ennek eleget téve vizsgálják ellenőrzik a vízmintákat, így biztosítva, hogy a fogyasztókhoz a megfelelő minőségű víz jusson el. A laboratóriumi módszerek közül vannak olyanok jól működő mérési módszerek, amelyek

teljesen megbízhatóan képesek kimutatni a különböző vizsgálat paramétereket, megállapítva, hogy történt-e határérték túllépés. A pontos laboratóriumi vizsgálati tevékenység mellett is elmondható azonban, hogy vannak olyan már meglévő vizsgálati módszerek, amelyek fejlesztésre és változtatásra szorulnak. Célszerű lenne esetlegesen további, új módszereket is alkalmazni. Ezen új módszerek és fejlesztések azonban munkaerőt, szakértelmet és legfőképpen anyagi hátteret igényelnek, amelyek kivitelezése hazánkban nem mindig lehetséges.

FELHASZNÁLT IRODALOM

[1] HORVÁTH I., LIGETVÁVRI F., MARJAI GY., SIMÁNDI P.: *Vízellátás és csatornázás*; Szent István Egyetem, Budapest 2011.

[2] BOZÓKY K.: *Vízellátás és csatornázás*; Tervezési segédlet, Tankönyvkiadó, Budapest 1974.

[3] PREGUN CS., JUHÁSZ CS.: *Vízminőségvédelem*; Debreceni Egyetem, Debrecen 2012. ISBN: 978-615-5138-34-8

[4] GAYER J.; LIGETVÁRI F.: *Települési vízgazdálkodás*; Környezetvédelmi és Vízügyi Minisztérium, Budapest 2007.

[5] SIMONFFY Z.: *Vízigények és vízkészletek*; Magyar Tudományos Akadémia, Budapest 202.

[6] KOVÁCS ZS., KÁRPÁTI Á.: *Ivóvíztisztítás és víztisztaságvédelem*; Pannon Egyetem, Veszprém 2013. ISBN: 978-615-5044-93-9

[7] 1995. évi LVII. *törvény a vízgazdálkodásról*

[8] BEREK T.: *A vízbiztonsági tervezés szerepe a fenntartható vízgazdálkodásban.* Műszaki Katonai Közlöny XXVI. évfolyam 2016. 2. szám. http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2016_2sz/mkk_2016_2sz.pdf (letöltve: 2018.03.01.)

[9] HEGEDŰS H.: *Az ivóvízbázisok, mint kritikus infrastruktúra elemek kijelölésével kapcsolatos problémák*. Társadalom és Honvédelem XIX évfolyam 2015/2. http://archiv.uni-nke.hu/uploads/media_items/tarsadalom-es-honvedelem-2015_-evi-2_-szam.original.pdf (letöltve: 2018.03.02.)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

CYTOGENETIC DETECTION TOOLS FOR EFFECTS OF IONIZING RADIATION ON HUMAN

IONIZÁLÓ SUGÁRZÁSOK EMBERRE GYAKOROLT HATÁSÁNAK CITOGENETIKUS VIZSGÁLATA

DELI Gábor

(ORCID: 0000-0003-4483-3138)

deli.gabor87@freemail.hu

Abstract

Everyday people are constantly exposed to a background dose of ionizing radiation which comes from the rocks and from outer space. Soldiers on mission could be exposed to ionizing radiation more frequently than it would be expected. In case of a terror attack, a radiological accident or industrial disaster people can receive much higher dose than in everyday life. People can get a dose even unperceived, as humans have no specialized sensing organ for ionizing radiation. Tumors can develop years after the irradiation due DNA damage caused by ionizing radiation. In cases when affected people didn't wear any personal dosimeter, the received dose can be estimated with different biodosimetry tools in order to decide about the appropriate medical treatment or even the compensation. In this article the author gives a short review about the recently used biodosimetry methods.

Keywords: *biodosimetry, micronucleus, chromosome aberrations, dicentrics.*

Absztrakt

Ionizáló sugárzásnak folyamatosan ki vagyunk téve, ez a háttérsugárzás elsősorban a kőzetekből és a világűrből származik. Ennek sokszorosát szenvedhetjük el katasztrófahelyzetben, például egy nukleáris baleset vagy támadás után. A Magyar Honvédség állománya nagyobb valószínűséggel kerülhet kapcsolatba ionizáló sugárzással, mint a civilek. Tekintve, hogy nincs az ionizáló sugárzás érzékelésére specializálódott érzékszervünk, a sugárzás észrevétlenül érhet minket. Az ionizáló sugárzás által kiváltott DNS károsító hatás következményeként évekkel a besugárzás után is keletkezhetnek a sérülteken daganatos megbetegedések. A személyi dozimétert nem viselő személyeknél a sugársérülés mértékét különböző biodozimetriai eljárásokkal tudjuk megbecsülni, így kiválasztható a megfelelő kezelés. Jelen közleményben a szerző ismerteti, majd röviden összehasonlítja ezeket az eljárásokat.

.

Kulcsszavak: *biodozimetria, mikronukleusz, kromoszóma aberráció, dicentrikus kromoszóma*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.22.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.11.

INTRODUCTION

Biodosimetry is a monitoring system which reveals whether the examined animal or human has been exposed to ionizing radiation or not and how much dose of radiation was received. Biodosimetry always gives an estimation, because each living organism always reacts to the ionizing radiation on his own way, but the huge amount of knowledge and experimental data accumulated during the last few decades helps us to assign the past radiation burden to the outcome.

Biodosimetry is a monitoring system which reveals whether the examined animal or human has been exposed to ionizing radiation or not and how much dose of radiation was received. Biodosimetry always gives an estimation, because each living organism always reacts to the ionizing radiation on his own way, but the huge amount of knowledge and experimental data accumulated during the last few decades helps us to assign the past radiation burden to the outcome.

As during the evolution there is no a single organ has specialized for perception of radiation, though it could reach us, it remains unnoticed in our environment. This information would important for a soldier, who was around a radiation source; he may need medical treatment even though he doesn't have any symptoms. Another time the possibility of radiation exposure is emerging due to paradox clinical symptoms of the soldiers getting back from missions.

Basically we can have two different reasons for carrying out a dosimetry test:

1. We know about the radiation event – we need to evaluate the received dose
2. We have to elucidate, whether suspicious clinical symptoms are caused by a former radiation (e.g. events around Alexander Litvinenko's death, although his polonium poisoning was not a past rather an ongoing process)

The biodosimetric methods reviewed below are selected by – to combined with each other - be suitable to examination of people who were possibly exposed by ionizing radiation. These people can be industrial workers, casualties or soldiers getting back from missions.

These methods are also important tools in triage of a large scale incident or disaster. Triage is the process which makes ranking of the casualties by priority of service. In situations where ionizing radiation is involved can be many people who have no symptoms but they were potentially exposed to radiation, these people must be examined to minimalize the chance of cancerous diseases in the future.

The possibility that terrorism or a large-scale incident could result potential radiation exposure of hundreds of thousands of people is a real threat in our days. Emergency preparedness to these kinds of scenarios includes the usage of biodosimetry tools to make retrospective dose estimation. Biodosimetry is an important tool in any radiological event since the estimation of the received dose makes the triage and the medical treatment of the affected people easier.

Biodosimetry would help:

- estimate the number of people received doses that did not require acute care
- classify patients who need further evaluation into treatment-level categories
- guide the actual treatment
- help handle the long-term consequences of exposures to ionizing radiation (including planning for treatment and patient compensation) [1]

Every biodosimetry tools by definition assess changes in the examined person's cells or tissues which happen in response to ionizing radiation and whose resulting measurements can be reliably attributed to the level of dose received. [2]

Much of the available biodosimetry methods are „biology based", i.e. they detect the direct or indirect biological response to the irradiation in living cells, [3] however changes can be detected in non-living materials of the human body as well (hair, teeth, bones). [4]

Most part of biologically-based biodosimetry methods measures changes in white blood cells. Besides these methods there are such techniques assess biological markers of DNA damage and repair, gene activation, metabolomics or proteomics. Generally, these responses involve such biological systems whose normal function is to respond to pathophysiological processes or physical injuries, thus, these systems are not specific to ionizing radiation. [2]

Most of the available techniques are not specific to ionizing radiation exposure, and their results can be confounded by a variety of factors (e.g. age, disease status, stress, lifestyle, and gender) [5]

The ideal biodosimetry method is radiation specific, has a low background and dispersion, the dose-effect can be calibrated, detects a long-term effect, sampling is easy, can give result quickly and the false positive and false negative results can be distinguished. [6]

Not a single technique fulfils all the criteria of an ideal dosimeter, however an integrated approach using multiple techniques tailored to the exposure scenario can cover most requirements. [4]

As regards in most cases these methods have significantly different characteristics (e.g. time requirement, throughput) it's important to set them together, this way one can select the most suitable method or methods in case of disaster situations.

The comparison also important in planning the methodology, and the proper instruments.

The aim of this article is to review the most commonly used cytogenetic biodosimetry techniques and compare their major parameters.

An important aspect in the view of mass events the automation of the test or at least a high throughput semi-automated solution and it is also worthy of note that biodosimetry methods are also suitable to study radioprotective substances and their mechanism of action.

CYTOGENETIC TECHNIQUES

Besides chemical substances which can cause various genetic damages, ionizing radiation causes several kind of changes in DNA of the exposed cells as well; it can alter the morphology of the chromosomes (e.g. chromosome shape alterations, minutes). For biodosimetric purposes it's common to examine the cytogenetic damage caused by ionizing radiation in peripheral blood lymphocytes. The application of certain methods depends on the stability of the examined chromosome aberration. The frequency of the dicentric chromosomes, PCC fragments and micronuclei decrease with the renewal of the lymphocytes, thus these methods can be applied mostly in the cases where irradiation happened in the recent past. If the irradiation happened years or decades earlier, the FISH method is the best choice due it detects stable translocations.

DICENTRIC CHROMOSOME ASSAY

The centromere is the part of a chromosome which has dual function: links a pair of sister chromatids and during mitosis, spindle fibers attach to the centromere via the kinetochore. [7] Ionizing radiation causes breaks in the chromosomes what makes the possibility to the fusion of two chromosome segments, each with a centromere, resulting acentric fragments and formation of dicentric chromosomes. [8] On rare occasions ring chromosomes can be formed. During the analysis the ration of dicentric chromosomes to normal ones is assessed. A dicentric chromosome are always accompanied by an acentric fragment which helps the investigator, because during the microscopic work the acentric fragments can be identify easier than its dicentric partner.

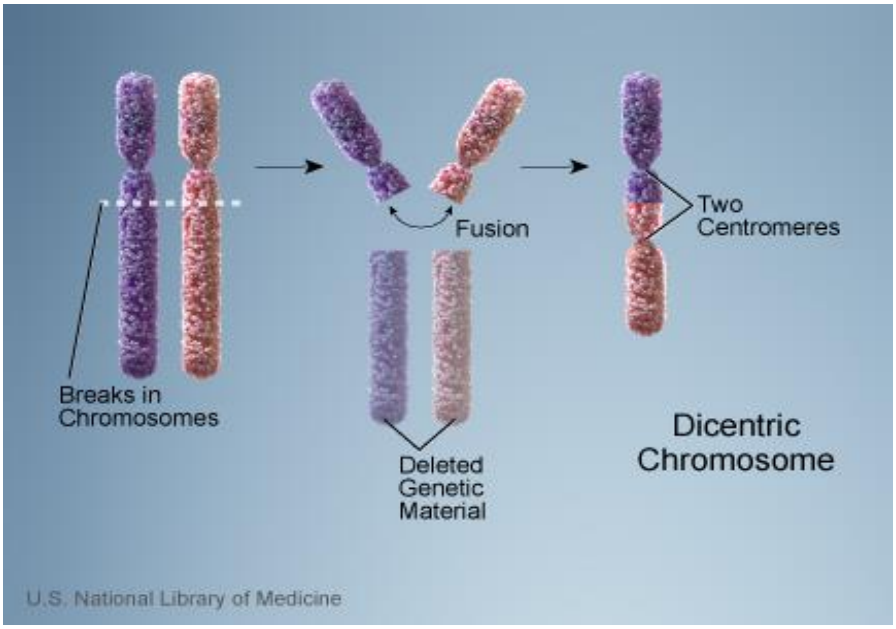


Figure 1. Formation of dicentric chromosomes: Fusion of the broken ends of two chromosomes. [9]

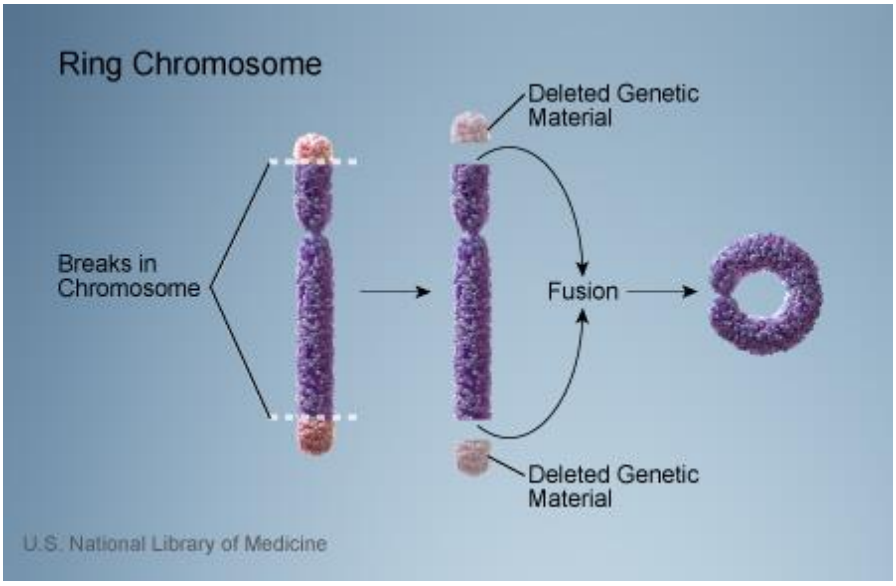


Figure 2. Formation of ring chromosomes: Fusion of the two broken ends of the same chromosome. [9]

Alterations resulted by double strand breaks (dicentric chromosomes, centric rings) are specific to ionizing radiation. The number of these alterations grows with the dose. [10] [11]

Double strand breaks hereby dicentric chromosomes arise nearly exclusively by the effect of ionizing radiation [8] thus this method is considered as „gold standard" [12]. The dose range and time frame make this method useful for biodosimetric purposes. However, it requires cell culturing and induction of cell division as chromosomes condensate only in dividing cells. Mature lymphocites in healthy people's peripheral blood are not dividing cells. In order to make the chromosomes visible, phytohemagglutinin and colcemid are added to the cells to trigger lymphocyte cell division and arrest them at metaphase, respectively. Mostly the CD4+ and CD8+ T cells are stimulated in vitro by phytohaemagglutinin thus are used for biological dosimetry. [13]

In case of acute irradiation, the frequency of the dicentric chromosomes in peripheral lymphocytes can be characterized by a linear-quadratic dose-response curve up to 5 Gray. In

healthy humans the background of dicentric chromosomes is low (~1 dicentric/1000 cells). Due to the low background the sensitivity of the method is good, a ~0,1 Gray whole-body radiation burden can be detected by examining 500-1000 metaphases. [13] [14]

The main disadvantage of this assessment besides its time consuming microscopic analysis is that dicentric chromosomes can be disappear by the renewal of the lymphocytes, as in the bone mellow. Thus in cases when irradiation happened many years ago the dicentric method can be applied with restrictions.

There are efforts to automatize the dicentric chromosome assay (e.g. LUCIA, Metafer) however these are semi-automatic techniques, the human verification is always necessary.

PREMATURE CHROMOSOME CONDENSATION (PCC)

Chromosome condensation happens normally in the prophase of cell division under physiological circumstances; however experimentally it can be caused before the synthesis phase. In vitro adding chemical substances or suitable regulator proteins via cell fusion, chromosomes appear earlier and they become analyzable.

PCC has two subtypes: fusion with Chinese hamster ovary (CHO) mitotic cells and chemically induced PCC. In the first case the rate of countable cells is lower and it requires much experience, but this is a method how to form chromosomes as fast as possible. The chromosomes, what we obtain by PCC, contains only one chromatid therefore – this feature and the smaller size help the investigator to distinguish between human and hamster chromosomes - we can investigate the centromeres only with additional labeling, but it is suitable to detects translocations as well. At the case of chemically induced version of PCC, we don't need CHO cell to fuse with, but is more time consuming due to the extended incubation.

Figure 3. Human G_0 PCC [10]

Cell fusion PCC is also a potential biodosimetric method [15] if the fast and accurate dose evaluation is the main priority. [10] PCC allows of measure the chromosomal aberrations immediately after irradiation. The method needs fusing human lymphocytes with Chinese hamster ovary (CHO) mitotic cells in the presence of a fusing agent, polyethylene glycol

(PEG), this way there is no need for any mitogen stimulation or culturing. [16] Using polyethylene glycol-mediated cell fusion with mitotic cells or chemically induced PCC using calyculin A or okadaic acid chromosome condensation can be achieved without the completion of DNA replication. [4] This method was first described in 1984. [17]

In PCC assay the number of PCC fragments over the 46 chromosomes is counted. On average 4-5 extra fragments/cell/Gray are perceptible in case of low LET irradiation. The background of spontaneous PCC fragments is like dicentric chromosomes, 1-3/1000 cells. [4] The length of the fragments can be informative as well. [18] If the assay is combined with staining procedures, centromeres and dislocations can be measured as well.

Using proper calibration curves, Giemsa stained PCC fragments allow a fast dose evaluation [17] [19] especially if PCC is combined with C-banding, [20] FISH, specific DNA libraries, telomere-centromere staining or peptide nucleic acid (PNA) probes. In the latter case it's possible to detect not only the PCC fragments and translocations but the dicentric chromosomes as well, thus the method can provide fast and accurate dose evaluation. [21] [22] [23]

The assay is useful either to determine low dose exposure or following life threatening high acute doses (both low and high LET radiation). PCC can discriminate accurately between total and partial body exposures. PCC can be a useful tool "for triage of a population after a mass exposure event" especially if it's combined with TC staining or computerized automation. [21]

The cells contain PCC fragments are searched and identified manually but semi-automated systems (e.g. MetaSystems) make scoring much easier. The evaluation makes scoring of light stained chromatids necessary, they can be easily distinguished from dark stained CHO mitotic chromosomes. In unirradiated lymphocytes there are 46 PCC fragments. In irradiated samples the number of PCC fragments is registered, the evaluation made by the number of PCC fragments is correlated to number of PCC fragments in unirradiated samples.

Time after irradiation affects the result of dose evaluation. After irradiation the lymphocytes sampling must be happens as soon as possible in order to make them fusion with the Chinese hamster ovary cells. If the sampling delays, we must calculate with the DNA repair mechanisms during the dose assessment. Studies revealed that the number of PCC fragments 4 hours after irradiation was double as after 1 and 7 days after irradiation, while there wasn't significant difference in numbers between the 1 and 7 days samples. [24]

The assay has several recognized problems, namely radiation induced mitotic delay and cell death during the two day assay culture (especially after high doses), can cause considerable underestimation of the radiation exposure dose. [13]

FLUORESCENT IN SITU HYBRIDIZATION (FISH)

FISH assays are the most important methods in cases where the exposure happened a long time ago. Translocations detected by FISH techniques are alterations which don't affect centromeres and don't perturb the cell division process. This assures the alterations to pass during the cell divisions and to accumulate through life.

FISH techniques are used for assessment of past exposures for many years. The most commonly used version of the technique is single color FISH (sFISH), which makes the detection of inter-chromosomal exchanges - such as dicentrics and translocations - possible. Multi-color FISH and for whole genome analysis M-FISH have been also developed in order to assess induced translocations among different labelled chromosomes. Using pancentromeric and telomeric probes combined with chromosome paint probes enable to discriminate accurately between translocations and dicentrics, as well as between two-way and one-way translocations between chromosomes. In case of protracted exposure (e.g.

occupational doses, or for historic exposure assessment), translocations are the aberration of choice.

In circulating lymphocytes translocation frequencies have been shown persistent for many years, particularly when the analysis is restricted to stable lymphocytes, [25] [26] [27] [28] however background frequencies show significant increase with age [29] [30] and can be greatly variable between individuals of similar age and dose history. Gender or race have been observed have no significant effects on the translocation frequencies but smoking has been suggested to be of significance. [30]

Due to these aforementioned confounding factors the lower detection limit is around 0.5 Gy cumulative lifetime dose for individual dose assessment. [28] In younger non-smoking individuals the detection limit may lower to 0.2 Gy. In partial-body exposures, translocation containing cells are often unstable thus the frequency is reduced with time. [28] First results by FISH are available only ~5 days after receipt of a blood sample, because the method needs for mitotic lymphocytes and lengthy hybridisation protocols.

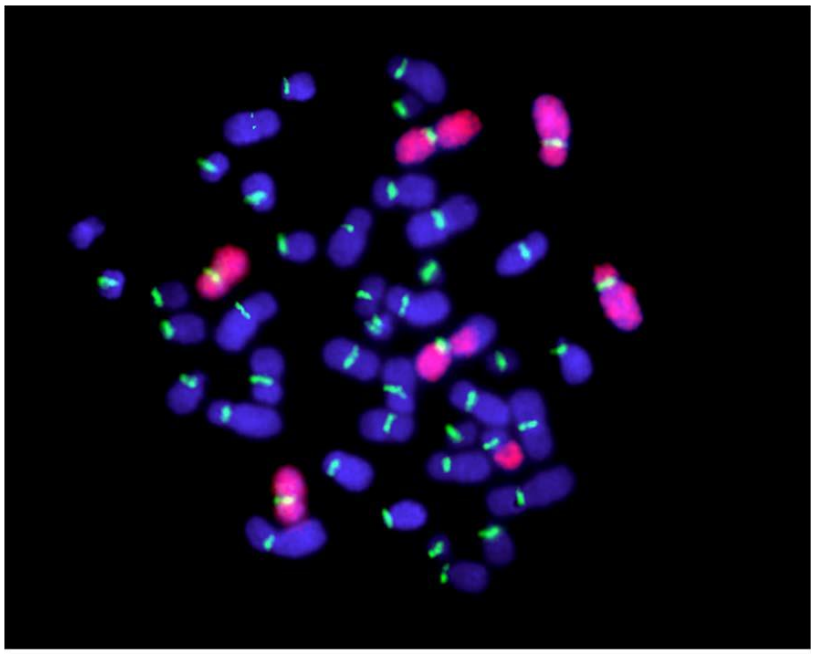


Figure 4. Human metaphase with monocoloured painted chromosomes. Cromosomes 1, 4 and 11 labelled with Cy3 (red), centromeres highlighted with a pancetromeric probe labelled with FITC (green), and the rest counterstained with DAPI. [10]

Using fluorescence microscope with proper staining protocols improves the specificity of every cytogenetic assay, however FISH assays are based only on fluorescence microscopy.

Most retrospective dosimetry has been undertaken on individuals exposed to low LET radiation (reviewed in [4]). FISH techniques have also been used to retrospectively assess chromosome damage in individuals with exposure to high LET radiation. In plutonium workers many years after the exposure increased translocation frequencies have been observed. [4] However, their situation is confounded by significant external gamma irradiation, making the interpretation of results difficult. Other aberrations, such as insertions, intra-chromosomal and complex aberrations have also been suggested as biomarkers of high LET exposure.

Two EU concerted actions aimed at standardizing sFISH concluded that only ‘complete’ cells (i.e. those with all ‘painted’ material present and 46 chromosomes) should be used and frequencies calculated using stable cells only. For population-based studies it is recommended

to analyze at least ~300 genome equivalent cells per individual. Accurate individual dose assessment requires at least ~1000 genome equivalent cells." [4] Automated scoring systems available e.g. LUCIA control-system. [31]

MICRONUCLEUS ASSAY

In vitro cytokinesis blocked micronuclei method is also a cytogenetic biodosimetry assay. By the definition of IAEA: "Ionizing radiation induces the formation of acentric chromosome fragments and to a small extent malsegregation of whole chromosomes. Acentric chromosome fragments and whole chromosomes that are unable to interact with the spindle lag behind at anaphase, and as a result they are not included in the main daughter nuclei. A lagging chromosome fragment or whole chromosome forms into a small separate nucleus; hence the term micronucleus."

In methodology aspect it resembles to the dicentric chromosome assay however it's simpler thus more popular as well.

It requires a lower magnification (~40-60X) than dicentric chromosome analysis, latter needs ~100X magnification. Usually you do not need a fluorescence microscope to perform the micronucleus assay, however fluorescent centromere staining improves the specificity of the assay since micronuclei containing centromere are uncharacteristic to ionizing radiation.

As peripheral lymphocytes are non-dividing cells, the induction of cell division in ex vivo samples requires phytohemagglutinin just as in dicentric chromosome assay. The postmitotic nucleus can be investigated in telophase, so the division is stopped with cytochalasine-B what makes the cell culturing one day longer than in case of dicentric chromosomes. [32] Cytochalasine-B inhibits the actine polymerization thus prevents the separation of the daughter cells resulting binuclear cells. Binuclear cells already have two nuclei but they have only one cytoplasm yet, so that the freshly divided cells are clearly distinguishable from other ones, which are not divided. Usually the micronuclei are formed by those acentric fragments or chromosomes which can't migrate to the poles during the cell division, [33] however they can be formed even from whole chromosomes in case of mitotic spindle or centromere attachment damage [10] These are recognizable spherical bodies in the binuclear cell's cytoplasm which are smaller and have a similar morphology and staining properties as nuclei. [4]

The micronucleus formation is not radiation specific; they can be influenced by many clastogenic and anegenic agents.

The number of micronuclei increases because of exposure to ionizing radiation, [10] age, [32] untreated tumorous diseases, [34] smoking, harmful environmental and occupational factors [35].

The CBMN assay is a well validated and standardized assay to evaluate the exposure of occupationally, medically and accidentally exposed individuals. [4] Like dicentric chromosomes, micronuclei are unstable cytogenetic aberrations, which disappear with time after exposure, and thus their use is limited for exposures that occurred many years ago.

The lower limit of the dose detection is 0,2-0,3 Gray [4] what caused by the relatively high and variable spontaneous MN yield. This yield is more pronounced in females and increases with age. [36]

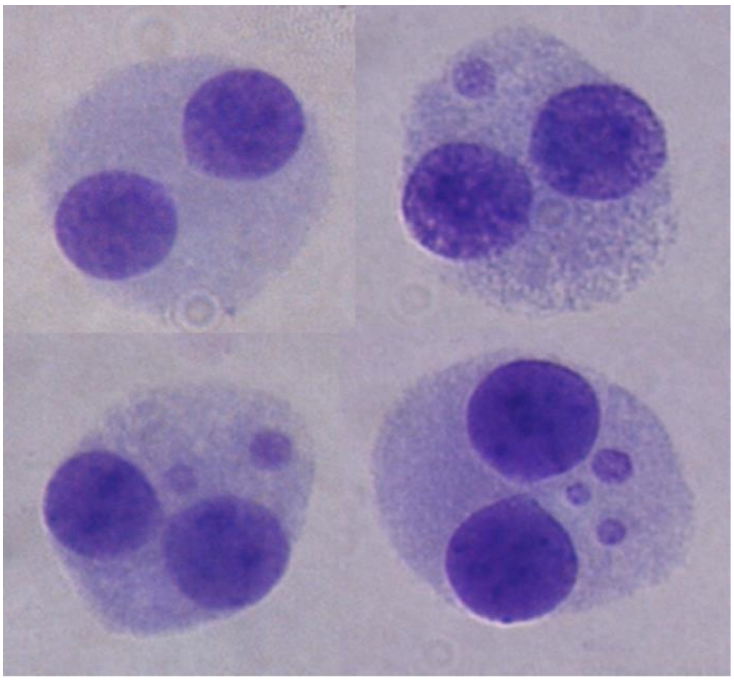


Figure 5. Human Lymphocytes with 0, 1, 2 and 3 micronuclei respectively (our workgroup's own preparations. Thanks to Sandor Papp for contribution).

Compared to the dicentric chromosome assay, although the cell culturing is one day longer, scoring CBMN assay is easier and requires less time consuming microscopic work.

In case of CBMN assay there are some automation efforts as well (e.g. LUCIA, [31] RABiT, [37] Metafer [38]). The main problem of older systems in this field is the shortage of cytoplasm detection. As the binuclear cells are identified on the basis of the distance between the nuclei, they work with a high dilution of cells to minimize this error.

CONCLUSIONS

After a terror attack or an industrial accident with numerous casualties the first steps of the triage is to identify the clinical symptoms and a complete blood count / haemogram determination. These are routine clinical dosimetry processes. The decline of the white blood cells number alludes to radiation exposure.

Numerous biodosimetric tests may require cooperation of several laboratories. These times those laboratories come to the fore where automated biodosimetry systems are available.

The most plausible solution is the micronucleus assay due it has the highest throughput amongst the aforementioned techniques if it's made manually and it can be automated. However the method is not clearly specific to ionizing radiation, if the involvement of ionizing radiation is known, the method is suitable to dose evaluation.

The sensitivity and specificity of the dicentric assay is considerably good, it can be partly automatized and can be carried out in any laboratory.

Fortunately, mass casualty radiation event is rarely occurs, more often we search the answer to a different kind of question with biodosimetry. Examination of soldiers getting back from missions can reveal whether they were exposed by ionizing radiation or not. It's especially important if one has medical problems. In these situations, there are enough time and opportunity for an accurate medical check-up. It's advisable to apply several different biodosimetry tests at the same time; for example, comparing the results of micronucleus and dicentric assays can be informative, because if only the micronucleus count shows alteration, then the received harmful impact most likely was not ionizing radiation.

Detection of chromosome aberrations (e.g. dicentrics, acentric fragments) and cytogenetic damages by micronucleus assay is commonly used for dose assessment.

Translocations detected by FISH techniques are useful especially in exposure scenarios happened years before, but the results are questionable on occasion (mostly due the variable background).

This comparison of the above mentioned methods is shown in table 1.

Assay	**Minimum time from exposure until marker is valid**	**Maximum time from exposure when marker remains valid**	**Total processing time (from receiving sample to get the result)**	**Lowest detection limit** (Gy)
Cytogenetic dosimetry methods				
Dicentric chromosome	0–1 day	>6 months	4–9 days	0,1 Gy
Mikronucleus	0–1 day	1 year	4-6 days	0,2–0,3 Gy
PCC	0–1 day	7 days[5]	CHO-23 hours chemically induced–51 hours[5]	0,2 Gy[5]
FISH	0–1 day	years	5 nap[4]	0,5 (0,2) Gy
Routine laboratory test to take into account for triage				
Lymphocyte count decrease	12 hours	48 hours	1,5–2 days	~0,5 Gy

Table 1. Timeframes and detection limits of the cytogenetic biodosimetry assays. (After Flood et al. 2014. [39] reworked)

There is no method which is ideal for every scenario, thus it's expedient to select the method accordingly the actual situation. The best solution is to apply several methods at the same time, putting together all possible pieces of information from multiple sources, however in some cases (disasters, terror attack) it's cannot be accomplished due to the huge number of samples and the lack of time. It shell be considered how to get the more information with the less effort under minimal term.

The methods presented here were selected according to the consideration, that the tests, combined with each other, would be able to quickly and comprehensively examine persons suffering from a suspected casualty injury, whether they are casualties or a smaller or larger group of mission-returning soldiers. It is why the procedures in their most important parameters (thresholds of detection, time of completion, timely detection of effect) may differ significantly.

REFERENCES

[1] SWARTZ, H.M., FLOOD, A.B., GOUGELET R.M., REA, M.E., NICOLALDE, R.J., WILLIAMS, B.B.: *A critical assessment of biodosimetry methods for large-scale incidents.* Health Physics, Vol. 98, No. 2 (2010), 95–108. doi: 10.1097/HP.0b013e3181b8cffd.

[2] FLOOD, A.B., ALI, A.N., BOYLE, H.K., DU, G., SATINSKY, V.A., SWARTS, S.G., WILLIAMS, B.B., DEMIDENKO, E., SCHREIBER, W., SWARTZ H.M.: *Evaluating the Special Needs of the Military for Radiation Biodosimetry for Tactical Warfare against Deployed Troops: Comparing Military to Civilian Needs for Biodosimetry Methods*. Health Physics, Vol. 111, No. 2 (2016), 169–182. doi: 10.1097/HP.0000000000000538

[3] DR. SOMOSY Z., DR. GALÁNTAI R.T., DR. HORVÁTH GY., DR. GACHÁLYI A.: *A szomszédsági hatás és lehetséges szerepe az arterioszklerotikus folyamatokban.* Honvédorvos, 64. évf (2012.) 3-4. szám, 185-201.

[4] AINSBURY, E.A., BAKHANOVA, E., BARQUINERO, J.F., BRAI M., CHUMAK V., CORRECHER V., DARROUDI, F., FATTIBENE P., GRUEL G., GUCLU I., HORN, S., JAWORSKA A., KULKA, U., LINDHOLM, C., LLOYD, D., LONGO, A., MARRALE, M., MONTEIRO GIL, O., OESTREICHER, U., PAJIC, J., RAKIC, B., ROMM, H., TROMPIER, F., VERONESE, I., VOISIN, P., VRAL, A., WHITEHOUSE, C.A., WIESER, A., WODA, C., WOJCIK, A., ROTHKAMM, K.: *Review of retrospective dosimetry techniques for external ionising radiation exposure.* Radiation Protection Dosimetry, Vol. 147, No. 4 (2011), 573–592. doi: 10.1093/rpd/ncq499.

[5] SULLIVAN, J.M., PRASANNA P.G.S., GRACE, M.B., WATHEN, L., WALLACE, R.L., KOERNER, J.F., COLEMAN, C.N.: *Assessment of Biodosimetry Methods for a Mass-Casualty Radiological Incident: Medical Response and Management Considerations,* Health Physics, Vol. 105, No. 6 (2013), 540-54. doi:10.1097/HP.0b013e31829cf221.

[6] KIS E.: *A NAÜ citogenetikai biodozimetria tanfolyama: Alkalmazás a nukleáris veszély-helyzetre való felkészültségben és reagálásban*. Sugárvédelem, VI. évf. (2013) 1. szám. 38 – 43.

[7] SZEBERÉNYI J.: *Molekuláris sejtbiológia*. Budapest: Dialóg Campus Kiadó, 2014. ISBN 978-615-5376-44-3

[8] PESZNYÁK CS., SÁFRÁNY G.: *Sugárbiológia,* Budapest: Typotex Kiadó, 2016. ISBN 978-963-279-952-0

[9] U.S. National Library of Medicine, https://ghr.nlm.nih.gov/primer/mutationsanddisorders/structuralchanges, Downloaded: 2018.03.05.

[10] INTERNATIONAL ATOMIC ENERGY AGENCY: *Cytogenetic Dosimetry: Applications in Preparedness for and Response to Radiation Emergencies*, IAEA, Vienna, 2011.

[11] HOFFMANN W, SCHMITZ-FEUERHAKE I.: *How radiation-specific is the dicentric assay?*, J. Expo. Anal. Environ. Epidemiol. Mar-Apr;9(2) (1999):113-33.

[12] VOISIN, P.: Standards in biological dosimetry: *A requirement to perform an appropriate dose assessment*, Mutation Research, Vol 793 (2015), 115–122. doi: 10.1016/j.mrgentox.2015.06.012

[13] INTERNATIONAL ATOMIC ENERGY AGENCY: *Cytogenetic analysis for radiation dose assessment,* A manual. IAEA Technical Report Series 405 (2001).

[14] ROMM, H., OESTREICHER, U., KULKA, U.: *Cytogenetic damage analysed by the dicentric assay,* Ann. Ist. Super. Sanita, Vol. 45, No. 3 (2009), 251-259.

[15] TERZOUDI G.I., PANTELIAS G.E.: *Cytogenetic methods for biodosimetry and risk individualization after exposure to ionising radiation,* Radiation Protection Dosimetry, Vol. 122, No. 1-4 (2006), 513-520. doi:10.1093/rpd/ncl509

[16] PANTELIAS, G.E., MAILLIE H.D.: *A simple method for premature chromosome condensation induction in primary human and rodent cells using polyethylene glycol,* Somatic Cell Genetics, Vol. 9, No. 5 (1983), 533-547. doi: 10.1007/BF01574257

[17] PANTELIAS, G.E., MAILLIE H.D.: *The use of peripheral blood mononuclear cell prematurely condensed chromosomes for biological dosimetry,* Radiation Research, Vol. 99, No. 1. (1984), 140-150. doi: 10.2307/3576452

[18] GONZÁLEZ, J.E., ROMERO, I., GREGOIRE, E., MARTIN, C., LAMADRID, A.I., VOISIN, P., BARQUINERO, J.F., GARCÍA, O.: *Biodosimetry estimation using the ratio of the longest:shortest length in the premature chromosome condensation (PCC) method applying autocapture and automatic image analysis*, Journal of Radiation Research, 2014, 55, 862–865. doi: 10.1093/jrr/rru030.

[19] LAMADRID BOADA, A.I., ROMERO AGUILERA, I., TERZOUDI, G.I., GONZALEZ MESA, J.E., PANTELIAS, G., GARCNA, O.: *Rapid assessment of high-dose radiation exposures through scoring of cell-fusion-induced premature chromosome condensation and ring chromosomes*, Mutat Research, Vol. 757, No. 1 (2013), 45-51. doi: 10.1016/j.mrgentox.2013.06.021.

[20] PANTELIAS, G.E., Iliakis, G.E., Sambani, C.D., Politis, G.: *Biological dosimetry of ab-sorbed radiation by C-banding of interphase chromosomes in peripheral blood lymphocytes. Int J Radiat Biol.*, Vol. 63, No. 3 (1993), 349-354. doi: 10.1080/09553009314550461

[21] M'KACHER, R., EL MAALOUF E, TERZOUDI, G., RICOUL, M., HEIDINGSFELDER, L., LAPLAGNE, E., HEMPEL, W.M., COLICCHIO, B., DIETERLEN, A., PANTELIAS, G., SABATIER, L.: *Detection and automated scoring of dicentric chromosomes in non-stimulated lymphocyte prematurely condensed chromosomes following telomere and centromere staining*, International Journal of Radiation Oncology Biology Physics, Vol. 91, No. 3 (2015), 640-649. doi: 10.1016/j.ijrobp.2014.10.048.

[22] KARACHRISTOU, I, KARAKOSTA, M., PANTELIAS, A., HATZI, V.I., KARAISKOS, P., DIMITRIOU, P., PANTELIAS, G., TERZOUDI, G.I.: *Triage biodosimetry using centromeric/telomeric PNA probes and Giemsa staining to score dicentrics or excess fragments in non-stimulated lymphocyte prematurely condensed chromosomes*, Mutat Res Genet Toxicol Environ Mutagen, Vol. 793 (2015), 107-114. doi: 10.1016/j.mrgentox.2015.06.013.

[23] TERZOUDI, G.I., PANTELIAS, G., DARROUDI, F., BARSZCZEWSKA, K., BURACZEWSKA, I., DEPUYDT, J., GEORGIEVA, D., HADJIDEKOVA, V., HATZI, V.I., KARACHRISTOU, I., KARAKOSTA, M., MESCHINI, R., M'KACHER, R., MONTORO, A., PALITTI, F., PANTELIAS, A., PEPE, G., RICOUL, M., SABATIER, L., SEBASTIÀ, N., SOMMER, S., VRAL, A., ZAFIROPOULOS, D., WOJCIK, A.: *Dose assessment intercomparisons within the RENEB network using G0-lymphocyte prematurely condensed chromosomes (PCC assay),* Int J Radiat Biol., Vol. 93, No. 1 (2017), 48-57. doi: 10.1080/09553002.2016.1234725.

[24] DARROUDI, F., FOMINA, J., MEIJERS, M., NATARAJAN, A.: *Kinetics of the formation of chromosome aberrations in X-irradiated human lymphocytes, using PCC and FISH*, Mutation Research, Vol. 404, No. 1-2 (1998), 55–65. doi: 10.1016/S0027-5107(98)00095-5

[25] TAWN, E. J., WHITEHOUSE, C. A.: *Persistence of translocation frequencies in blood lymphocytes following radiotherapy: implications for retrospective radiation biodosimetry,* J. Radiol. Prot., Vol. 23, No. 4 (2003), 423–430. doi: 10.1088/0952-4746/23/4/005

[26] LLOYD, D.C., MOQUET, J.E., ORAM, S., EDWARDS, A. A., LUCAS, J. N.: *Accidental intake of tritiated water: a cytogenetic follow-up case on translocation stability and dose reconstruction*, Int. J. Radiat. Biol., Vol. 73, No. 5 (1998), 543–547. doi: 10.1080/095530098142095

[27] LINDHOLM, C., EDWARDS, A.: *Long-term persistence of translocations in stable lymphocytes from victims of a radiological accident,* Int. J. Radiat. Biol., Vol. 80, No. 8 (2004) 559–566. doi: 10.1080/09553000412331283498

[28] EDWARDS, A.A., LINDHOLM, C., DARROUDI, F., STEPHAN, G., ROMM, H., BARQUINERO, J., BARRIOS, L., CABALLIN, M.R., ROY, L., WHITEHOUSE, C.A., TAWN, E.J., MOQUET, J., LLOYD, D.C., VOISIN, P.: *Review of translocations detected by FISH for retrospective biological dosimetry applications*, Radiation Protection Dosimetry, Vol. 113, No. 4 (2005) 396–402. doi: 10.1093/rpd/nch452

[29] WHITEHOUSE, C.A., EDWARDS, A.A., TAWN E.J., STEPHAN, G., OESTREICHER, U., MOQUET, J.E., LLOYD, D.C., ROY, L., VOISIN, P., LINDHOLM, C., BARQUINERO, J., BARRIOS, L., CABALLIN, M.R., DARROUDI, F., FOMINA, J.: *Translocation yields in peripheral blood lymphocytes from control populations*, Int. J. Radiat. Biol., Vol. 81, No. 2 (2005), 139–145. doi: 10.1080/09553000500103082

[30] SIGURDSON, A.J., HA, M., HAUPTMANN, M., BHATTI, P., SRAM, R.J., BESKID, O., TAWN, E.J., WHITEHOUSE, C.A., LINDHOLM, C., NAKANO, M., KODAMA, Y., NAKAMURA, N., VOROBTSOVA, I., OESTREICHER, U., STEPHAN, G., YONG, L.C., BAUCHINGER, M., SCHMID, E., CHUNG, H.W., DARROUDI, F., ROY, L., VOISIN, P., BARQUINERO, J.F., LIVINGSTON, G., BLAKEY, D., HAYATA, I., ZHANG, W., WANG, C., BENNETT, L.M., LITTLEFIELD, L.G., EDWARDS, A.A., KLEINERMAN, R.A., TUCKER, J.D.: *International study of factors affecting human chromosome translocations*, Mutation Research, Vol 652, No. 2 (2008), 112–121. doi: 10.1016/j.mrgentox.2008.01.005

[31] Lucia Cytogenetics, http://www.lucia.cz/en/front-page, Downloaded: 2017.11.06.

[32] FENECH, M., MORLEY, A.A.: *Cytokinesis-block micronucleus method in human lymphocytes: effect of in vivo ageing and low dose X-irradiation*, Mutation Research, Vol. 161, No. 2 (1986), 193-198. doi: 10.1016/0027-5107(86)90010-2

[33] TURAI I., KÖTELES GY. (szerk.): *Sugáregészségtan*, Budapest: Medicina Kiadó, 2014. ISBN: 9789632265032

[34] MILOSEVIĆ-DJORDJEVIĆ O, GRUJICIĈ D, VASKOVIĈ Z, MARINKOVIĈ D.: *High micronucleus frequency in peripheral blood lymphocytes of untreated cancer patients irrespective of gender, smoking and cancer sites*, Tohoku J. Exp. Med. 2010 Feb;220(2):115-20. doi: 10.1620/tjem.220.115

[35] MIGLIORE L, PARRINI M, SBRANA I, BIAGINI C, BATTAGLIA A, LOPRIENO N.: *Micronucleated lymphocytes in people occupationally exposed to potential environmental contaminants*, the age effect. Mutation Research. 1991 Jan; 256(1):13-20. doi: 10.1016/0921-8734(91)90028-A

[36] FENECH, M: *The cytokinesis-block micronucleus technique: a detailed description of the method and its application to genotoxicity studies in human populations*, Mutation Research, Vol. 285, No. 1 (1993), 35–44. doi: 10.1016/0027-5107(93)90049-L

[37] REPIN, M., PAMPOU, S., KARAN, C., BRENNER, D.J, GARTY, G.: RABiT-II: *Implementation of a High-Throughput Micronucleus Biodosimetry Assay on Commercial Biotech Robotic Systems*, Radiat Research, Vol. 187, No. 4 (2017), 492–498. doi: 10.1667/RR011CC.1.

[38] ROSSNEROVA, A., SPATOVA, M., SCHUNCK, C., SRAM, R.J.: *Automated scoring of lymphocyte micronuclei by the MetaSystems Metafer image cytometry system and its application in studies of human mutagen sensitivity and biodosimetry of genotoxin exposure*, Mutagenesis, Vol. 26, no. 1 (2011), 169–175. doi: 10.1093/mutage/geq057.

[39] FLOOD, A.B., BOYLE, H.K., DU, G., DEMIDENKO, E., NICOLALDE, R.J., WILLIAMS, B.B., SWARTZ, H.M.: *Advances in a framework to compare bio-dosimetry methods for triage in large-scale radiation events*, Radiation Protection Dosimetry Vol. 159, No. 1–4 (2014), 77–86. doi: 10.1093/rpd/ncu120

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

A KATASZTRÓFAVÉDELEM TŰZOLTÓI MUNKAKÖRBE TÖRTÉNŐ JELENTKEZÉS MOTIVÁCIÓI

THE MOTIVATIONS OF SIGN UP FOR THE DISASTER MANAGEMENTS THE FIREMANS SCOPE OF JOB

FRIGY Éva Gyöngyi

(ORCID: 0000-0002-0432-5385)

freevick@gmail.com

Absztrakt

Tanulmányomban a katasztrófavédelem tűzoltói munkakörbe történő jelentkezés motivációit vizsgáltam. Arra kerestem a választ, hogy milyen befolyásoló tényezők, motivációk játszanak szerepet e munkakörbe való jelentkezéskor.

A kutatásom elméleti hátttereként a pályaválasztás és a pályaválasztás motivációi szolgáltak. Vizsgálatom célcsoportja a tűzoltói munkakörbe jelentkezők voltak.

A saját vizsgálatom három módszer mentén öt felvetés megfogalmazásából áll. Elsődleges módszerként – a lehetőségeimhez mérten – a tűzoltó munkakörre vonatkozó, pályamotivációt vizsgáló kérdőíves felmérést végeztem. Másodlagos vizsgálati módszerként – a szervezet által részemre bocsátott – előző évi adatok alapján statisztikaelemzéssel trendvizsgálatot készítettem. Harmadlagos vizsgálati módszerként a szervezet által közvetített toborzó szöveg tartalomelemzését választottam.

A tanulmányom a Fővárosi Katasztrófavédelmi Igazgatóság tűzoltói munkakörbe történő kiválasztásrendszere és a jelentkezés motivációi című diplomamunkám nyomán készült.[1]

Kulcsszavak: *pályaválasztás, pályaválasztási motivációk, pályaismeret, pályakép, tűzoltói kompetenciák*

Abstract

In my study I have made a research on the motivation of registration of the fireman of the Disaster Management. I looked for the answer of the following question: which influential factors, motivation are playing a role in the application in to this role.

The choice of carrier and the motivations of the carrier choice worked as a background of my theoretical researches. The target of my research were the applicants of the firemen.

My own research includes five hypothesis alongside three methods. I have used a questionnaire of the fireman carrier motivation as my primary researching instrument. As the second method I have created a trend test with statistic analysis from the data of the last year, which was provided by the institute to me. As the third method I chose a content analysis of the institutes recruiting text.

My study was made based on my thesis work on The extractor system and the motivation of registration of the firemen of the Capital Institute of Disaster Management.[1]

Keywords: *career choice, career motivations, career knowledge, career plans, firefighter skills*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.07.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.05.17.

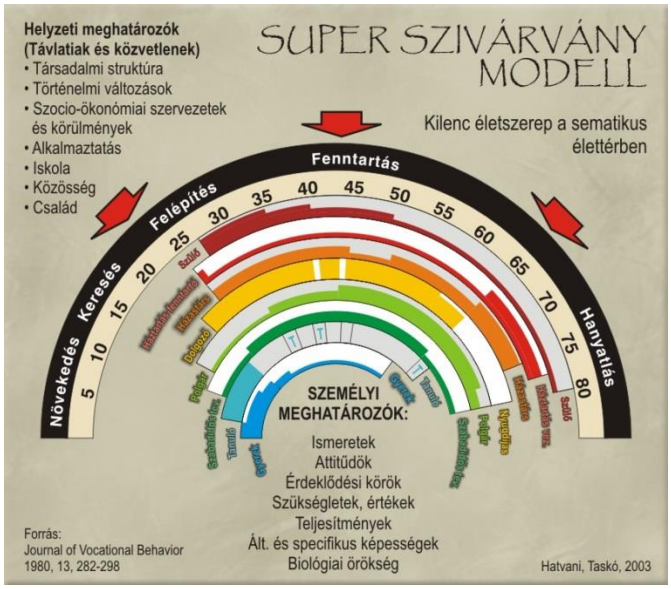
BEVEZETÉS

2016. január 01-jével kerültem a katasztrófavédelem állományába. Ettől az időtől kezdve ismerkedek a tűzoltói munkakör sokrétűségével, és látok bele abba, hogy milyen elhivatottnak kell lennie annak, aki ezt a – fizikailag és gyakran lelkileg is – komoly megterhelést jelentő szakmát választja, űzi. Tanulmányom – mely *A Fővárosi Katasztrófavédelmi Igazgatóság tűzoltói munkakörbe történő kiválasztásrendszere és a jelentkezés motivációi* című diplomamunkám [1] nyomán készült – arra keresi a választ, hogy milyen befolyásoló tényezők, motivációk játszanak szerepet a beosztott tűzoltói munkakörbe való jelentkezéskor. A felállított felvetéseim helyességének megvizsgálása érdekében elkészítettem egy – a tűzoltó munkakörre vonatkozó – pályamotivációt vizsgáló kérdőívet, mint eszközt, amelyet a Fővárosi Katasztrófavédelmi Igazgatóság toborzása alkalmával a beosztott tűzoltó munkakörbe meghirdetett státuszokra jelentkezők körében vetettem be.

SZAKIRODALMI ÁTTEKINTÉS

Az egyén életének egyik legmeghatározóbb döntése maga a pályaválasztás, amely az egész életútját befolyásolja az iskolapadtól a munkavilágában való elhelyezkedésén keresztül a társadalomban elfoglalt pozíciójáig. [2] A pályaválasztás tehát az egyén életútjának egyik legmeghatározóbb lépése, mivel a nem kellőképpen megalapozott döntés nemcsak az iskolai sikerességre lehet hatással, hanem negatívan befolyásolhatja az egyén jövőbeni életesélyeit is. [3]

A pályaválasztás területével számos külföldi és hazai kutató foglalkozott (Super, Csirszka, Rókusfalvy, Ritoók, Szilágyi stb.). Ahhoz, hogy ezt a pályaválasztás fogalmát jól értelmezni tudjuk, először meg kell határozni mit is értünk a pálya kifejezés alatt. [4] Csirszka meghatározása alapján a pálya nem más, mint „a személyiség életútjának munkával töltött szakasza”, mely sosem létezik önmagában, hanem az egyénhez tartozik, sőt „belőle fakad”. [5] Az életpálya pedig az egyén élete során betöltött szerepeinek az együttese melyet Super egy úgynevezett életút-szivárványban ábrázolva foglal rendszerbe a születéstől az idős korig, amelyben a munka csupán egy a nyolc életszerep közül. [6] Super életpálya-modelljében (lásd: 1. ábra) a valóságban is megélt párhuzamos szerepvállalások alkotják a szivárvány sávjait. Minden szerep megvalósulását külső (szocioökonómiai környezet) és belső (attitűd, érdeklődés, képességek stb.) tényezők alakulásának együttes kapcsolata határozza meg. Az életkor előrehaladtával az egyes szerepek jelentősége változik. Az életelégedettség mértékét befolyásolja, hogy az egyénnek mennyi egyszerre betöltött szereppel kell megbirkóznia, hogyan, milyen szinten sikerült betöltenie azokat, illetve ezeket mennyire sikerül egymással összhangba állítania. [7] Az az életpálya-modell szerint minden életszerephez (gyermek, szülő tanuló, házastárs, nyugdíjas stb.) tartozik valamilyen jellemző feladat (növekedés, exploráció, megállapodás, fenntartás stb.) illetve tanácsadási területet. [8]



1. ábra Super Életpálya szivárvány modellje [9]

A megfelelő pályaválasztáshoz feltétlenül arra van szükség, hogy az érdeklődésen túl az egyén tisztában legyen saját képességeivel, illetve adottságaival. Lényegében ennek eredménye a pályaválasztási érettség. Rókusfalvy megfogalmazása alapján: „Pályaválasztási érettségnek nevezzük a tanuló egész személyiségének olyan arányos fejlettségi állapotát, amely egyrészt lehetővé teszi az elhelyezkedési lehetőségeknek és a személyiségnek megfelelő pálya adekvát választását, másrészt biztosítja a szakmai képzésnek legalább minimális sikerét és felébreszti a tanulóban a szakmai beilleszkedésre irányuló tartós törekvést.” [10] Számos kutatás igazolja, hogy a pályaválasztási döntés minőségét a pályaidentitás kialakulása és a tanulási motiváció mértéke nagymértékben befolyásolja. [11] Ennek hiányában nagy az elhibázott szakmaválasztás lehetősége. Sokan nehezen vagy egyáltalán nem tudják megfogalmazni a pályaválasztásukat befolyásoló motivációs tényezőiket, hiszen nagyon összetett a motivációs rendszer. Ráadásul erősen függ az adott személy lehetőségeitől is, így a munkával kapcsolatos szükségletek, motivációk egyénenként eltérőek, vagyis ugyanazon motiváló erők teljesen más foglalkozás választását eredményezhetik, vagy különböző motivációk vezethetnek egyazon munkakörbe. Szilágyi a motivációk és elvárások, értékek összefüggésére is rámutat: „a motivációk mindig szoros kapcsolatba hozhatók a társadalom által preferált értékekkel.” Ebből kiindulva összefoglalhatjuk, hogy a pályaválasztás motivációit a szükségleteken túl belső (érték, érdeklődés) és külső (pályával kapcsolatban megfogalmazott társadalmi elvárások) tényezők alkotják. [12]

KUTATÁS

A kutatásom célcsoportja a beosztott tűzoltói munkakörbe jelentkezők köre. A saját vizsgálatom három módszer mentén öt felvetés megfogalmazásából áll. Mivel korlátozottak voltak a lehetőségeim, hogy ezzel a célcsoporttal kvalitatív vizsgálati módszert megvalósíthassak, így primer kutatásként az engedélyezett kérdőíves kvantitatív vizsgálati módszerrel éltem, amit szekunder kutatásban kiegészítettem a szervezet által részemre bocsátott – előző évi adatok alapján 2012-től egészen – az általam vizsgált – 2016-ig az elmúlt évek statisztikai adatainak elemzésével és trendvizsgálatával, valamint a toborzás csatornáinak és a csatornákon elhangzott hirdetések tartalmának elemzésével, hogy milyen csatornákon hirdették meg, milyen információk voltak elérhetők.

A kérdőíveket a tavaszi toborzáson 52 főből 49 fő; az őszi toborzás alkalmával pedig 57 főből 45 fő töltötte ki, így összesen 109 főből 94 főtől kaptam valamennyi kérdésre választ. Ez a 94 darab kitöltött kérdőív adja a beosztott tűzoltói munkakörbe jelentkezők (alapsokaság) motivációs tényezőinek vizsgálatához a mintavételezésem alapját.

A fent vázolt mintán a szakirodalomra hivatkozva a következő felvetéseket vizsgáltam meg:

I. felvetés: Feltételezésem szerint a tűzoltói munkakörbe szakképesítéssel rendelkezők jelentkezők közül a műszaki szakképesítés a jellemző.

II. felvetés: Feltételezésem szerint a tűzoltói szakma választása közeli példa alapján jellemző.

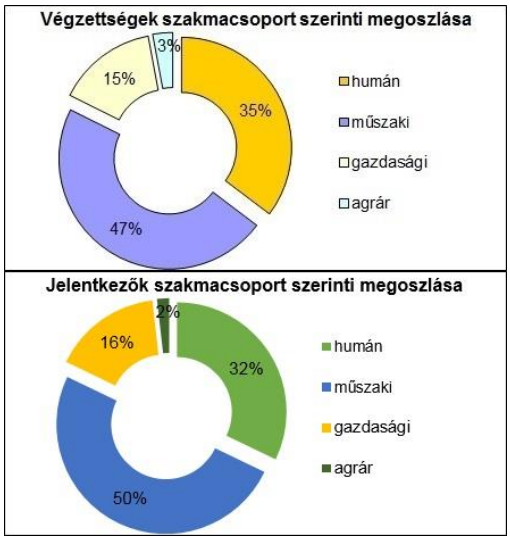
III. felvetés: Feltételezésem szerint a tűzoltó hivatás alap motívuma a bajbajutottakon való segítség, életmentés szándéka.

IV. felvetés: Feltételezésem szerint a fizikai és pszichikai teherbírás, illetve a csapatmunka kompetenciák hangsúlya megjelenik a jelentkezők pályaismeretében.

V. felvetés: Feltételezésem szerint a 2016. év és előző évek közötti időintervallumban demográfiai (életkor, lakhely, iskolai végzettség) változások figyelhetőek meg.

EREDMÉNYEK ÉS KÖVETKEZTETÉSEK

Az I. felvetés – a tűzoltói munkakörbe szakképesítéssel rendelkezők jelentkezők közül a műszaki szakképesítés a jellemző – beigazolódott, mert a kérdést relevánsan megválaszolók 50%-a (28 fő) műszaki és 32%-a (18 fő) humán szakmacsoportba tartozó végzettséggel rendelkezik. (Lásd: 2. ábra) Természetesen a humán beállítottságú jelentkezők magas aránya sem meglepő ezen a közszolgálati területen.



2. ábra A jelentkezők iskolai végzettségének szakmacsoport szerinti megoszlása (saját szerkesztés)

A II. felvetés – a tűzoltói szakma választása leginkább közeli példa alapján jellemző –, csak részben igazolódott, mivel ugyan a kitöltők 82%-ának (77 fő) közvetlen környezetében valóban van tűzoltó, tehát a választ adók több, mint 75%-ának). Ebből 21-nek családi, 51-nek baráti, ismerősi és 5-nek mindkét körben (vagyis összesítve 26 főnek (28%) családi, 56 főnek (60%) baráti, ismerősi körben – Lásd: 3. ábra). Azonban a 26 tűzoltó családtaggal büszkélkedő személyből csak 9 fő jelölte meg jelentkezését befolyásoló motivációként a *„családi befolyás, tradíció folytatása miatt”* és megint 9 fő a *„gyermekkorom óta tűzoltó akartam lenni”* válaszlehetőségeket. Ezek közül a két válaszlehetőség metszéspontjába csak 4 fő került, akire mindkét motívum hatással bírt a jelentkezést illetően, tehát 14 fő esetén biztos motívum a

közvetlen környezetben látott minta. A 4 fő esetében pedig teljes mértékben megalapozott tudatos döntést feltételezhetünk, pláne, hogy közülük 3 már rendelkezik tűzoltói tapasztalattal.

3. ábra Közvetlen környezetben lévő tűzoltók (saját szerkesztés)

A III. felvetés – a tűzoltó hivatás alap motívuma a bajbajutottakon való segítség, életmentés szándéka –, azt gondolom, hogy teljes mértékben igazolódott, hiszen 94 főből 83-an, azaz a jelentkezők 88%-a a pályaválasztás egyik motivációjaként a tűzoltói szolgálatra jellemző *„segítségnyújtás másoknak”* választ adta (lásd: 4. ábra). Ennek ellenére – a IV. felvetésemre hivatkozva – számomra meglepő volt, hogy a maradék 11 főből, akiknél nem szerepel másokon való segítségnyújtás igénye, 4 fő olyan személy, akinek a családjában (1 fő) vagy a barátai, ismerősei között (3 fő) van tűzoltó.

4. ábra A jelentkezők motivációs tényezőinek megoszlása (saját szerkesztés)

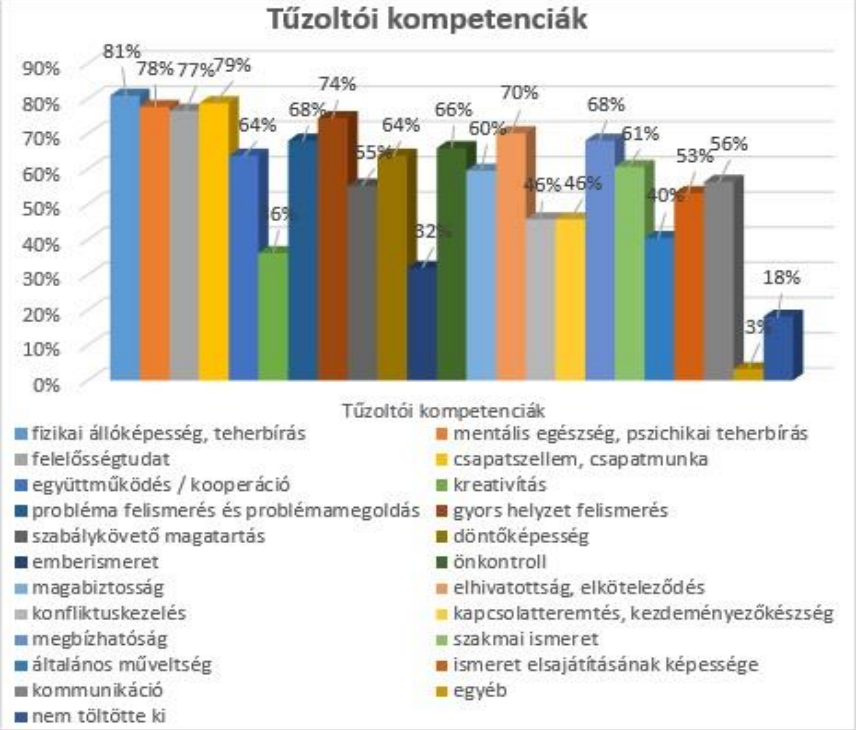
A szófelhő gyakoriságelemzés is alátámasztotta a fenti eredményt (lásd: 5. ábra és a szavakat összesítő 1. táblázat). A 11-es és a 12-es asszociációs kérdések válaszainak rögzítése után elkészült ábrákon a „SEGÍTSÉGNYÚJTÁS”, „SEGÍTSÉG”, „ÉLETMENTÉS”, „segítőkész” szavak, hangsúlyos nagy mérettű betűkkel szerepelnek, vagyis ezek meghatározó kulcskifejezések a tűzoltó szakmára, illetve tűzoltókra vonatkoztatva.

5. ábra 11-es, 12-es és 14-es kérdésekre adott válaszok szófelhő elemzése (saját szerkesztés)

Előforduló kulcsszavak	Kérdőív 11-es kérdésére adott válasza „Mi jut eszébe elsőként a tűzoltói hivatásról?”	Kérdőív 12-es kérdésére adott válasza „Ön szerint mi jellemzi a tűzoltót?”	Kérdőív 14-es kérdésére adott válasza „Amennyiben felvételt nyer, a tűzoltói hivatásban mit szeretne elérni?”	összesen
segítség, segítőkészség, segítségnyújtás	**48**	**23**	9	**80**
életmentés, mentés	9	0	5	**14**
bajba jutottak	4	0	2	**6**
veszély, veszélyes, veszélyhelyzetek	3	1	1	**5**
bátorság, vakmerő, félelmet nem ismerő	12	**39**	0	**51**
elhivatottság, hivatástudat, hivatás	**21**	**20**	3	**44**
cselekvőképesség	0	1	0	**1**
biztos munka	0	0	1	**1**
hazaszeretet	1	1	0	**2**
szolgálat	2	0	1	**3**

11. táblázat A visszatérő szavak előfordulásának számszerűsítése (saját szerkesztés)

A IV. felvetés – a fizikai és pszichikai teherbírás, illetve a csapatmunka kompetenciák hangsúlya megjelenik a jelentkezők pályaismeretében – azt gondolom, hogy teljes mértékben igazolódott, hiszen a megkérdezettek 81%-a a *„fizikai állóképesség, teherbírás”*, 79%-a a *„csapat szellem, csapatmunka”*, illetve 78%-a a *„mentális egészség, pszichikai teherbírás”* válaszlehetőségeket jelölte meg. Ezeken a válaszokon túl a „felelősségtudat” (77%) és a „gyors helyzet felismerés” (74%) lehetőségeket is sokan választották, mint ebbe a munkakörben szükséges kompetenciákat (lásd: 6. ábra).
Továbbá kijelenthető az is, hogy a szervezet által közvetített toborzó szöveg és a jelentkezők előzetes pályaképe között tartalmi összefüggés található, mivel – a tartalomelemzés során – mind a szervezet által kibocsátott üzenetben, mind pedig a kérdőív pályaképre vonatkozó kérdésére kapott válaszok között fellelhetők a *„segítségnyújtás”*, a *„bátorság”*, illetve az *„elhivatottság”* fogalmak.
Ez alapján elmondható, hogy a jelentkezők többsége tisztában van a tűzoltói munkakör kompetenciajellemzőinek sajátosságaival, illetve a pályaismeret, pályakép a szervezet által közvetített üzenet alapján egyezést mutat.



6. ábra Tűzoltói kompetenciák (saját szerkesztés)

A V. felvetés – a 2016. év és előző évek közötti időintervallumban demográfiai (életkor, lakhely, iskolai végzettség) változások figyelhetőek meg – csak részben igazolódott be, mivel – a trendvizsgálat során – a felsorolt demográfiai adatok közül az előző évek adataihoz képest a 2016-os eredményekben – csak a legmagasabb iskolai végzettség vonatkozásában mutatkozik meg jelentős eltérés (lásd: 7. ábra). Ennek oka a társadalmi, illetve a munkaerő piaci elvárásokban, valamint az oktatásban bekövetkező változások, amelynek köszönhetően a diplomások száma jelentős mértékben megnövekedett, a szakemberképzés pedig teljesen visszaszorult. Ez a hiányszakmák kialakulásával is kapcsolatban van. Éppen ezért azt gondolom, hogy a szakmák népszerűsítése, valamint átgondoltabb bérezése révén a helyzet stabilizálódna.

7. ábra Jelentkezők legmagasabb iskolai végzettsége (saját szerkesztés)

ÖSSZEFOGLALÁS

A felvetéseim következtetéseit és eredményeit az alábbi táblázatban foglaltam össze:

Kérdéskör	Felvetés	Teljesülés	Eredmény
A tűzoltói munkakörbe jelentkezők végzettségének irányvonala.	A tűzoltói munkakörbe szakképesítéssel rendelkezők jelentkezők közül a műszaki szakképesítés a jellemző.	teljesült	A szakképzettséget megjelölők többsége műszaki végzettséggel rendelkezik.
A pályaválasztás család illetve ismerősi kör befolyása.	A tűzoltói szakma választása közeli példa alapján jellemző.	részben	Míg a jelentkezők jelentős többségének közvetlen környezetében van tűzoltó, azonban csak kevesen erősítették meg motivációik megjelölésével, hogy befolyásolta volna őket a pályaválasztásukban.
A tűzoltó hivatás pálya motivációi a tűzoltó szakmáról alkotott kép tükrében.	A tűzoltó hivatás alap motívuma a bajbajutottakon való segítség, életmentés szándéka.	teljesült	A megkérdezettek jelentős többségének a segítségnyújtás szerepelt a pályaválasztási motivációiban.
A jelentkezők reális pályaismeretének vizsgálata a tűzoltói munkakörbe szükséges kompetenciákról.	A fizikai és pszichikai teherbírás, illetve a csapatmunka kompetenciák hangsúlya megjelenik a jelentkezők pályaismeretében.	teljesült	A választ adók többsége tisztában van az - általam vizsgált - munkakörbe szükséges kompetenciákkal.
A jelentkezők demográfiai (életkor, lakhely, iskolai végzettség) trendváltozásai 2016-ig.	A 2016. év és előző évek közötti időintervallumban demográfiai (életkor, lakhely, iskolai végzettség) változások figyelhetőek meg.	részben	A demográfiai adatok közül csak a legmagasabb iskolai végzettség az, ami egyértelmű változást mutat, ugyanis a főiskolai végzettségű jelentkezők száma dinamikusan növekszik az elmúlt 3 évet tekintve. Mind az életkorok, mind a lakhely alakulása tekintetében nem tapasztalható szignifikáns változás.

22. táblázat A felvetéseim következtetései és eredményei (saját szerkesztés)

FELHASZNÁLT IRODALOM

[1] FRIGY, É. Gy. (2017). *A Fővárosi Katasztrófavédelmi Igazgatóság tűzoltói munkakörbe történő kiválasztásrendszere és a jelentkezés motivációi.* Budapest: Szent István Egyetem Gazdaság- és Társadalomtudományi Kar Társadalomtudományi és Tanárképző Intézet (saját diplomamunka)

[2] NÉMET, T. (2015). A pályaválasztás és pályaorientáció vizsgálata egy empirikus kutatás során. *Hadtudományi Szemle VIII. évf. 1. szám*, 319-340. Forrás: http://uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi_szemle/szamok/2014/2015_1/15_1_alt_nemett.pdf

[3] MÜLLER, I. (2014). Pályaválasztást segítő kompetenciamérés. *Életpálya-tanácsadás III. szám*, 18-23. Forrás: http://epa.oszk.hu/02500/02512/00008/pdf/EPA02512_eletpalya_tanacsadas_2014_03_18-23.pdf

[4] PAPULA, L. (2008). Mi leszel, ha nagy leszel? A pályaválasztást meghatározó tényezők. *Bolyai Szemle, XVII. évf. 1. szám*. Forrás: http://uni-nke.hu/downloads/bsz/bszemle2008/1/02_papula.pdf

[5] CSIRSZKA, J. (1966). *Pályalélektan.* Budapest: Gondolat Könyvkiadó

[6] MIKES, L., & ÁGOSTON, F. (2014). *Adalékok a szegedi joghallgatók pályaképének vizsgálatához.* Szeged: Szegedi Tudományegyetem Állam- és Jogtudományi Kar. Forrás: http://www.juris.u-szeged.hu/download.php?docID=49865

[7] POGÁTSNIK, M. (2015). A pályadöntési folyamat, és az ezt alakító tényezők serdülő- és ifjúkorban. *EDU 5. évfolyam 2. szám*, 43-55. Forrás: http://epa.oszk.hu/02900/02984/00007/pdf/EPA02984_edu_2015_2_043-055.pdf

[8] KARNER, O. (2010). KARRIERTANÁCSADÓI KOMPETENCIÁK NEMZETKÖZI ÖSSZEHASONLÍTÁSA. *Alkalmazott Pszichológia XII. évf. 3-4. szám*, 87-105. Forrás: http://ap.elte.hu/wp-content/uploads/2015/07/APA_2010_3_4_KARNER.pdf

[9] Dr. HATVANI, A., BUDAHÁZY-MESTER, D., Dr. HÉJJA-NAGY, K. *Tanári személyiségfejlesztés és attitűdformálás* (e-learning anyag) – Super szivárványmodellje http://old.ektf.hu/hefoppalyazat/tanszemfejl/super_szivrvnymodellje.html

[10] RÓKUSFALVY, P. (1969). *Pályaválasztás és pályaválasztási érettség.* Budapest: Tankönyvkiadó

[11] MEIJERS, F., KUIJPERS, M., & GUNDY, C. (2013). The relationship between career competencies, career identity, motivation and quality of choice. *Int J Educ Vocat Guidance*, 13:47–66. Forrás: http://www.cdanz.org.nz/files/Symposium%202013/The%20relationship%20between%20career%20competencies,%20career%20identity,%20motivation%20and%20quality%20of%20choice.pdf

[12] NAGYNÉ BÁRES, A. (2016). Hatékony-e a korcsoportos motiváció? *Opus et Educatio III. évf. 5. szám*, 622-629. Forrás: http://epa.oszk.hu/02700/02724/00010/pdf/EPA02724_opus_et_educatio_2016_05_622-629.pdf

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

A GLOBÁLIS KATASZTRÓFA ELŐREJELZŐ ÉS KOORDINÁCIÓS, VALAMINT A KÖZÖSSÉGI VESZÉLYHELYZETI KOMMUNIKÁCIÓS ÉS INFORMÁCIÓS RENDSZEREK BEMUTATÁSA

THE INTRODUCTION OF GLOBAL DISASTER ALERT (GDACS), AND THE COMMON EMERGENCY COMMUNICATION AND INFORMATION (CECIS) SYSTEMS

HÁBERMAYER Tamás
(ORCID:0000-0002-6677-9163)
dr.habermayer.tamas@katved.gov.hu

- HARTNER Péter
(ORCID: 0000-0002-7099-9548)
peter.hartner@katved.gov.hu

- MUHORAY Árpád
(ORCID: 0000-0003-3832-293X)
muhoray.arpad@uni-nke.hu

Absztrakt

A katasztrófák és krízishelyzetek kezelése gyors beavatkozási képességet követel a nemzetközi szakértők és mentőcsapatok részéről csakúgy, mint a védekező ország erőitől. Rendkívül fontos, hogy a riasztás és a mentés megkezdéséhez szükséges információk a lehető leghamarabb eljussanak a megfelelő személyekhez, és a globális műveletek végrehajtása nemzetközi szinten is koordinálható legyen. Ennek lehetőségét teremtik meg a Globális Katasztrófa Előrejelző és Koordinációs-, valamint a Közösségi Veszélyhelyzeti Kommunikációs és Információs rendszerek, amelyeket a nemzetközi közösség alkalmaz. A szerzők betekintő tájékoztatást adnak az érintett rendszerek működésébe, és javaslatokat fogalmaznak meg a rendszerek alkalmazására.

Kulcsszavak: *Nemzetközi, katasztrófa, előrejelzés, kommunikációs és koordinációs rendszer*

Abstract

The reaction against disasters and crises requires the ability of fast intervene from international experts and teams, as well, as the forces of the defending country. It is extremely important that the alert and the necessary information for starting the rescue must be reach the proper person as soon as possible, and there must be a way to control the global operations efficiently from international level. The Global Disaster Alert and Coordination System (GDACS) and the Common Emergency Communication and Information System (CECIS) can handle this task, and are widely used by international experts. The authors shortly introduce these two systems and making suggestions how to use them efficiently.

Keywords: *International, disaster, early warning, communication and coordination system*

A kézirat benyújtásának dátuma (Date of the submission): 2018.03.17.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.05.04

BEVEZETÉS

Katasztrófák és krízisek esetén az általános elgondolás szerint akkor kerül sor nemzetközi segítség kérésére és igénybe vételére, amikor az érintett ország erői, eszközei már nem elegendőek a védekezéshez. Ez az elgondolás ugyanakkor pontosításra és kiegészítésre szorul, hiszen a nemzetközi erők, eszközök kérése már a felkészülés, és akár a későbbi, helyreállítás-újjáépítés időszakában is bekövetkezhet. Az egyes országok a jelenkor kockázatainak felismerésére és kezelésére, a veszélyeztetettségek felmérésére számos, különböző szempontrendszer szerint megalkotott, az egyes esetekre országonként is eltérő hatékonyságú technikát és módszert alkalmaznak. Ehhez hozzájárul, hogy a kockázatok felmérése során az országok általános fejlettségi szintje miatt is jelentősen eltérő eredmények születhetnek. A hagyományos tervezési rendszerek (megismert tények alapján történő felkészülés) az ismert és feltárt kockázatoknak megfelelően tudnak elsősorban hatékonyan reagálni, ezért ilyenkor kiemelten fontos, hogy minél több veszélyeztető hatás (akár más országok különböző módszerekkel végrehajtott elemzése által feltárt) felismerése és számításba vétele megtörténjen. Egyes újabb rendszerek már nem a megtörtént eseményekre alapoznak, hanem a veszélyes folyamatok időbeli felismerésével, a kockázatok irányába történő jelző és radar, valamint monitoring rendszerek kiépítésével dolgoznak. Bármelyik tervezési formáról is beszélünk, nemzetközi szinten szükséges egy olyan rendszer, amely a világ különböző pontjain, eltérő szakterületen, de közös cél érdekében dolgozó szakértőket összefogja. Ezt a feladatrendszert az ENSZ a Globális Katasztrófa Előrejelző és Koordinációs rendszer (Global Disaster Alert And Coordination System – GDACS) és az Európai Unió a Közösségi Veszélyhelyzeti és Információs Rendszer (Common Emergency Communication And Information System - CECIS) segítségével valósítja meg. Felmerülhet a kérdés, hogy Magyarország számára milyen hasznosulást jelent egy ilyen rendszerekbe történő regisztráció, valamint a használat egy ország szempontjából milyen lehetőségeket rejt magában.

A GLOBÁLIS KATASZTRÓFA ELŐREJELZŐ ÉS KOORDINÁCIÓS RENDSZER (GDACS)

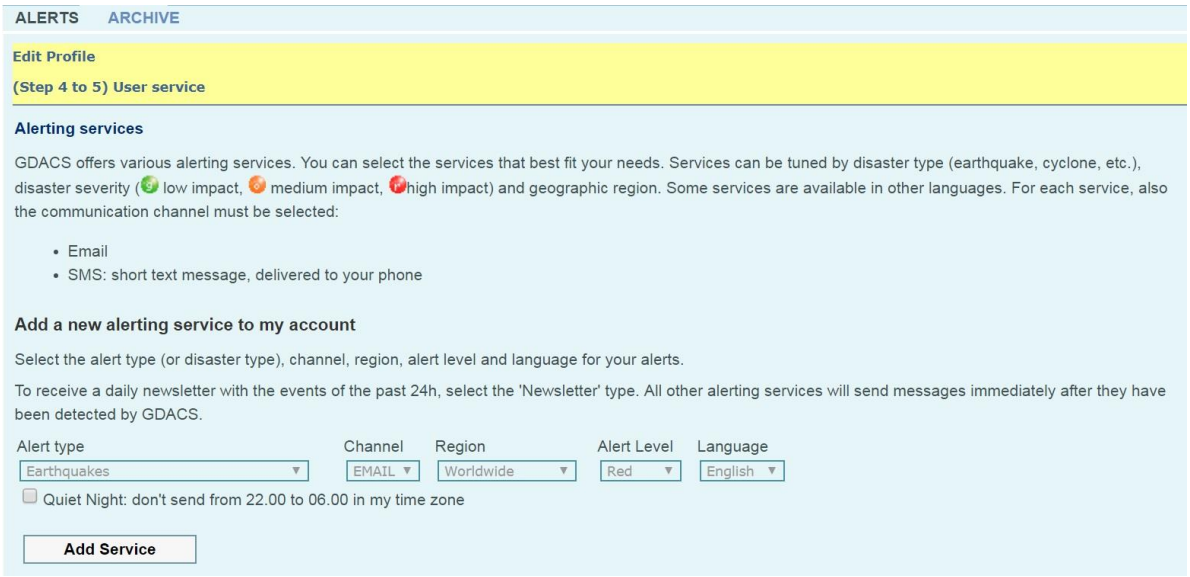
A több részegységből álló, integrált rendszer az ENSZ és az EU közötti együttműködés részeként jött létre 2004-ben. A célja az volt, hogy hatékonyabbá tegye a nemzetközi szervezetek és a katasztrófavédelmi szakértők közötti kommunikációt, különösen a káresemények bekövetkezésének kezdeti szakaszában. Az eltelt közel 15 év alatt a rendszer folyamatosan fejlődött és mind a mai napig egyre bővülő funkciókkal használatban van. A www.gdacs.org weboldalról elérhető a jelenlegi 4 fő rész: riasztások (Alerts), virtuális helyszíni művelet - irányító központ (Virtual On-Site Command Center - VOSOCC); adat - térképtár és műholdképtár (Data, Maps and Satellite Imagery), tudományos portál (Science Portal). Az oldal felhasználóinak számát tekintve a virtuális helyszíni művelet - irányító központot közel 32.000-en, a riasztások felületet közel 25.000-en használják világszerte. A térképeket és műholdképeket kiemelt nemzetközi szervezetek, az (United Nations Institute for Training and Research Operational Satellite Applications Programme – UNOSAT) és MapAction biztosítják, a tudományos portál működtetését az Európai Tanács Műveleti Kutató Központja (European Commission Joint Research Centre) végzi. Az integrált rendszer a létrejötte óta számos alkalommal bizonyította hatékonyságát, amelyet az egyre magasabb szintű, nemzetközi szervezetek közötti interoperabilitás megkövetel. A katasztrófavédelmi és humanitárius szervezetek működése egyre hatékonyabbá és gyorsabbá vált, amely nagymértékben köszönhető a GDACS rendszeren keresztül történő kommunikációnak és információáramlásnak. Magyarországon a rendszer hatékony felhasználója a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (BM OKF) Nemzetközi Főosztálya.

1. ábra: a Globális Katasztrófa Előrejelző és Koordinációs rendszer – www.gdacs.org (a szerzők szerkesztése a [1] alapján)

A rendszer arab, angol, francia és spanyol nyelven érhető el, a kezdőlap kialakítása a célszerűséget tükrözi. Az 1. számú ábra szerint a portál tetején a megnevezés, valamint a nemzetközi szervezetek logója található, balról jobbra haladva a kiadott legfrissebb katasztrófa - riasztások, majd a virtuális helyszíni művelet - irányító központban folyamatban lévő katasztrófa beavatkozások. Továbblépve a portál legfrissebb hírei, illetve a tagok részére a bejelentkező felület található. A felsoroltak kiegészülnek a weboldal alján látható, katasztrófák helyszínét bemutató világtérképpel, illetve a térkép alatti részen további információk, mobil applikáció letöltés és közösségi weboldalak hozzáférése található.

KATASZTRÓFA – RIASZTÁS A GLOBÁLIS KATASZTRÓFA ELŐREJELZŐ ÉS KOORDINÁCIÓS RENDSZERBEN

A riasztások funkció előzetes regisztrációhoz kötött, amely során a felhasználónév, jelszó, email cím megadásával azonosítanunk kell magunkat, szervezetünket, illetve meg kell adnunk a regisztrációnk célját. Ezen információk kitöltése után választanunk kell, hogy emailban, vagy sms-ben kapjunk értesítést az eseményekről (hangposta és fax funkció is létezik). Ki kell töltenünk, hogy milyen típusú események bekövetkezésére kérünk riasztást (jelenleg földrengés, cunami, trópusi ciklon, hírlevelek érkezése választható). Meg kell adnunk a 2. ábrán bemutatott módon, hogy melyik régiókban bekövetkezett eseményekről akarunk tudni (pl. világszinten, Ázsia, Európa, Afrika), illetve, hogy rendszerhez tartozó mely riasztási fokozat érdekel bennünket (piros – legveszélyesebb, legnagyobb kihatással bíró, narancs – közepes kihatással bíró, illetve zöld – legkisebb kihatással bíró események). Végül beállíthatjuk, hogy milyen nyelven kérjük a riasztást (angol, spanyol, francia).



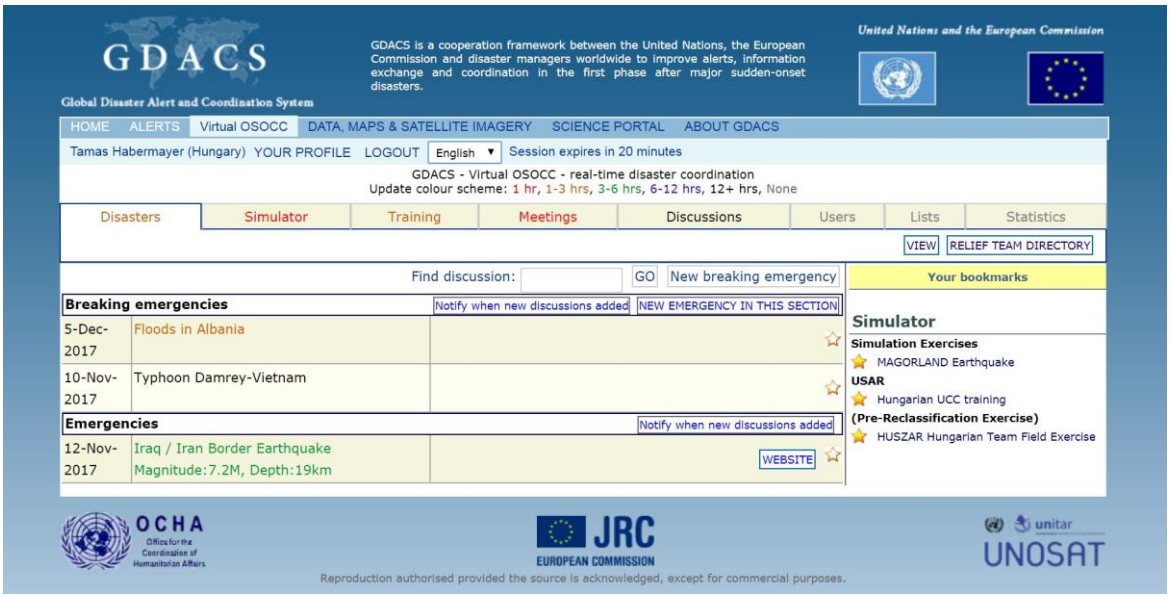
2. ábra: a Globális Katasztrófa Előrejelző és Koordinációs rendszer katasztrófa - riasztás regisztrációs felülete (a szerzők szerkesztése az [1] alapján)

A sikeres regisztrációt követően a választásunknak megfelelően kapunk tájékoztatást a bekövetkezett eseményekről. Az integrált weboldal riasztási felülete kiemelt fontossággal bír, hiszen az események bekövetkezése és jelzésük rendszerbe történő megérkezése után szinte azonnal küld riasztást a regisztrált felhasználóknak, akik így jelentősebb időbeli késedelem nélkül értesülnek, és be tudnak kapcsolódni a nemzetközi segítségnyújtás feladataiba. Mindazon káresemények bekövetkezésénél, ahol a mentésnél, ill. a védekezésnél rendelkezésre álló idő korlátozott, (pl. földrengések esetében az első 100 óra a kritikus idő) a riasztás elindítja és felgyorsítja a szervezetek közötti kommunikációs és szervezési feladatokat, gyorsabb információáramlást tesz lehetővé. Véleményünk szerint hasonló riasztási felületet ki lehetne alakítani Magyarországon is a szakértői szintű katasztrófavédelmi önkéntesek számára.

Jellemző, hogy a riasztás alapján az érintett katasztrófavédelmi szakemberek azonnal belépnek a virtuális helyszíni művelet - irányító központ felületére, ahol tovább tudnak tájékozódni (pl. a katasztrófa sújtotta ország igényel-e nemzetközi segítséget). A tájékoztatás következő lépcsője, hogy ezek után akár a saját képviselt szervezetüket is értesítik (pl. városi kutató-mentő csapatok, humanitárius szervezetek) és azok ez alapján megkezdik a műveleti feladataik végrehajtását.

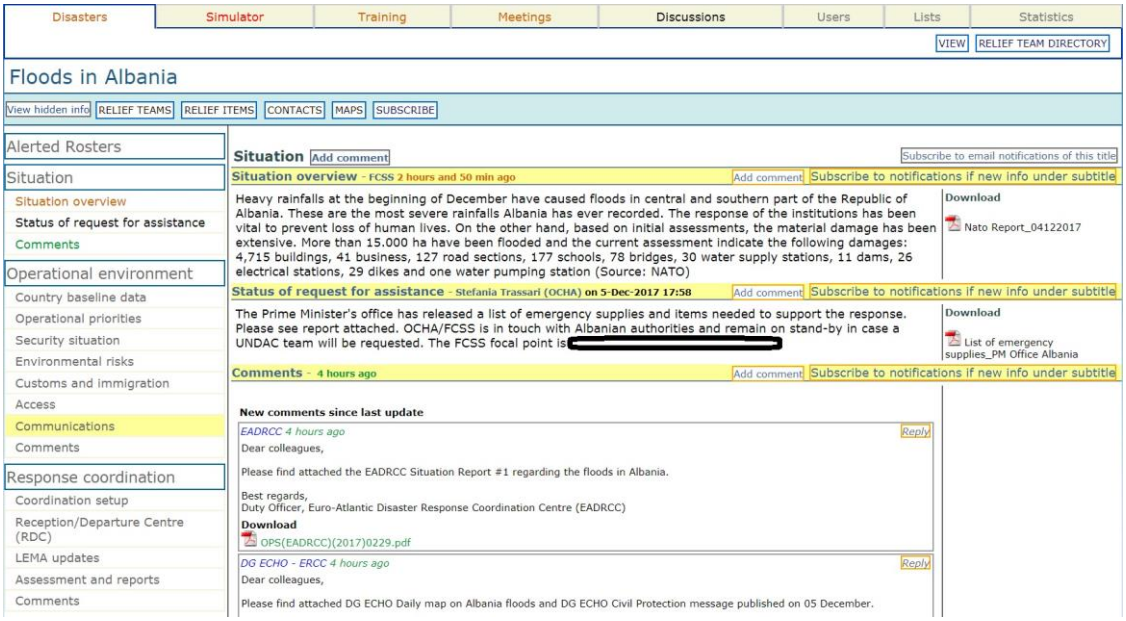
VIRTUÁLIS HELYSZÍNI MŰVELETIRÁNYÍTÓ KÖZPONT A GLOBÁLIS KATASZTRÓFA ELŐREJELZŐ ÉS KOORDINÁCIÓS RENDSZERBEN

A virtuális helyszíni műveletirányító központ a GDACS része, az ENSZ Humanitárius Ügyeket Koordináló Hivatala (UN OCHA) által menedzselt on-line kommunikációs eszköz. A belépés a felhasználók számára előzetes regisztrációhoz kötött, amely során a munkakörről, képviselt szervezetről, nemzetközi szervezetben betöltött tagságról nyilatkozni kell. A kiképzés (Training), szimuláció (Simulator), értekezletek (Meeting), megbeszélések (Discussions) funkciók mellett ezen a felületen történik egy éles helyzet kezelése is, amely a katasztrófa (Disaster) menüpont megnyitása során érhető el. Itt a folyamatban lévő katasztrófák nyilvántartását érhetjük el, amelyből a kijelölt megnyitása azonnal előhozza a kapcsolódó legfontosabb információkat.



3. ábra: a Globális Katasztrófa Előrejelző és Koordinációs rendszer virtuális helyszíni műveletirányító központ felülete (a szerzők szerkesztése az [1] alapján)

A weboldal a szövegezésben színkódokat használ, ahogy a 3. számú ábrán is látható. A legfrissebb információk vörös színnel jelennek meg (1 órán belüli közlés). Barna szín jelzi az 1-3, zöld a 3-6, kék a 6-12 órán belüli, majd fekete a 12 óra eltelte utáni információkat. A felületen lehetőség van a tartalomban keresni (Find discussion), illetve katasztrófahelyzetet a nemzetközi közösség számára bejelenteni (New breaking emergency). A könyvjelző (Bookmarks) egy felhasználóbarát funkció, használatának segítségével a fontosnak tartott események kiemelhetőek, így a weboldalon a keresés jelentősen leegyszerűsödik. Lehetőségünk van még a felhasználók név vagy ország szerinti keresésére (Users), különböző listák (pl. szakértők névjegyzéke) lekérésére (Lists), illetve a virtuális helyszíni műveletirányító központ statisztikai adatainak megtekintésére (Statistics).



4. ábra: a Globális Katasztrófa Előrejelző és Koordinációs rendszer virtuális helyszíni műveletirányító központ – katasztrófák felülete (a szerzők szerkesztése a [1] alapján)

A konkrét katasztrófa kiválasztásával eljuthatunk az adott esemény tájékoztató és műveleti felületére. A teljesség igénye nélkül - itt megtalálhatjuk a nemzetközi riasztott egységek adatait (Alerted rosters), illetve amennyiben volt, akkor a kárt szenvedett ország nemzetközi segítség kérésére tett nyilatkozatát (Status of request for assistance). A megfelelő helyre kattintva a védekezésben érintett szervezetek képességeit láthatjuk (Relief teams), megtalálhatjuk a kapcsolattartásra (Contacts), illetve a környezeti biztonságra vonatkozó információkat (Security situations). Megfelelő feltöltés után az ország adatok (Country baseline data), a műveleti prioritások (Operational priorities), a környezeti kockázatok (Environmental risks), vám és bevándorlási szabályok (Customs and immigration) egy helyen megtalálhatóak.

A feltöltések minőségére és tartalmára a nemzetközi közösség kiemelt figyelmet fordít, az esetek döntő többségében ezt a feladatra speciálisan felkészített katasztrófavédelmi szakember (jellemzően összekötő – liaison) végzi el. A feladatok végrehajtását segíti a műveleti koordinációs rész (Response coordination), ahol a nemzetközi koordinációt elősegítő szabályok (Coordination setup), az indító/fogadó központokra vonatkozó információk (Reception/departure centre), a helyi hatóságok közlései (LEMA updates), jelentések és értékelések (Assessment and reports) találhatóak. A felület legújabb fejlesztése – amely elsősorban földrengések bekövetkezése esetén lényeges – a városi kutatást - mentést koordináló egység (USAR Coordination Cell -UCC) feladatrendszerét, közöttük a Kobo Toolbox rendszer alkalmazását, illetve a veszélyhelyzeti orvosi csapat (Emergency Medical Team - EMT) műveletének információit foglalja magában. Ezen részekhez a feltöltést már teljes mértékben felkészített informatikai vagy orvos szakembereknek kell végezniük, akik munkájából az összes többi csapat a közös platformon dolgozni és kommunikálni fog.

A következő rész a szimulátor felület, melynek segítségével a felhasználóknak, gyakorlatok szervezőinek lehetőségük van az éles alkalmazáshoz hasonló rendszerkörnyezetben dolgozni. Ezen részben a fórumszerű felületen adminisztrátori jogosultsággal rendelkezik a regisztrált felhasználó, így a programot a gyakorlatok igényeinek megfelelően át lehet alakítani, illetve speciális funkciókhoz is hozzá lehet férni. Megfelelő felkészülés és az adatok feltöltése után a valóságoshoz rendkívül hasonló körülmények teremthetőek. Ez lehetőséget biztosít a szakértők számára a feladatok begyakorlására, illetve a kiképzés alatt állók kockázatok nélküli gyakoroltatására. A szimulátor az alábbi fő kategóriákban jelenít meg adattartalmat (dátumhoz kötött programokat):

Megnevezés	Angol megnevezés
Szimulációk és kiképző hálózatok	Simulations and Training Networks
Szimulációs gyakorlatok	Simulation Exercises
Városi kutatás- mentés gyakorlatai	INSARAG
EU kiképzések	EU Training
ENSZ Civil – Katonai Együttműködési gyakorlatok	UN-CMCoord
Helyszíni műveleti központ gyakorlatok	OSOCC
PREP gyakorlatok	PREP training

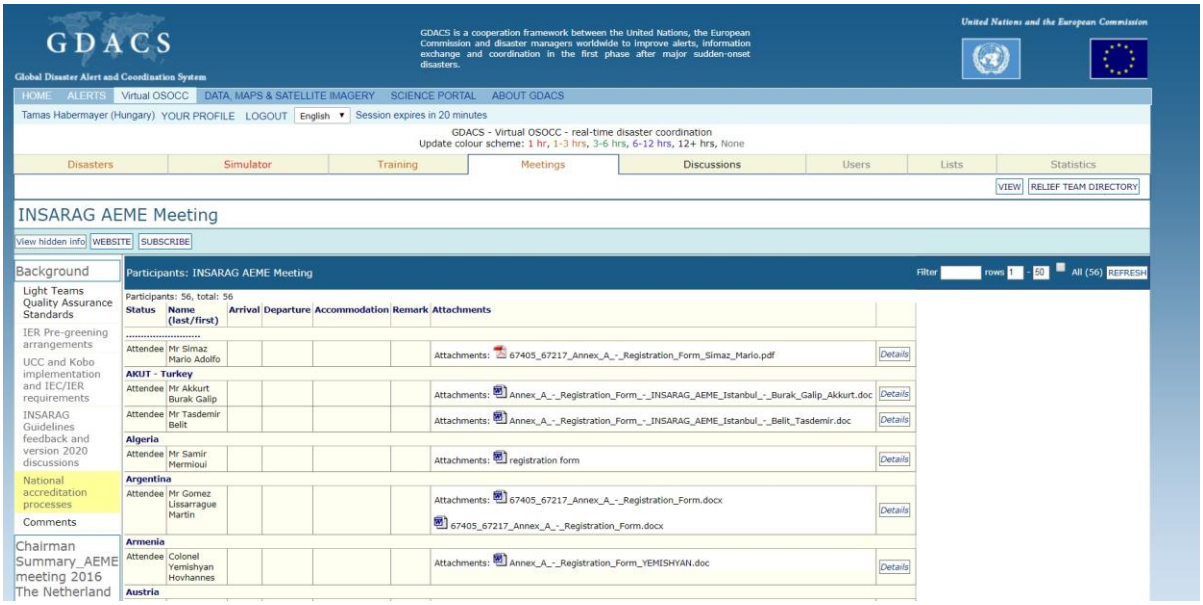
1. táblázat: a Globális Katasztrófa Előrejelző és Koordinációs rendszer virtuális helyszíni művelet irányító központ – szimulátor kategóriák (a szerzők szerkesztése a [1] alapján)

5. ábra: a Globális Katasztrófa Előrejelző és Koordinációs rendszer virtuális helyszíni műveletirányító központ – szimulátor felülete (a szerző szerkesztése a [1] alapján)

A szimulátort követi a találkozók (meetings) felület, amelyen szakterületenként (Pl. INSARAG) rögzíti a nemzetközi közösség által szervezett programokat, eseményeket, kiképzéseket. Az alábbi ábrán látható, hogy a dátum és megnevezés mellett a helyszín, a kapcsolattartó személyek, a státusz, regisztrálhatóság és a szervezői weboldal tekinthető meg az oldalon, a találkozók felületén.

6. ábra: a Globális Katasztrófa Előrejelző és Koordinációs rendszer virtuális helyszíni művelet irányító központ – találkozók felülete (a szerzők szerkesztése a [1] alapján)

Egy találkozót kiválasztva hozzá lehet jutni a kapcsolódó legfontosabb információkhoz, így lehetőség van részt venni a nemzetközi közösség munkájában még akkor is, ha fizikailag az adott találkozón nem tudunk részt venni. Listázni lehet a résztvevőket, és könnyedén megtalálhatjuk az adott témakör szakértőjét, esetenként le tudjuk tölteni a komplett munkaanyagot. Az következő ábrán egy INSARAG találkozó felületének egy részét láthatjuk. A háttér információk (Background) rész taglalja a találkozó legfontosabb kérdéseit, a résztvevők (Participants) résznél pedig láthatjuk, hogy 56 szakértő regisztrált (országonként, vagy nemzetközi szervezetenként csoportosítva).



7. ábra: a Globális Katasztrófa Előrejelző és Koordinációs rendszer virtuális helyszíni művelet irányító központ – INSARAG AEME találkozó (a szerzők szerkesztése a [1] alapján)

AZ EURÓPAI UNIÓ POLGÁRI VÉDELMI MECHANIZMUSA

Az Európai Uniós polgári védelmi segítségnyújtás olyan humanitárius tevékenység, amely egy katasztrófa bekövetkezését követően az azonnali segítségnyújtásra, a védekezések támogatására, a károk enyhítésére, valamint a katasztrófa következményeinek helyreállításra irányul. Ez történhet például természetbeni segítség formájában, speciálisan képzett és felszerelt csapatok küldésével, vagy a katasztrófa helyszínén történő beavatkozások hatékonyságának fokozásával (nemzetközi megfigyelők és szakértők értékelése és műveleti koordinációja). Tényként rögzíthető, hogy mivel a katasztrófák nem ismernek határokat, a nemzetközi segítségnyújtás során tett erőfeszítések duplikálásának elkerüléséhez, valamint a katasztrófa sújtotta területeken jelentkező valós igények és a tagállamok által nyújtott felajánlások egyeztetéséhez egy jól koordinált, európai szintű válaszra van szükség. Ennek érdekében 2001-ben hozták létre az Európai Unió Polgári Védelmi Mechanizmusát [2], amely az európai nemzeti polgári védelmi szervezetek közötti szorosabb együttműködést volt hivatott elősegíteni. Jelenleg a Mechanizmus 28 Európai Uniós tagállamból áll, amelyet Izland, Montenegró, Norvégia, Szerbia, Albánia, Macedónia és Törökország részvétele egészít ki.

A Mechanizmus működésének célja, hogy a katasztrófa segítségnyújtást a lehető leghatékonyabb módon, koordináltan valósíthassák meg a természeti és civilizációs katasztrófák beavatkozói. A közelmúlt nagyszámú veszélyhelyzetére válaszul az Európai Bizottság 2017. novemberben bejelentette, hogy további tervet dolgoz ki az Unió polgári védelmi reagálásának erősítésére annak érdekében, hogy támogassa a tagállamok hatékonyabb

reagálási képességét, illetve a természeti és civilizációs katasztrófákra történő felkészülését. A terv végrehajtásának egyik legfontosabb eleme a Mechanizmus műveleti irányító központja (Veszélyhelyzeti Reagálási Koordinációs Központ - Emergency Response Coordination Center; a továbbiakban: ERCC), amely 0-24 órában folyamatosan nyomon követi a világban, de elsődlegesen Európában bekövetkezett, vagy várható katasztrófákat, valamint koordinálja a segítségnyújtásban részt vevő tagállamok munkáját. Szintén kiemelt szerepet kap a Közösségi Veszélyhelyzeti és Információs Rendszer, a CECIS, amely az Európai Unió és a tagállamok katasztrófák elleni védekezésre hivatott szervezetei közötti biztonságos kommunikációt, a nemzetközi felajánlásokat, a valós idejű eseménykövetést, és az erő - eszköz nyilvántartást biztosítja. A rendszer működésének egyértelmű hasznossága az Európai Számvevőszék Uniós Polgári Védelmi Mechanizmust vizsgáló 2016-os külön jelentésében is megjelenik, mely alapján a további fejlesztésekre tesznek javaslatot az uniós számvevők [3: 25-26].

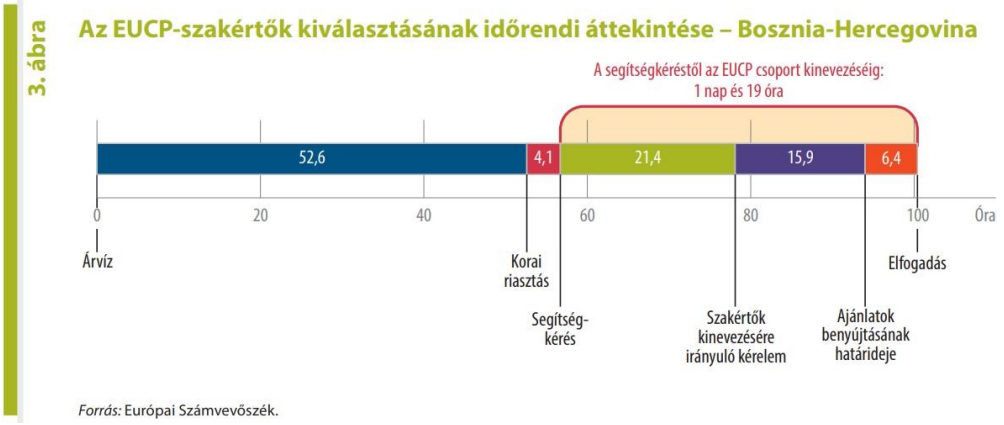
8. kép Az ERCC monitorozza a Mexikóvárosban bekövetkezett földrengést (a szerzők szerkesztése az [4] alapján)

A rendszer segítségével a tagállamok az előre felkészített és önellátó polgári védelmi moduljaiknak köszönhetően azonnal képesek beavatkozni mind az Európai Unió területén, de az EU képviseletében akár azon kívül is. 35 feletti a tagországok részéről beregisztrált modulok száma, akik többek között olyan speciális feladatok végrehajtását vállalják, mint a kutatás és a mentés, a légi tűzoltás, vagy tábori kórházak működtetése. Fontos tény, hogy a világon bármely ország kérheti az Európai Unió Polgári Védelmi Mechanizmusának segítségét, nem szükséges tagállamnak vagy szerződött államnak lennie. A 2001-es megalapítás óta a Mechanizmuson keresztül több mint 300 katasztrófa eseményeinek a követése, illetve 200 segítségkérés koordinációja valósult meg. A működés sikeresen hozzájárult a világon a legpusztítóbb katasztrófákat követő helyreállításokhoz. Ezek közül kiemelhetjük a 2010-es haiti földrengést, a 2011-es japán hármas katasztrófát, a 2013-as Fülöp-szigeteki Haiyan tájfunt, a 2014-es szerbiai és bosnyák árvizet majd az ebola járványt és az ukrán konfliktust, végül a 2015-ös nepáli földrengést.

Az uniós szintű polgári védelmi rendszer képzési lehetőséget is biztosít a résztvevő országok kutató-mentő csapatai számára. A jó gyakorlatok és tapasztalatok megosztásával, valamint a közös képzésekkel a résztvevők tovább növelhetik hatékonyságukat a katasztrófa - reagálás területén. A BM OKF szakértői éves rendszerességgel tartanak hazai képzéseket bevonva azokba a külföldi partnereket, bemutatva számukra a hazai eljárásokat és legjobb gyakorlatokat. Emellett a hazai szakértők számos alkalommal vettek részt a szakterületüknek megfelelő felkészítésen külföldön. Erre szükség is van a szakemberek képzettségi színvonalának emelése, a beavatkozások hatékonysága miatt, illetve azért, mert az Európai Számvevőszék a későbbiekben a felajánlott szakértők szakmai teljesítményét és személyi magatartását [3: 18] is értékelni kívánja. A rendszer fejlesztését fogja továbbá szolgálni, hogy jelentős mértékben csökkenteni kívánják a szakértők kiküldésének döntéshozatali idejét, amely további professzionalizálódást kell, hogy jelentsen a szakértőket jelölő szervezeteknél [3: 16-17].

21

Az Unión kívüli katasztrófák esetében az EUCP-csoportok bevetése nem függ a kérelmező/érintett ország jóváhagyásától. Az ERCC számára ezért megengedett, hogy a segítségkérés beérkezése után azonnal kinevezésekre vonatkozó megkereséseket küldjön a részt vevő államoknak. Nepál és Bosznia-Hercegovina esetében már korai jelzések utaltak arra, hogy az események súlyossága miatt minden valószínűség szerint szükség lesz uniós koordinációra. Ennek ellenére a két katasztrófahelyzet esetében a hivatalos segítségkérés és a CECIS rendszerben az első csoport tagjainak kinevezésére vonatkozó kérelem beérkezése között Bosznia-Hercegovina esetében 21,4 óra, Nepál esetében pedig 22,8 óra telt el (lásd: ***3. ábra*** és ***4. ábra***).



9. ábra: az European Union Civil Protection - EUCP- szakértők kiválasztásának időrendi áttekintése Bosznia – Hercegovina (a szerzők szerkesztése az [3:16] alapján)

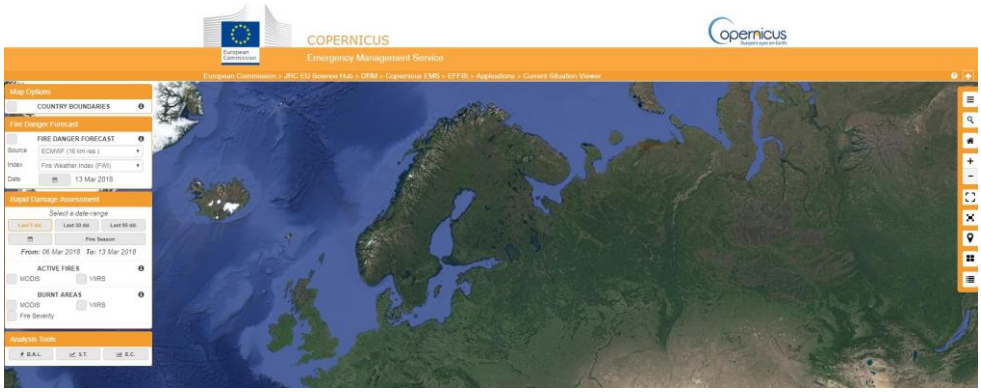
A képzéseken túl a Mechanizmus veszélyhelyzeti kommunikációs és megfigyelő eszközöket is biztosít a CECIS-en keresztül, amelynek felügyeletét az Veszélyhelyzeti Reagálási Koordinációs Központ, az ERCC központ látja el. Az Európai Bizottság különösen támogatja a tagállamok katasztrófa megelőzésre és felkészülésre irányuló törekvéseit, azokra a területekre koncentrálva, amelyek esetében egy összeurópai megközelítés hatékonyabbnak bizonyulhat, mint az egyes tagállamok nemzeti megoldási javaslatai és egyéni beavatkozásai. Ide tartozik a katasztrófákra vonatkozó információk minőségének és elérhetőségének javítása, az ellenálló képesség fokozása, valamint a korai előrejelző rendszerek erősítése.

Jelen korunkban extrém időjárás rendkívül rövid idő alatt bárhol és bármikor előfordulhat, amely a váratlanság okán sokszor nemzeti szinten is nehézzé teszi a reagálás megszervezését. Ilyenkor szinte lehetetlenné válik a nemzetközi megerősítő erők igénybe vétele. Előfordulhat, hogy erre mégis szükség van, hiszen a katasztrófák nem ismernek határokat, és a káresemény kapcsán akár több ország szervezett formában együtt kell, hogy működjön a következmények

felszámolásában. Amennyiben egy fejlődő országban következik be katasztrófa, a polgári védelmi segítségnyújtás bonyolódik, és jellemzően Európai Uniós humanitárius segítségnyújtással párosul.

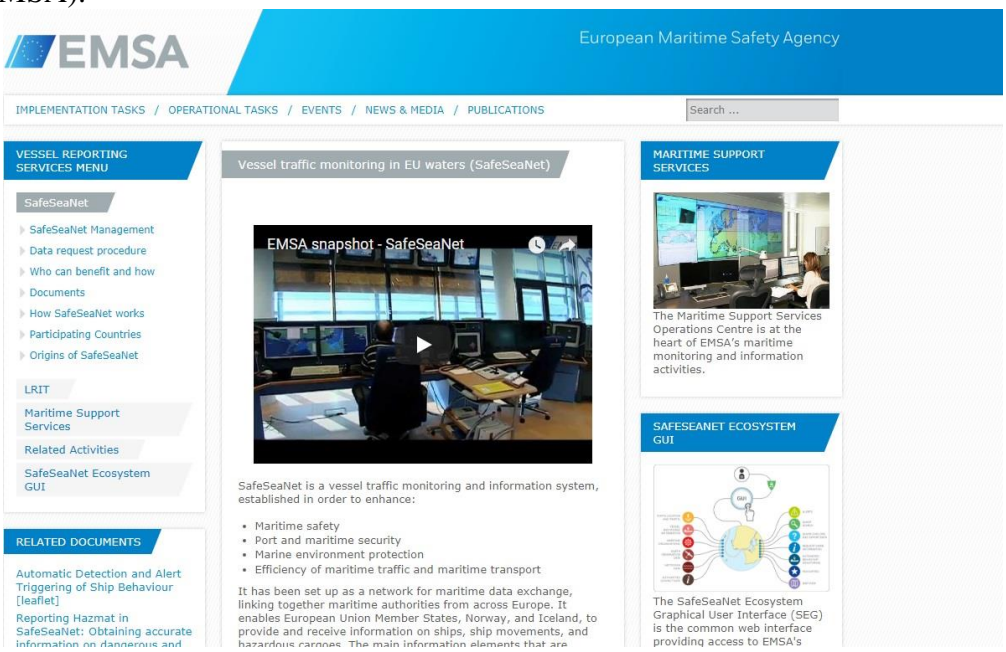
Az Európai Unióban számos rendszer működik, amelyek használatával jelentősen növelhető a megbízható információk áramlása, a szakértői szintű anyagok továbbítása, átadása, ugyanúgy az országhatárokon túlnyúló veszélyek előrejelzése. Az alábbiakban néhány példán keresztül bemutatjuk ezeket a rendszereket.

A Bizottság Környezetvédelmi és Fenntarthatósági Intézete (Institute for Environment and Sustainability; a továbbiakban: IES) fejlesztette ki az Európai Erdőtűz Információs Rendszert (European Forest Fire Information System; a továbbiakban: EFFIS). Míg előbbi minden jelentősebb árvízről tájékoztatja az ERCC központot, utóbbi napi meteorológiai tűzveszélyességi térképet és előrejelzést készít a következő 6 napos időszakra, szemléltetve a leégett területeket és a keletkezett károkat.



10. ábra: az Európai Erdőtűz Információs Rendszer térképi felülete (a szerzők szerkesztése az [5] alapján)

A Mechanizmus a tengeri katasztrófák esetén is segítséget nyújt, amelynek során szorosan együttműködik az Európai Tengerbiztonsági Ügynökséggel (European Maritime Safety Agency; EMSA).



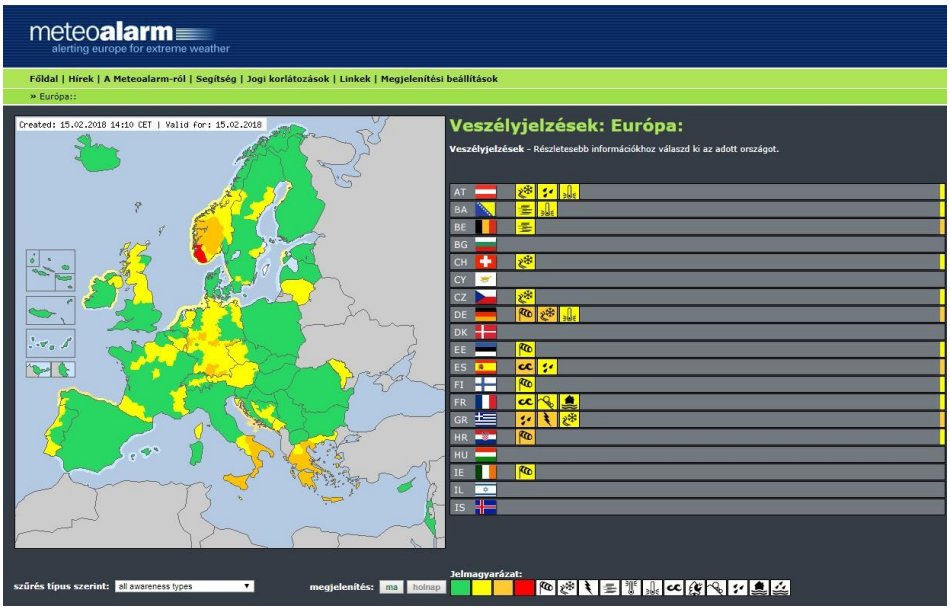
11. ábra: az Európai Tengerbiztonsági Ügynökség weboldala (a szerzők szerkesztése az [6] alapján)

Az Európai Mediterrán Szeizmológiai Központtal (European Mediterranean Seismological Centre; EMSC) kötött megállapodás lehetővé teszi a földrengések gyors és pontos előrejelzését a Mediterrán régióban.

12. ábra: az Európai Mediterrán Szeizmológiai Központ weboldala (a szerzők szerkesztése a [7] alapján)

Az Európai Bizottság szintén együttműködik a Kormányközi Oceanográfiai Bizottsággal annak érdekében, hogy szökőár előrejelző rendszereket létesítsen az észak-atlanti és a mediterrán régiókban.

A Meteoriasztási platform (Meteoalarm) egy online riasztási felület, amelyet az európai meteorológiai szolgálatok hoztak létre azzal a céllal, hogy előrejelzéseket készítsenek a tagállamok számára.



13. ábra: a Meteoriasztási platform (a szerzők szerkesztése a [8] alapján)

A legtöbb korai riasztási és előrejelző rendszer az Európai Unió tagállamainak területéről gyűjt és oszt meg információkat, működésüket és fejlesztésüket az Európai Unió finanszírozza. A Mechanizmus a katasztrófa kockázat értékelés és az adatok elemzése során minél szélesebb spektrumon keresztül gyűjti az információkat, és azok megosztásával célja a várható károk enyhítése, valamint a lehető legalaposabb felkészülés.

VESZÉLYHELYZETI REAGÁLÁSI KOORDINÁCIÓS KÖZPONT (ERCC)

Egy katasztrófa bekövetkezését követően a reagálásnál minden perc számít. Az életmentés érdekében azonnali, koordinált és előre megtervezett válaszadásra van szükség. Ez fokozottan igaz a klímaváltozás következtében állandósuló és egyre nagyobb számban előforduló természeti és civilizációs katasztrófák esetében, valamint a növekvő népesség, a városiasodás és a fokozott ipari tevékenység miatt. A szolidaritás szellemében az Európai Unió támogatja a katasztrófákra történő időbeni és hatékony reagálást, az Unió igyekszik biztosítani, hogy a segítségnyújtás során a valódi szükségleteknek megfelelő segítség és segély érkezzen a helyszínre az áldozatokhoz bárhol a világon.

Az ERCC központ az Európai Unió Polgári Védelmi és Humanitárius Segítségnyújtási Főigazgatóságának (DG ECHO) keretén belül létesült. A világon bármely ország közvetlenül segítségért fordulhat hozzá. Feladata a gyors reagálás lehetővé tétele, amelynek érdekében a Mechanizmus 34 országának erőforrásait használja fel. Az ERCC központ a korábban hasonló feladatot ellátó Monitoring és Információs Központ (Monitoring and Information Centre**;** MIC) feladatkörét vette át. Az ERCC a különböző időzónákban bekövetkező katasztrófák egyidejű kezelésével és nyomon követésével látja el a koordinációs feladatait, ezzel egy koherens európai reagálást valósít meg, valamint lehetővé teszi a fölöslegesen drága és szükségtelen duplikációk elkerülését. A Központ valós idejű információkat gyűjt és elemez, nyomon követi a veszélyforrásokat, megtervezi a szakértők, csapatok és felszerelések vezénylését és bevetését, valamint együtt dolgozik a tagállamokkal az elérhető erőforrások feltérképezésében.

KÖZÖS VESZÉLYHELYZETI KOMMUNIKÁCIÓS ÉS INFORMÁCIÓS RENDSZER (CECIS)

A Közös Veszélyhelyzeti Kommunikációs és Információs Rendszer (CECIS) egy olyan internet-alapú alkalmazás, amely a regisztrált nemzeti kapcsolattartó felhasználók számára lehetőséget biztosít hiteles katasztrófa riasztások küldésére és fogadására, a segítségkérés részleteinek megosztására, katasztrófa segítségnyújtások felajánlására, valamint az aktuális veszélyhelyzetek valós idejű nyomon követésére. Az alkalmazás fő feladata, hogy interaktív felületet biztosítson a segítségnyújtás során potenciálisan elérhető eszközök számára, ezek alapján kezelje a segítségkéréseket, lehetőséget biztosítson a felhasználók közötti információ megosztásra, valamint dokumentálja az eseményeket és üzeneteket. A CECIS-ben regisztrált modulok az Európai Veszélyhelyzeti Reagálási Kapacitás nyilvántartásába (Önkéntes Eszköztár – Voluntary Pool) kerülnek, ahol a Mechanizmusban részt vevő tagállamok által önkéntesen és előzetesen felajánlott erőforrások érhetőek el. A tagállamok részéről a modulok egyértelműen meghatározott képességei, valamint a dokumentált felajánlások kiszámítható, gyors és megbízható Uniós szintű reagálást tesznek lehetővé. A CECIS alkalmazás felhasználói az Európai Unió tagállamai, valamint Izland, Liechtenstein, Szerbia, Macedónia, Törökország, Albánia és Norvégia. A felhasználó országok hivatalos kapcsolati pontjai 0-24 órában elérhetőek.

Az Egyesült Nemzetek Szervezete (a továbbiakban: ENSZ) hasonló céllal létrehozott Globális Katasztrófa Riasztási Koordinációs Rendszere (Global Disaster Alert Coordination System; a továbbiakban: GDACS) több szempontból azonos feladatokat lát el, mint az EU CECIS rendszere. A két alkalmazás azonban a –felhasználóit tekintve különbözik egymástól. A CECIS rendszerben az országok jellemzően egyetlen felhasználói profillal rendelkeznek, így a nyílt, magánszemélyként történő regisztrálásra nincsen lehetőség. A GDACS rendszer ennek az ellentéte, amely több tízezres nagyságrendű felhasználói létszámmal rendelkezik. Ez a különbség a segítségnyújtás kérésekor és elfogadásakor rendkívül fontos, hiszen a CECIS rendszer felhasználói az országok kijelölt nemzetközi kapcsolati pontjai – azaz hiteles és nem nyilvános források –. A segítségek kérése és a felajánlások fogadása a GDACS esetében is megvalósulhat, de ez a nyílt rendszer, a nagyszámú felhasználó és a nyilvánosság miatt a lehető legritkábban valósul meg. Itt inkább az a jellemző, hogy a szakértők gyors bevonása érdekében a segítségkérés kinyilvánítása akár percek, órák alatt is megvalósulhat, de az országok által tett felajánlások, a kommunikáció hivatalos része már nem itt történik. Ez egy rendkívül fontos kérdés, hiszen egy állami szintű segítségkérés vagy felajánlás minimum kormányzati felhatalmazást igényel, azt nem teheti meg bárki. Magyarországon a CECIS nemzetközi szintű kapcsolattartási pontja a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (BM OKF) Nemzetközi Főosztálya és a Központi Főügyelete. [9: 247-248].

A CECIS alkalmazás jogszabályi hátterének teljes szövege elérhető az Eur-lex weboldalon. A felhasználói jellegéből adódóan a CECIS rendszer szenzitív információkat tartalmazhat, hiszen egy-egy tagállami felajánlás vagy segítségkérés során az anyagi, eszközbeli és erőforrásbeli tartalékok és hiányosságok konkrétan megnevezésre és számszerűsítésre kerülnek. Ezt figyelembe véve a Bizottság alkalmazza a titkos adatkezelés európai uniós szabályozását, amely okán a rendszerbe nem lehet nyíltan regisztrálni. A veszélyhelyzetek hatékony kezelése érdekében a CECIS alkalmazás számára létfontosságú, hogy gyors és hatékony információs platformként működjön, így a felhasználók a manapság legelterjedtebb, e-mail üzeneteket kezelő levelező rendszerekhez hasonló felületet használnak benne. Fontos különbség azonban, hogy a hagyományos, nyílt internet-alapú levelező rendszerektől eltérően a CECIS rendszer teljesen védett kommunikációs felület, így az ott megjelenített üzenetek nem érhetők el a nyilvánosság számára.

A CECIS rendszer kezelésének hatékony elsajátítása érdekében az Európai Bizottság minden ország regisztrált felhasználója számára ingyenes képzést biztosít. Az egy napos kurzus

keretében a résztvevők 6-8 fős csoportokban ismerhetik meg az ERCC központ napi feladatait, valamint magát az alkalmazást. A segítségkérések és felajánlások párosítására egy könnyen átlátható és szemléletes, táblázatos formában megjelenő speciális felület áll rendelkezésre. Az erőforrások generálásával (pl.: szakértők, csapatok, modulok, egyéni erőforrások) egy-egy tagállam előzetesen regisztrálhatja, illetve a későbbiekben dokumentálhatja a segítségnyújtás során megtett felajánlásait. A felhasználói profillal rendelkező országok a műveleti (*operational*) és az utólagos irányítási (*command post*) mód mellett tréning (*training*) módban is elérhetik a rendszert, amely lehetővé teszi számukra a rendszer használatának gyakorlását, és a képzésen tanultak szervezeten belüli átadását.[1]

KÖVETKEZTETÉSEK

A GDACS rendszer a nyílt regisztrációja révén közel 120 magyarországi felhasználóval rendelkezik, ugyanakkor maga a nemzetközi szintű rendszer ismertsége meglehetősen alacsony. Az információk gyűjtése, a nemzetközi közösséggel folytatott kommunikáció, a befogadó nemzeti támogatás és a katasztrófa–segítségnyújtási feladatok végzése ugyanakkor megköveteli, hogy szükség esetén számos jól képzett felhasználó működjön közre. A bonyolult, vagy kiterjedt káresemények elhárítása során a nemzetközi erők és eszközök igénybe vétele mindenképpen a hatékonyság növelését eredményezheti, hiszen egyrészről speciális eszközök tekintetében hiányokat pótolhatnak (így a nemzeti képességhez képest többlet erők és eszközök állhatnak rendelkezésre), illetve a szakértők bevonása a feladatok időben hamarabb, vagy nagyobb hatékonysággal történő elvégzését eredményezheti. Ezt támasztják alá a korábban elmondottak, amelyek szerint egyre növekszik a szakmaiság és döntéshozatali mechanizmusok magas szintű számonkérése a nemzetközi szintű feladatok végzése során. Tényként megállapítható, hogy az ENSZ és az Európai Unió is jelentős forrásokat biztosít a korai előrejelző és koordinációs rendszerek és eszközök megfelelő működtetéséhez, amelyhez a tagállamoknak kell biztosítani a megfelelő szakértelemmel és felkészültséggel rendelkező szakembereket. A nemzetközi műveletekben részt vevők tudását folyamatosan fejleszteni kell, így egyre inkább célszerűvé válhat ezen szakértők speciális kiválasztásának, tudatos és tervszerű képzésének megvalósítása. A nemzetközi szintű szoftverek ismerete és használata megkönnyítheti a nemzeti szintű, hasonló funkciókkal bíró rendszerek kialakítását. Az egyes szoftverek jól működő részei átemelhetőek, a nemzeti sajátosságoknak megfelelően átalakíthatóak, de mintaként szolgálhatnak egy-egy feladat végrehajtás vagy például nyilvántartások vezetése kapcsán is. A hasznos programok és alkalmazások palettája egyre bővül, mindegyik újonnan megjelenő hozzátesz valamit a biztonsághoz. A korai előrejelző rendszerek csökkenthetik a természeti katasztrófák által okozott károkat, valamint megfelelő képességekkel és felkészültséggel rendelkező felhasználó esetén jelentős mértékben javíthatják a koordinációt és a katasztrófavédelmi műveletek hatékonyságát. Az Európai Unió és az ENSZ tagállamai folyamatosan hajtanak végre olyan fejlesztéseket, amelyek révén az előrejelzések hatékonysága, a bevethető nemzetközi erők mennyisége, minősége és eszközrendszere fejlődik. Előfordulhatnak olyan esetek, amikor Magyarországon eddig nem ismert kockázatok és következményeik (pl. Ebola – járvány) elhárítására kell felkészülni és védekezni. Ilyenkor kiemelten hasznos lehet az a tapasztalat, amelyet azon országok szakértői tudnak biztosítani a katasztrófavédelmi szakemberek számára, akik már látták, tapasztalták, átélték az adott eseményt. Magyarország katasztrófavédelmi rendszere a hagyományos, megismerésen alapuló rendszer, amely rendszer esetében kiemelt fontossággal bír az előre megismerés és a

felkészülés. Ennek érdekében javasolt olyan szakemberekből álló csoport létrehozása, amely folyamatosan képes az eddig Magyarországon ismeretlen, vagy csak nemzetközi színtéren meglévő veszélyforrások felderítésére, majd képes az egyes események Magyarországra történő modellezésére, védekezési javaslatok kidolgozására.

FELHASZNÁLT IRODALOM

[1] Globális Katasztrófa Előrejelző és Koordinációs rendszer
http://gdacs.org/ (A letöltés ideje: 2017.12.06.)

[2] Az Európai Parlament és a Tanács 1313/2013/EU határozata az Uniós polgári védelmi mechanizmusról
https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013D1313&qid=1520934350013&from=HU
(A letöltés ideje: 2018.03.01)

[3] Európai Számvevőszék Különjelentés: Uniós Polgári Védelmi Mechanizmus – Az Unión kívül bekövetkezett katasztrófákra adott válaszok koordinálása nagyrészt eredményes volt
https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52016SA0033&qid=1520934827325&from=HU
(A letöltés ideje: 2018.03.01)

[4] AZ ERCC monitorozza a Mexikóvárosban bekövetkezett földrengést
https://ec.europa.eu/echo/news/emergency-response-coordination-centre-monitoring-earthquake-situation-mexico-city_en
(A letöltés ideje: 2018.03.01)

[5] Európai Erdőtűz Információs Rendszer térinformatikai felülete
http://effis.jrc.ec.europa.eu/static/effis_current_situation/public/index.html
(A letöltés ideje: 2018.03.01)

[6] Európai Tengerbiztonsági Ügynökség weboldala
http://www.emsa.europa.eu/
(A letöltés ideje: 2018.03.13)

[7] Európai Mediterrán Szeizmológiai Központ weboldala
https://www.emsc-csem.org/#2w
(A letöltés ideje: 2018.03.13)

[8] Az EU Meteoriasztási platform
http://www.meteoalarm.eu/
(A letöltés ideje: 2018.03.13)

[9] MUHORAY Á.: Katasztrófamegelőzés I., NKE Szolgáltató Nonprofit Kft. 2016, ISBN 978-615-5527-85-2
https://ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10287/ebook_XL_KVI_Katasztrofamegelozes_I.pdf?sequence=1&isAllowed=y
(A letöltés ideje: 2017.12.03)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

MAGYAR RÉSZVÉTEL AZ EURÓPAI BIODOZIMETRIAI HÁLÓZAT (RENEB) KIALAKÍTÁSÁBAN

HUNGARIAN PARTICIPATION IN REALISING AN EUROPEAN NETWORK OF BIODOSIMETRY

KIS Enikő

(ORCID: 0000-0002-6761-0423)

kise@osski.hu

Absztrakt

A RENEB hálózatot 16 európai ország 23 biodozimetriai tapasztalattal rendelkező laboratóriuma hozta létre és a továbbiakban a nemzeti és nemzetközi katasztrófavédelmi szervek háttérintézményeként működne. Az elmúlt évek során szoros együttműködés alakult ki ezen laboratóriumok között, módszer-összemérő és virtuális baleset-szimulációs gyakorlatok során készültünk fel arra, hogy egy esetleges tömeges szerencsétlenség esetén gyors és megbízható segítséget tudjunk nyújtani. Munkánkat a NAÜ irányelveknek megfelelően végezzük. Jelen cikk célja e munka és a magyarországi sugárbiológiai biodozimetriai laboratórium részvételének bemutatása a fent említett projektben.
Ez a munka a GA295513 EU FP7-es projekttámogatásával készült.

Kulcsszavak: *biodozimetria, RENEB, összemérés, MNA, DIC*

Abstract

A sustainable network has been created in Europe, which could be an important backup organisation for the national and international emergency response organisations. 23 laboratories with biodosimetrical experience from 16 European countries prepared to give a fast and reliable response in case of a large-scale radiological emergency. To achieve this goal, methodological intercomparison and accident simulation exercises were carried out during the past few years. The applied methodology is conform IAEA directives. The goal of this article is to disseminate this work and present the Hungarian radiological biodosimetry team's participation.
This work was supported by EUFP7WP (GA295513)

Keywords: *biodosimetry, RENEB, intercomparison, MNA, DIC*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.16.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.24.

BEVEZETÉS

Közismert történelmi példák mutatnak rá arra, hogy a nukleáris energia már felfedezése óta részint etikailag elfogadható, gazdasági haszonnal is járó, részint a fegyver szerepét is betöltő eszköz volt. A CIA már a 2003-as terror-ellenes stratégiájában kiemelte, hogy bizonyos terrorista csoportok radiológiai vagy nukleáris fegyverek (radiological dispersal device, RDD) birtoklására, létrehozására és felhasználására törekednek. A nukleáris fegyverek változó összetételűek lehetnek a forgalmas helyen elhelyezett nyitott vagy zárt sugárforrástól a radioaktív anyagot tartalmazó és szétszóró piszkos bombán vagy éppenséggel nukleáris tölteten keresztül az aeroszolubilis sugárforrás kibocsátásáig (pl. 131I, 137Cs, 90Sr). Napjainkban világszerte léteznek és tevékenykednek olyan terrorista csoportok, amelyek céljaik elérése érdekében a világ különböző pontjain okoznak támadásokat békés állampolgárok ellen. Egy RDD használata nem csupán egészségügyi, környezeti és gazdasági károkkal járhat, hanem politikai és szociális következményei is lehetnek: az általa kiváltott pánik miatt aggódó érintettek nem feltétlenül sérültjei a támadásnak, viszont szeretnének mielőbb meggyőző és megnyugtató választ találni félelmeikre. Ez esetben az aggódó tömeg az egészségügyi intézmények túlterhelését okozhatja, illetve a helyzet stabilizálása államigazgatási-politikai közbelépést is igényelhet. [1] Egy másik lehetőség az emberek terrorizálására a pánikkeltés, amely egy láthatatlan és érzékelhetetlen veszélyt kivetítve a pszichológiai fegyverviselés egy módja is lehet. Ez esetben a tünetek hiányában is aggódó tömeg ostromolhatja segítségért a hatóságokat, ami szintén szociális-politikai nehézségekhez vezethet. A 2016-ban, Washingtonban megtartott Nukleáris Biztonsági Csúcstalálkozó hivatalos kommünikéjéből idézzük: „A nukleáris és radiológiai terrorizmus fenyegetése egyike a nemzetközi biztonság legnagyobb kihívásainak és a fenyegetés folyamatosan fokozódik.” [2]

A nukleáris és radiológiai balesetek áldozatainak száma is változó. A Goianai baleset párszáz áldozatot követelt (112 000 személy került monitorozásra, közülük 249 szenvedett külső vagy belső sugárszennyezést). [3] A csernobili baleset következtében 116000 személyt evakuáltak (részben a robbanást követően 20 órával, részben pedig néhány nap illetve hét múlva). Összességében, több mint 600000 munkás került bevetésre a baleset utáni munkálatokban. A telephelyen tartózkodó 400 munkás dozimeterei túlexponálódtak. Az akut sugárbetegség miatt kórházi kezelésre szoruló 237 személy esetén biodozimetriai módszerekkel 1-16Sv sugárdózist állapítottak meg. [4] A fukusimai balesetek során 2400 helyreállításban résztvevő munkás kapott különböző méretű sugárdózist, 78000 embert költöztettek ki a környező területről, közülük 23 mutatott bizonyos szintű kontaminációt. Az északi félteke különböző részein volt kimérhető az erőműből származó radioaktivitás. [5]

Egy tömegeket érintő katasztrófa meghaladhatja az azt elszenvedő ország védelmi és egészségügyi rendszerének kapacitását. A következmények nem csupán a sérülések típusától és a sérültek számától, hanem a beavatkozások gyorsaságától is függenek. A sürgősségi helyzet kezelésének első lépéseként elengedhetetlen a sugársérültek expozíciójának megbecsülése, valamint az ál-negatív illetve -pozitív esetek beazonosítása. Ily módon a biodozimetriai szűrések következtében kizárólag a tényleges sérültek kerülnek sürgős kórházi ellátásra. Azokban az esetekben, amikor a megbecsülendő minták száma meghaladja jelenlegi képzett munkatársaink kapacitását, létfontosságúvá válik a biodozimetriai laboratóriumok határokon keresztül ívelő együttműködése a retrospektív dozimetriai vizsgálatok átfutási idejének csökkentésére. [6,7,8]

A sugársérültek klinikai megfigyelése elengedhetetlen teendő nagyobb elnyelt dózis esetén, viszont a fiziológiás tünetek nagy része - a limfociták számának csökkenése, a hányás, hasmenés, fejfájás, levertség - nem specifikus és nem mindig elégséges a pontosabb dózisbecsléshez. A tünetek egy részének oka lehet vegyi mérgezés vagy akár pszichés reakció is. Ilyen esetekben feltétlenül szükség van az elnyelt dózis becslésére biológiai és fizikai retrospektív dozimetriai eszközökkel. Szintén fontos a kisebb dózisokat elszenvedők orvosi

nyomon követése a sztochasztikus hatások mielőbbi detektálása és kezelése céljából. Az aggódó tömegre kifejtett pszichológiai hatás – félelem, szorongás – elkerülése, a hamis tüneteket mutató egyének kiszűrése és az emberek megnyugtatása nem csupán egy pszichológiai fegyverrel szembeni védekezés eszköze, hanem a tömegkatasztrófa politikai-szociális kezelésének egyik alapvető pillére is lehet. [9,10]

2012-ben 23 európai ország biodozimetriai laboratóriumainak bevonásával indították útjára a RENEB: Realizing the European Network of Biological Dosimetry and Physical Retrospective Dosimetry (Az Európai Biodozimetriai és Retrospektív Fizikai Dozimetriai Hálózat Megvalósítása) projektet Európai Uniós támogatással. Az Európai Biodozimetriai Hálózat kialakításában az akkor Országos „Frédéric Joliot-Curie" Sugárbiológiai és Sugáregészségügyi Kutató Intézet, ma pedig Országos Közegészségügyi Intézet Sugárbiológiai és Sugáregészségügyi Főosztályának (továbbiakban: OSSKI)1 biodozimetriai laboratóriuma a kezdetektől fogva, mint alapító tag vett részt. [6, 7, 11, 12]

A RENEB hálózat megfelelő működése céljából fontos a tevékenységünk megismertetése mind a hazai, mind a nemzetközi sürgősségi felkészültségben és válaszban feladattal rendelkező szervezetekkel. [11] Jelen közlemény célja a projekttel kapcsolatos angol nyelvű irodalom összefoglalása és az Európai Biodozimetriai Hálózat, valamint az abban való magyar részvétel bemutatása a katasztrófavédelmi szervek és a magyar közönség számára.

TÖRTÉNETI ÁTTEKINTÉS

A Nemzetközi Atomenergia Ügynökség 1988-ban, a Goiana-i balesetet követően kiadott javaslatában megfogalmazta, hogy a sugársérült személy expozíciójának retrospektív meghatározásában a biológiai dozimetria nagyon hasznosnak bizonyult. Javaslat született a nemzeti sürgősségi tervek felülvizsgálatára és nemzeti vagy nemzetközi kollaboráció létrehozására a biodozimetriai felmérések nagyobb mintaszám esetén történő elvégzéséhez. Egy másik javaslat összeméréses programok létrehozására irányul a különböző laboratóriumok eredményeinek egységesítéséhez. [3] A NAÜ védnöksége alatt Latin-Amerika területén hat biodozimetriai laboratóriumból álló hálózat jött létre.

Az Amerikai Egyesült Államokban, Japánban és Kanadában nemzeti szinten jöttek létre hasonló hálózatok. Európában először egy hármas, Nagy-Britannia-Franciaország-Németország közötti kölcsönös segítségen alapuló memorandumot írták alá 2004-ben a súlyos radiológiai események kezelésére. A NAÜ bevonta válasz és segítségnyújtási hálózatába (Response and Assistance Network – RANET) a biodozimetriai laboratóriumokat és globális szinten a WHO létrehozta a BioDoseNet -et. [7]

Az „Egy kiváló európai biológiai dozimetriai hálózat felé" (Towards a European Network of Excellence in Biological Dosimetry, TENEB) című felmérés a tapasztalt európai biodozimetriával foglalkozó laboratóriumok beazonosítására és feljegyzésére irányult, amelyet 2009-ben teljesített is. [7,11,13]

2010-2013 között a MULTIBIODOSE projekt keretein belül megtörtént a multidiszciplináris biodozimetriai eszközök elemzése és tömegszerencsétlenség esetén való alkalmazásra való adaptációja. [14]

Hasonló célkitűzései voltak az Európai Sugár-Dozimetriai Csoport (EURADOS) 10. munkacsoportjának: a biológiai és fizikai módszerek alkalmazása retrospektív dozimetriai felmérésekre, a retrospektív dozimetria lehetőségének népszerűsítése a hatóságok között, új

1 - A RENEB pályázat lebonyolítása idején az Országos Sugárbiológiai és Sugáregészségügyi Intézet (OSSKI) különálló intézményként vett részt. Időközben az állami intézményi átszervezések kapcsán az Országos Közegészségügyi Intézet, Országos Közegészségügyi Igazgatóságának Sugárbiológiai és Sugáregészségügyi Főosztálya lett.

módszerek bevezetése illetve a parciális testdózis és belső sugárszennyezés megállapítására irányuló módszerek kialakítása. [15]

Az előzetes felmérő és megalapozó munkák során több ország jelezte igényét és elköteleződését egy hosszú távú európai biodozimetriai hálózat létrehozására, amely végül 2012-ben 16 európai ország 23 laboratóriumának együttműködésének folytán létrejött.

CÉLKITŰZÉS

A RENEB célja az volt, hogy a meglévő tudást, labor-kapacitást megossza az együttműködő európai országokkal, egységesítse a vizsgálati módszereket és a kiértékelést, és megalapozza a kölcsönös segítségnyújtási lehetőséget. 2012-ben tizenhat országból származó 23 európai szervezet működött közre ennek a projektnek az elindításában, hogy a lehető legmagasabb hatékonysággal gyors és megbízható dózis-becslést garantáljon. A projekt az egyes laboratóriumokban fennálló és már használatban lévő biodozimetriai tudás összehangolására és egységesítésére irányul, ennek keretein belül pedig az eddig ismert legnagyobb számú biodozimetriai laboratórium együttműködése valósult meg. A végső cél az állandó készenlét lenne egy nagy számú sérülttel járó radiológiai katasztrófa esetére, amit a résztvevő szervezetek a laboratóriumaik közötti együttműködés folyamatos fenntartásával és a dózis-meghatározás minőségének állandó biztosításával szeretnének elérni.

Retrospektív biodozimetriai módszerek

Amennyiben egy sugár-sérüléssel járó baleset sérültje nem viselt fizikai dozimétert a baleset megtörténtekor, az általa elszenvedett dózis utólag, visszamenőleg is meghatározható, egy úgynevezett retrospektív dózisbecslési eljárás során. Az előző fejezetben említett együttműködést laboratóriumi szinten ú.n. összemérések formájában valósítottuk meg: a különböző laboratóriumokban alkalmazott hét biológiai és két fizikai módszer lebonyolítási módját (kísérleti protokollok összehasonlítása) valamint eredményeit hasonlítottuk össze. Már a kezdeti fázisban újabb módszereket is kipróbáltunk, melyek célja a gyorsabb, pontosabb dózis-becslés, valamint a mérések objektivitásának növelése volt.

A nemzetközi összemérések lebonyolítása úgy történt, hogy egyik szervező laboratórium munkatársai begyűjtötték a humán vérmintát, besugarazták, szétosztották, majd csomagküldő szolgálat útján eljuttatták a résztvevők számára. Minden résztvevő elvégezte a saját kísérleti protokollja alapján az általa vállalt méréseket és saját laboratóriumi körülményei között, saját dózis-hatás görbéje alapján becsülte meg az elnyelt dózisokat. Az első összemérés során négy, a második összemérés során két különböző dózissal kezelt minta került kiküldésre. [16,17]

Az eredmények a MultiBioDose által meghatározott kategóriákba sorolva, az expozíció testfelületre vetített arányával együtt kerültek jelentésre. A MultiBioDose által meghatározott kategóriák:

- alacsony (<1Gy) – kismértékű sérülés, nem igényel klinikai ellátást: zöld kód;
- közepes (1 és 2 Gy között) – orvosi monitorozás szükséges: narancssárga kód;
- magas (>2Gy) – súlyosan sérült, sürgős orvosi beavatkozás szükséges: piros kód.

Az összeméréseket szervező laborok munkatársai végezték el az eredmények statisztikai értékelését, kielemzését. [16,17]

Sugárkezelés

A vérmintákat 37°C-on különböző dózisú Cs-137 gamma-sugárzással kezelték, majd két órán át 37°C-on inkubálták, lehetővé téve a DNS hibajavító folyamatok lezajlását. Az első összemérés alkalmával 0-, 0,94-, 3,27Gy teljes test-dózissal valamint 4,75Gy parciális test-dózissal történt a kezelés. Ez utóbbit a kezelt és kezeletlen vérminták 1:1 arányú

összekeverésével szimulálták. A második összemérés alkalmával 0,85Gy, és 2,7Gy teljes test-dózissal sugarazták be a mintákat, amelyeket ezután kódoltak, szétosztottak és a résztvevőkhöz szállíttatták őket. [16,17]

Szállítás

A szállítás minden esetben a B kategóriájú biológiai anyagokra kiadott UN 3373-as számú csomagolási rendeletnek megfelelően történt. A szállítási hőmérsékletet hőmérsékletjelzővel, a szállítás során kapott háttérdózist SC-2-es típusú üveg-dozimétterrel követték nyomon. A mintához mellékelt dozimétereket és hőmérsékletjelzőket mindkét esetben kiértékelték. A minták minden esetben kevesebb, mint 1mGy többlet-sugárzást kaptak a szállítás folyamán. A hőmérséklet 11-30°C között változott az első, 11-29°C között a második minta szállítása során. [16,17]

Résztvevők

A résztvevők száma módszerenként és gyakorlatonként változott.

A dicentrikus kromoszóma aberrációkat mérő módszert az első összemérésben 14 laboratórium végezte el. A második összemérés egy nagy létszámú gyakorlattá nőtte ki magát, mivel ezúttal a Kanadai Hálózat-, az Ázsiai Hálózat-, a Latin Amerikai Hálózat-, a Dél-Afrikai és a NAÜ Hálózat tagjai valamint a BioDoseNet/WHO partnerei is részt vettek. A 14 Európai Uniós RENEB partner ország 19 laboratóriumán kívül még három nem RENEB-partner európai ország négy laboratóriuma, illetve 16, nem-EU tagállam 19 laboratóriuma vett részt az összemérésben. Így egy alkalommal 31 ország 41 laboratóriuma hangolta össze biodozimetriai méréseit. Ennek jelentősége igen nagy a módszer nemzetközi szinten történő egységesítése szempontjából, ugyanis ilyen volumenű mérés-szinkronizálás tudomásunk szerint még nem történt a biodozimetria történetében. [16,17]

Ahhoz, hogy a dicentrikus assayt teloméra-centroméra festéssel pontosabbá tegyük, egy másik egységesítő kísérletet is szerveztek a müncheni laboratóium munkatársai, ebben tizenhét európai laboratórium munkatársai vettek részt. [16,17]

Az első mikronukleusz assay összemérésben 12, a másodikban 16 RENEB-partner labor vett részt. [16,17]

Biodozimetriai módszerek

A RENEB hálózatot már meglévő, több éve működő, gyakorlott biodozimetriai laboratóriumok hozták létre. Az ezekben a laboratóriumokban használatban lévő módszerek DNS – kromoszóma - sérüléseken alapuló módszerek: mikronukleusz assay (MNA), dicentrikus kromoszóma assay (DIC), fluoreszcens in situ hibridizáció (FISH), korai kromoszóma kondenzációs módszer (PCC) és a H2 hiszton foszforilációjának vizsgálata (γH2Ax). A biológiai módszerek mellett a fizikai retrospektív dozimetria két módszere is bekerült a RENEB hálózatban használatos módszerek közé: elektron paramágneses rezonancia (EPR) és optikailag szimulált lumineszcencia (OSL). [6, 18,19]

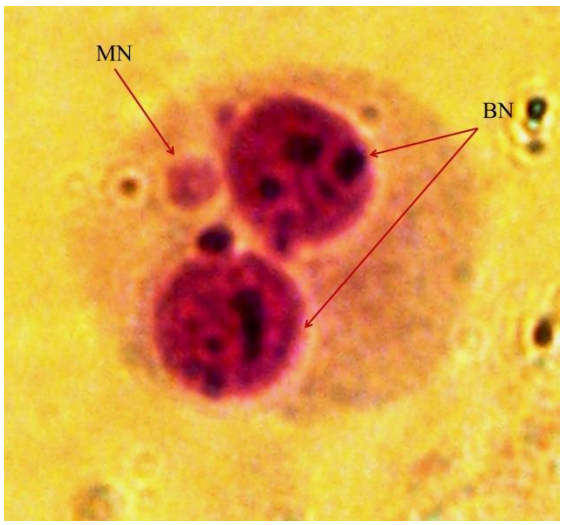
A könnyebb átláthatóság érdekében szükségesnek találjuk a fent említett módszerek rövid ismertetését. Az OSSKI biodozimetriai laboratóriumában használatos MNA és DIC assay-k módszereit kissé bővebben ismertetjük.

Mikronukleusz assay (MNA):

A mikronukleusz assay egy, a DNS kettős törések kimutatásán alapuló módszer. Sugárkezelést követően a DNS kettős láncon egy- és kétláncú törések jönnek létre. A sejtek ezen sérülések kijavítására törekszenek. Abban az esetben, ha nem, vagy nem helyesen javítódnak ki a kétláncú törések, a sérült DNS a sejtosztódás során kizáródhat a sejtmagból és apró, sejtmag-szerű képződmények alakulhatnak ki a citoplazmában, amelyeket mikronukleuszoknak nevezünk.

Amennyiben a sejtosztódást leállítjuk a leány sejtmagvak létrejötte után, de még a citoplazma kettéválása előtt, az így keletkező binukleáris sejtekben megjelenő mikronukleuszok arányosak az elnyelt dózissal. [9]

A módszer használatának korlátai: mivel osztódásra késztetjük a sejteket, amit a sugárkezelés dózisfüggően akadályoz, illetve a mikronukleuszok természetes hátterének köszönhetően a mikronukleusz assay 0,25-5Gy között használható retrospektív dózisbecslésre. A humán limfociták nem osztódnak a vérben, viszont körülbelül félévente lecserélődnek, így a bennük található sugárzás indukálta károsodások is eltűnnek. Ez egy további korlátja e módszer használatának. [9]



1. ábra mikronukleuszok sugárkezelt sejtekben. MN: mikronukleusz BN: a sejtosztódást követően kialakuló két leánysejtmag. (saját fotó)

A vérminták mindkét esetben 24 órán belül, problémamentesen érkeztek meg. Kézhezvételüket követően a vért 10% foetalis bovine szérum (FBS) tartalmú RPMI tápoldatban tenyésztettük sejtosztódást serkentő fehérje (phytohemagglutinin) jelenlétében. A teljes tenyésztési idő 72 óra volt, a 44. órában cytochalasine B segítségével, telofázisban[2] állítottuk le a sejtosztódást. A vérben lévő limfociták így a 72. órára két sejtmagvas, ún. binukleáris állapotba kerültek. A preparálási folyamat során 0.075M KCl-os oldatban hipotonizáltuk a sejteket, ezáltal megnöveltük a sejtek belső képleteinek a láthatóságát. Ezután 3:1 arányú metanol-ecetsav oldattal fixáltuk a sejteket. Tárgylemezre történő kicseppentést követően Giemsa oldattal festettünk.

Dózis-hatás görbe[3]: Az általunk használt dózis-hatás görbe manuálisan, ^{60}Co sugárforrás segítségével, <0,5Gy/perc dózis-rátával készült.

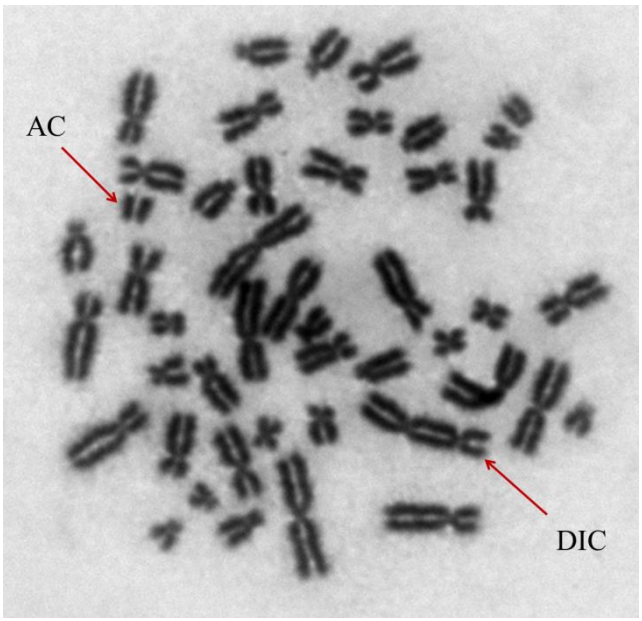
Értékelés: 1000 binukleáris sejtet vizsgáltunk meg minden dózis esetén. A NAÜ szabványnak megfelelően értékeltük a mikronukleuszokat és 1000 binukleáris sejtre kivetítve határoztuk meg arányukat. A dózist a fent említett dózis-hatás görbe segítségével CABAS [20] és DoseEstimate [21] software segítségével határoztuk meg. Az exponált testfelület arányát a CABAS program algoritmusa szerint állapítottuk meg.

[2] A sejtosztódásnak az a része, amikor a sejtmag állománya már ketté osztódik, viszont a citoplazma és a sejt még nem. A sejtmagokból kiesett sérült DNS szakaszok így még a sejtben vannak és megszámolhatóak.

[3] A dózis-hatás görbe a biodozimetriai módszerek mérő eszköze. Előállítása során egyre növekvő dózissal besugarazott egészséges emberi véren végezzük el az adott kísérletet, majd kiértékeljük és az eredményeket grafikusan ábrázoljuk. Az így keletkező görbe a MNA és DIC esetén exponenciális. A görbe másodfokú egyenletének ismeretlene a dózis.Napjainkban két szoftver is létezik a görbe alapján történő dózisbecslésre (CABAS, DoseEstimate)

Dicentrikus assay (DIC):

A dicentrikus kromoszóma assay szintén a DNS kettős lánctörések kimutatására épül. Sugárkezelést követően a DNS-ben létrejövő kétláncú törések kijavítódása során két különböző kromoszóma DNS állománya hibásan összekötődhet és két centromérával[4] rendelkező dicentrikus-, valamint centromérát nélkülöző, úgynevezett acentrikus szakaszok jöhetnek létre. Az ú.n. centrikus gyűrű úgy jön létre, hogy egyazon kromoszóma két vége törik le és a hátramaradó csonkolt végek egymáshoz záródnak. Amennyiben a sejtosztódást metafázisban[5] állítjuk le, a kromoszómák kondenzálódnak és láthatóvá válnak. A dicentrikus kromoszómák jellemzőek a sugársérült sejtekre és számuk arányos az elnyelt dózissal. A mikronukleusz assay esetén említett korlátok a dicentrikus assay esetén is fennállanak. Viszont ez a genetikai sérülés nem szokott spontán előfordulni, így alacsonyabb, akár 0,1Gy dózis esetén is használható. Az alacsony dózisok pontos becslését viszont nehezíti ritka előfordulása. [9]



2. ábra dicentrikus kromoszóma és acentrikus szakasz sugárkezelt sejtekben. AC: centroméra nélküli töredék; DIC: két centromérával rendelkező, sérült kromoszóma. (saját fotó)

A vérminták azonosak voltak a MNA esetében használt mintákkal. Kézhezvételüket követően a vért 10% FBS tartalmú RPMI tápoldatban tenyésztettük phytohaemagglutinin jelenlétében. A humán vérben lévő limfocitákban a 48. órára kondenzálódnak a kromoszómák, ezért a teljes tenyésztési idő 48 óra volt és a 45. órában colcemid oldat segítségével állítottuk le a sejtosztódást, metafázisban. Hipotonizálással (0.075M KCl) megnöveltük a sejtek térfogatát, majd 3:1 arányú metanol-ecetsav oldattal fixáltuk őket. Tárgylemezre történő kicseppentést követően Giemsa oldattal festettünk.

Dózis-hatás görbe: A mikronukleusz assay-hez hasonlóan a dózis-hatás görbe ^{60}Co sugárforrás segítségével, <0,5Gy/perc dózis-rátával készült, manuális kiértékeléssel.

Értékelés: az ú.n. Quickscan módszert alkalmazva 50 metafázist számoltunk le, ebből következtettünk a dózisra.

[4] A centroméra a kromoszóma központi része, ahol az osztódási orsóhoz kötődik.
[5] A sejtosztódás egyik szakasza, ahol láthatóvá válnak a kromoszómák.

Dicentrikus Assay teloméra-centroméra festéssel (DIC-TC):

A dicentrikus assay objektívebbé tételéhez a centromérákat és telomérákat[6] fluoreszcensen jelölték. Az összemérés virtuálisan, fényképek kiértékelésével történt. Ezen gyakorlatban az OSSKI biodozimetriai laboratóriuma az értékelés folyamatában vett részt, amely során részletesen kielemeztük nem csupán a dicentrikus kromoszómák számát, de az acentrikus szakaszok milyenségét és eredetét is (pl. intersticiális deléció: a DNS szálból kiszakadt apró szakasz centroméra és teloméra nélkül, egy- vagy két telomérával rendelkező acentrikus szakasz.) [22]

A lemezeket az első dicentrikus assay összemérés során állították elő a müncheni laboratórium munkatársai. 0.94-, 3,27 Gy teljes test dózissal és 4,75 Gy parciális test-dózissal sugárkezelt vérből, az eredeti DIC assay-hez hasonlóan. A teloméra-centroméra festést Q-FISH[7] technikával végezték el, Cy-3-jelölt teloméra-specifikus festéssel (piros), valamint FITC-jelölt centroméra-specifikus festéssel (sárga). A kromoszómákat DAPI-val festették kékre. Automatikus felvételek készítésére alkalmas Autocapt szoftverrel (MetaSystems, 3.9.1 verzió) fotózták végig a lemezeket és a fényképeket juttatták el elektronikusan a gyakorlatban résztvevő laboratóriumokba. [22]

A dózist M'kacher et al., 2014 cikkében leírt dózis-hatás görbe alapján CABAS V2.0 szoftverrel [20] értékelték ki a koordináló laboratóriumban. A teloméra-centroméra festéses módszer validációjakor az első DIC összemérés eredményei szolgáltak viszonyítási alapul. [22]

Korai kromoszóma-kondenzáció (PCC):

A sugárhatásra bekövetkezett kromoszóma törések gyors kimutatására szolgáló módszer, ami a dicentrikus kromoszóma vizsgálathoz hasonló elveken alapul. Ebben az esetben azonban nincs szükség 48 órás tenyésztésre, hanem a limfocitákat osztódásban lévő kínai hörcsög sejtekkel fuzionáltatják. Az osztódó sejtekben lévő fehérjék hatására a limfociták haploid[8] kromoszómái kondenzálódnak, a DNS törések kimutathatóvá válnak. Ezért hamarabb, alig néhány órán belül juthatunk eredményhez. Mivel a módszer nem igényel sejttenyésztést, nem kell a magasabb dózisok által okozott sejtosztódási eltolódással vagy a sérüléseik miatt sejtosztódásból kizáródó sejtekkel számolni, így akár 10Gy sérülés esetén is használható. Kombinálható teloméra-centroméra festéssel is. [9]

Fluoreszcencia in situ hibridizáció (FISH):

A stabilizálódott kromoszóma-károsodások kimutatására alkalmas: két-három különböző, fluoreszcens festékkel megfestett kromoszóma és a többi egyszínű kromoszóma között kicserélődött szakaszok értékelésén alapul. A transzlokációk stabilitása a dicentrikus kromoszómákénál jóval nagyobb, mivel a csontvelőben is kialakulnak és fennmaradnak, akár évekkel később is kimutathatóak a fehér vérsejtekből. Mivel hosszú évekig fennmaradó elváltozásokról van szó, későbbi retrospektív dózisbecslésre is alkalmas. Szintén osztódásra késztetjük a mérés elvégzéséhez a sejteket, ezért 0,3-5Gy dózis-tartományban érzékeny. [9]

γH_2A_X kimutatása:

Egy szintén gyorsan elvégezhető módszer, amely a kettős DNS törések helyén foszforilálódó H_2A_x hiszton antitestekkel történő jelölésén alapszik. Annak ellenére, hogy nem szükséges a sejtosztódás az elvégzéséhez, a jel telítődése miatt csupán 5Gy-ig alkalmazható. A DNS károsodások gyorsan kijavítódnak a sejtekben (kb 4 óra leforgása alatt), ezért csupán a sérülést követő 24 órán belül kimutatható a γH2AX. [9]

[6] A kromoszóma végén lévő, a genetikai anyag lemorzsolódásától védő szakaszok.
[7] a DNS szakaszhoz köthető fluoreszcensen jelölt próbákkal jelölték a centromérákat és telomérákat.
[8] egy példányban vannak jelen, nem duplázódik meg a DNS, mint sejtosztódáskor

Elektron paramágneses rezonancia (EPR):

Az okostelefonok folyékony kristály- és érintő képernyőjében sugárzás hatására keletkező rezgések kimutatásából következtet a dózisra. Fő előnyei, hogy specifikus a sugárzásra, és a jel hosszú távon, akár éveken keresztül is fennmarad. 10Gy fölött is használható módszer. [17]

Az optikailag szimulált lumineszcencia (OSL):

Ez a módszer az optikai szimulációs állapotban lévő okostelefonok ellenállásaiban a sugárhatás következtében emittált lumineszcenciát képes mérni és ez alapján megbecsülni az elnyelt dózist. Nagyon specifikus és érzékeny módszer. A jel felezési ideje körülbelül 10 nap. Szintén használható 10 Gy felett is. [17]

Balesetszimulációs gyakorlatok

A RENEB hálózat felépítése során a résztvevők egy olyan virtuális katasztrófavédelmi szcenáriót gyakorolhattak be, amelyhez a magas számú áldozattal járó nagyszámú adat értékelése és kezelése szükséges. A 2016-ban 27 héten keresztül tartó kétrészes szimulációs gyakorlat folyamán minden résztvevő biodozimetriai laboratóriumnak lehetőség nyílt egy nukleáris katasztrófa helyzetét mindkét szempontból: az elszenvedő és segítséget kérő (referencia laboratórium, RL) illetve a segítséget nyújtó (ú.n. kisegítő - service lab, SL) fél oldaláról begyakorolni. Minden héten más-más RL laboratórium aktiválta a hálózatot egy fiktív balesetet jelző elektronikus levéllel. A hálózat további tagjai (SL) válaszlevélben jelezték rendelkezésre állásuk paramétereit: az adott intézményben az adott időpontban hány ember milyen mennyiségű dozimetriai vizsgálatot képes vállalni.

A referencia laboratórium megállapította a hálózat kapacitását (az egyes laboratóriumok által vállalható minta-mennyiséget az adott héten), mérte a válaszok visszaérkezési idejét és összesítette a visszaérkező eredményeket. Mindezt továbbította a baleset szimulációs gyakorlatot koordináló laboratóriumnak, ahol az eredményekből statisztikát számoltak.

A RL ezt követően a visszajelző laboratóriumok részére egy 54 adatsorból álló táblázatot küldött ki. Minden SL elemezte ezeket, eredményeiket pedig visszaküldték a koordináló laboratóriumnak.

A táblázat a hét retrospektív módszer által korábban meghatározott dózisokat tartalmazta, ezen adatok alapján kellett a balesetet szenvedett egyént a már említett MultiBioDose kategóriákba sorolni. Az egyes módszerek korlátait ismerve a baleset időpontját is el lehet dönteni (a sérülést követő 24 órán belül, egy napon túl, illetve egy héten túl), valamint a sugárhatásnak kitett testfelület (parciális vagy teljes testdózis) mértékét is meg kellett becsülni: ahogy az előzőekben említettük, a γH2Ax hiszton foszforilációja 24 órán belül mutatható ki. Amennyiben sikerült ezzel a módszerrel dózist becsülni, a vérminta a balesetet követő 24 órán belül lett begyűjtve. Az OSL által mért jelenség erőssége tíz napon belül feleződik. Tehát, ha ez utóbbi módszerrel becsült dózis fele a többi módszer segítségével megbecsült értéknek, akkor nyilvánvalóan a mintavételhez képest legalább tíz nappal korábban történt a baleset. Ez esetben a γH2Ax foszforilációval nem kimutatható a sérülés.

A parciális testdózis meghatározásához ez esetben a hordozható elektronikus eszközök (portable electonic device - PED) és a sugárnyaláb útjának viszonyából következtettünk. Pl. ha minden módszerrel magas dózis került megállapításra, csupán a PED-ekből meghatározott dózis volt alacsony, akkor parciális test-dózisról beszélünk, ahol a PED nem került a sugárnyaláb útjába. A lehetséges szcenáriókat az 1. táblázat sorolja fel. [7]

A baleseti szcenáriót mind a segítséget nyújtó, mind az azt elfogadó laboratóriumoknak meg kellett fejteniük. Az eredmények összesítése és jelentése szintén az RL kötelezettsége volt. Ezen a ponton is mértük a válaszok beérkezési idejét, a hálózat terhelhetőségét. [7,23]

Szcenáriók		
Testfelület mérete	**Expozíció és vérvétel között eltelt idő**	**PED helyzete**
Teljes	0. napon begyűjtött vérminta	
	1. napon begyűjtött vérminta (24h)	
	1 héttel később begyűjtött vérminta	
Parciális	0. napon begyűjtött vérminta	sugárnyaláb útjában
	1. napon begyűjtött vérminta (24h)	
	1 héttel később begyűjtött vérminta	
Parciális	0. napon begyűjtött vérminta	sugárnyalábon kívül
	1. napon begyűjtött vérminta (24h)	
	1 héttel később begyűjtött vérminta	

1. táblázat Szcenárió-kategóriák. Brozowska et al. nyomán [7]

A gyakorlat nehézsége, különlegessége az OSSKI számára abban állt, hogy pont az augusztus 20-ai héten került sor a koordinálói feladatra. Ezen a héten munkatársaink túlnyomórészt szabadságon tartózkodtak, így onnan vettek részt a gyakorlatban. Ezáltal azt is észlelhettük, hogy munkatársaink mennyi idő alatt mozgósíthatóak egy baleseti szituációban. Az is fontos szempont, hogy Nemzeti Ünnepünk alkalmából nagy tömegek gyűlnek össze az ország különböző pontjain ezen a héten, ami nemzetbiztonsági szempontból igen jelentős lehet.

EREDMÉNYEK, A PROJEKT KIMENETELE, TANULSÁGAI

Nemzetközi összemérések tanulságai

A RENEB projekt folyamán két laboratóriumi és egy virtuális összemérésben vettünk részt. A laboratóriumi összemérésekhez előre besugarazott vérmintát kaptunk kézhez. Az első összemérésben mikronukleusz, míg a másodikban mikronukleusz és dicentrikus assay-ket végeztünk, az eredményeket manuálisan értékeltük ki, majd megbecsültük az elnyelt dózist. A virtuális összemérés[9] során a laboratóriumi összemérésből származó képek kerültek kiértékelésre.

Az első laboratóriumi összeméréshez 0, 0,94 és 3,27Gy teljes test-dózissal, valamint 4,75Gy 50% parciális test-dózissal kezelt vért szállítottak ki a résztvevő laboratóriumoknak, azzal az információval együtt, hogy van a minták között egy negatív kontroll, egy alacsony és egy magas teljes test-dózissal-, valamint egy parciális test-dózissal kezelt. A minták a szállítás során <1mGy sugárdózist kaptak, kb. 10°C hőmérsékleti különbséget szenvedtek el. [16,17]

A második összemérés során egy alacsony (0,85Gy) és egy magas (2,7Gy) teljes test-dózissal kezelt mintát szállítottak ki. [16,17]

A kiküldött mintákból elvégeztük a mikronukleusz- illetve a dicentrikus kromoszóma-assayt, az eredményeket a saját laborunkban használatos dózis-hatás görbe alapján kiértékeltük és továbbítottuk a szervező laboratórium felé.

Mindkét esetben a minták vakon történt kiértékeléséből kapott eredményeket a MultiBioDose által a radiológiai vészhelyzetekre megszabott ú.n. triage kategóriába soroltuk be. Az értékelés során szükségessé vált egy, a dózis-meghatározáshoz rendelt bizonytalansági

[9] Az előzőek során említett fotók alapján történő összemérés célja az eredmények kiértékelésének összehangolása és pontosítása volt a kromoszómák centroméra-teloméra végződéseinek festése révén.

intervallum bevezetése a minták triage módban történő rangsorolásához. Ezt az alacsony dózisok esetén 0,5Gy, míg a magas dózisok esetén a szórás 20%-ában állapították meg a szervezők úgy a MNA, mint a DIC esetén. [16,17]

Mikronukleusz assay

Az első összemérés során a résztvevők dózis-hatás görbéit is vizsgálták. A szervezők begyűjtötték a résztvevők dózis-hatás görbéinek adatait, valamint azok elkészítésének körülményeit. Annak érdekében, hogy minél inkább összhangban legyen a különböző laborok mérési eredménye, ezeket az ismereteket is összevetették és mindenki számára elérhetővé tették. A dózis-hatás görbék között mind az automatikus, a fél-automata és a manuális értékelés esetén nagy volt a variáció. Az inhomogenitás nőtt a dózissal és legnagyobb a manuális értékelés esetében volt. Ez valószínűleg a különböző munkacsoportok kísérleti körülményei közötti eltéréseknek tulajdonítható úgy a protokollok, mint a besugárzás körülményei vagy a kiértékelés terén. [16]

A manuális kiértékelési módszer nagyobb számú MN-t eredményezett a nagy dózisok esetében, mint az automatikus vagy fél-automatikus, míg az alacsony dózissal kezelt minták esetén ez pont fordítva történt. [16]

A kontrollt és alacsony dózist a részvevő laboratóriumok nagy hányada helyesen határozta meg: a 0- és 0,94Gy-t a laboratóriumok 88%, a 0,85Gy-t pedig a 84%-a. A magas dózisokat mindössze a laboratóriumok 47%-a (3,27Gy) illetve 74%-a (2,7Gy) határozta meg elfogadhatóan, míg a parciális test-dózis esetén az arány mindössze 35% volt. A parciális test-dózis esetén az eredmények nagyon szórtak úgy a dózis meghatározásában (2,28-7,89Gy), mint a sugárnyaláb útjába eső testfelület becslésében (31-75%). [16]

Az OSSKI biodozimetriai laboratóriumában az első összemérés során a besugarazatlan kontrollt, az alacsony teljes test-dózist valamint a parciális test-dózist a meghatározott bizonytalansági faktoron belül sikerült meghatározni. A magasabb teljes test-dózist csupán 0,08 ezreddel becsültük a bizonytalansági határ fölé, viszont a MultiBioDose által előírt dózis-kategóriákba minden dózist megfelelően soroltuk be. A 2. táblázat röviden összefoglalja a valós és általunk becsült dózisokat, a valós dózistól való eltéréseket, valamint a bizonytalansági faktorokat.

Triage kategória	alacsony		magas	
Valós dózis	0Gy	0,94Gy	3,27Gy	4,75Gy
OSSKI által becsült dózis	0Gy	1Gy	4Gy	5,60Gy
Abszolút deviációk	0	0,06	0,73	0,85
Elfogadhatósági intervallum	±0,5Gy	±0,5Gy	±0,65Gy	±0,95Gy

2. táblázat Az általunk mikronukleusz assay-vel becsült dózisok viszonyulása a valós dózishoz az első összemérés során.

A két összemérés között, eredményeink és dózis-becslési hatékonyságunk növelése érdekében biodozimetriai gyakorlatokon vettünk részt, aminek következtében valóban javult a második összemérés során laboratóriumunk teljesítménye.

A *második összemérés* során hasonlóképpen az alacsony dózist a megadott bizonytalansági határon belül, a magas dózist viszont 0,05%-kal felette sikerült becsülni, viszont ismét a megfelelő MultiBioDose értékkategóriákban. A 3. táblázat foglalja össze a valós és általunk becsült dózisokat az első összemérésben, valamint a bizonytalansági faktorokat.

Triage kategória	alacsony	magas
Valós dózis	0,85	2,7
OSSKI által becsült dózis	0,99Gy	3,29
Abszolút deviációk	0,14	0,59
Elfogadhatósági intervallum	±0,5Gy	±0,59Gy

3. táblázat Az általunk mikronukleusz assay-vel becsült dózisok viszonyulása a valós dózishoz a második összemérés során.

Dicentrikus kromoszóma assay

A második DIC összemérésben vettünk részt. Az alacsony dózis becslésénél (0,85Gy±0,5Gy) minden résztvevő a dicentrikusok átlagához közeli (5,13dic/50metafázis) számú dicentrikus kromoszómát jelentett le. Minden kiértékelt lemez esetében a megbecsült dózis a 95% konfidencia-szinten belülre esett. A magas dózis esetén (2,7Gy±20%) a résztvevők többsége helyesen ítélte meg a 28.8dic/50metafázis körüli dicentrikus kromoszómák számát. A 90 becslés 61%-a esett a tolerált régióba. [17] Az OSSKI munkatársai mindkét dózist felülbecsülték, viszont a nagyobb dózis esetén a megfelelő triage kategóriába soroltuk, míg az alacsony dózis esetén alig 0,03%-al tértünk el a bizonytalansági szinttől.

Triage kategória	alacsony	magas
Valós dózis	0,85	2,7
OSSKI által becsült dózis	1,38	3,52
Abszolút deviációk	0,53	0,82
Elfogadhatósági intervallum	±0,5Gy	±0,54Gy

1. táblázat: Az általunk becsült dózisok viszonyulása a valós dózishoz a második összemérés során.

Teloméra-centroméra festéssel kiegészített DIC assay:

Minden résztvevő az előzetesen megadott kritériumok alapján számolta le a dicentrikus kromoszómákat, acentrikus és centrikus gyűrűket, valamint az acentrikus kromoszóma darabokat. A négy telomérrel rendelkező acentrikus kromoszóma darabok a letört kromoszóma-végek fúziójával jönnek létre, a dicentrikus kromoszómák képződése során. A két telomérrel rendelkező acentrikusok vagy nem fuzionáló acentrikusok kromoszóma végződések delécii vagy a gyűrűk kísérői. A telomér nélküli acentrikusok interszticiális dekéciókat jelentenek. A DIC-TC assay nagyon homogén eredményeket adott: a teljes-test dózisok megbecsülése minden laboratórium esetén a valós dózis ±20% intervallumába esett. (0.94 és 3.27Gy). [22]

Baleseti szcenário levezetésének/ tanulságai

A virtuális radiológiai balesetet szimuláló gyakorlatok 27 héten keresztül zajlottak. Mindössze egy laboratórium utasította vissza a koordináló szerep (referencia laboratórium, RL) begyakorlási lehetőségét. Koordináló partnerként a laboratóriumok elektronikus levél útján aktiválták a hálózatot, begyűjtötték és jelentették az eredményeket. Az aktiváló e-mail-re érkező válaszok idejét rögzítették és összesítették. Az aktiváló e-mail-re érkező válaszok száma az elvárásoknak megfelelően júliusban és augusztusban volt a legalacsonyabb, szeptemberben pedig a legmagasabb. A válaszok átlagos ideje 8±4 óra volt, ez függött az intézmény típusától

(pl. egy kórházban a páciens kezelése nagyobb prioritást élvez) valamint az időzóna-eltolódástól (Canada, Uruguay) vagy a személyzet méretétől. A RL-ok válaszadási idejét is mérték, kiértékelték. Két jelentést kellett küldeniük a szimulációs gyakorlatot levezető laboratóriumnak, az első jelentés visszaérkezési ideje 7,6±2,1 nap, míg a második jelentés beérkezési ideje 8,3±2,4 nap volt. Átlagosan egy baleset eredményeinek a visszaérkezési ideje 14 nap volt. [7]

A RL-ok továbbá felmérték a hálózat heti kapacitását is az egyes laboratóriumok által vállalható minták számát illetően. A gyakorlat teljes ideje alatt a segítséget nyújtó laboratóriumok (SL) összességében 122115 mintát vállaltak, ami egy heti 4520±210 minta-átlaghoz vezet. A legkevesebb mintát június, július és augusztus során vállalták a RENEB partnerek, ami egybeesik a nyári szabadságolásokkal. A minták 40%-át γH2Ax módszerrel, a 20%-át DIC assay elvégzésével vállalták. Legkevesebb mintát a PCC assay segítségével vállaltak feldolgozni a laboratóriumok, ami annak köszönhető, hogy ez a módszer aránylag kevés, alacsony kapacitású laboratóriumatóriumban használatos. [7]

Azok a SL-ok, akik pozitív választ adtak a hálózatot aktiváló levélre, egy táblázatot kaptak kézhez, amelyben 54 virtuális sérült dozimetriai adatai voltak. Ezt a táblázatot kiértékelték, majd visszaküldték a RL-nak. A táblázatok 7%-a nem érkezett vissza, ami az internet kapcsolatok deficitjének, a személyzet egyéb fontos elfoglaltságának vagy a túlságosan megnyúlt válaszidőnek volt betudható (a határidőn kívül beérkező válaszokat nem vették figyelembe). [7]

A táblázatokban található értékeket a megadott kritériumoknak megfelelően értékeltük ki. Az értékelési sémák a SL-ok 40%-a automatikusan, a páciens kódokból listát alkotva vagy valamilyen macro bevezetésével értékelte ki a táblázatokat, a többi laboratórium pedig manuálisan, minden táblázatot új adatsorként kezelve. A SL-ok által adott válaszok az esetek több, mint 90%-ában megfelelőek voltak. A mi laboratóriumunk minden táblázatot új adatsorként, egymást ellenőrizve értékelte ki. A visszaérkező adatok szórásából egyértelműen kimutatható volt, hogy a különböző SL-ok gyorsan megtanulták kiértékelni a kézhez kapott adatsorokat. A gyakorlat folyamán a hálózatban részvevő laboratóriumok között maximum három adatsornyi eltérés volt ennek megítélésében. [7]

MEGBESZÉLÉS, KÖVETKEZTETÉSEK

Egy esetleges tömeg-katasztrófa helyzet bekövetkezése esetén a biológiai és fizikai retrospektív dózis-meghatározó módszerek rendkívül hasznosak lehetnek az orvosi személyzet munkájának támogatásában. A DIC napjainkban a nemzetközileg elismert arany sztenderd a biológiai dózis-meghatározásában.

A vérminták szállítása az európai országokba megoldható volt 24 órán belül. Az Európán kívül elhelyezkedő országokba a helyi sajátosságoknak köszönhetően elfogadhatatlan mértékű késések voltak tapasztalhatóak, amelyek arra engedtek következtetni, hogy egy tömeges szerencsétlenség esetén az Európán kívül található partnerek számára a speciális diagnosztikai anyagoknak megfelelő minták postázása ésszerűtlen szállítási és csomagolási költségekkel járna. Egy lehetséges alternatíva volna ezen országoknak az eredmények virtuális értékelésben való bevonása vagy előzetes felkészülés a sürgősségi helyzetekben történő szállítás megvalósítására. [17,24,25]

Legmegbízhatóbbnak a dózis-becslések során a fél-automata értékelési módszer bizonyult. Ez összhangban van a MultiBioDose és NATO tanulmányok eredményeivel. [25,26] Sürgősségi helyzetben gyors, megbízható dózisbecslésre van szükség a klinikai személyzet munkájának alátámasztására. Mivel nem minden laboratórium rendelkezik automatizált rendszerrel a binukleáris sejtek értékeléséhez, speciális, kevesebb munkát igénylő stratégiák kidolgozása lenne célszerű a manuális módszer gyorsabbá tételéhez. Nemrég a NAÜ javaslata

alapján a DIC assay triage módozatához hasonlóan a MNA értékelését is triage módban végeznénk, ami mindössze 200 binukleáris számolásával járna mintánként. Az összemérések során nem volt szignifikáns különbség 2000 és 500 sejt értékelése esetén az eredményeket illetően. [22] A két MNA összemérés alapján a módszer triage eszközként való bevetésének hasznossága bizonyítottá vált egy radiológiai tömeges vészhelyzet esetén: a RENEB partnerek mindhárom esetben elfogadható, alacsony hibahatárral jellemezhető dózisbecsléseket végeztek.

A DIC assay fontos eszköze az elnyelt dózis becslésének perifériás vér limfocitákban. A módszer egységesítése a hálózat munkájában részt vevő laboratóriumok között ugyanakkor létfontosságú egy tömegszerencsétlenség esetén. Ezért fektettek a szervezők nagy hangsúlyt a projektben résztvevő laboratóriumok számára, vontuk be a lehető legnagyobb számú laboratóriumot az összemérésekbe. Összesen 31 ország 42 laboratóriuma vett részt és 550 dózis-becslés került feljegyzésre és értékelésre. [17]

Annak ellenére, hogy a DIC assay egy jól kidolgozott biodozimetriai módszer, a protokollok nem teljesen egységesek a laboratóriumok között. A variációk beleestek a NAÜ által megadott irányelv-intervallumokba. Javasolt a rövid távú (3h) Colcemid kezelést követően fluoreszcens és Giemsa festést alkalmazni, vagy pedig a hosszú távú (24h) Colcemid kezelést választani. A dózis-hatás görbék többsége szintén a NAÜ irányelveknek megfelelő volt. Amint az erre irányuló kérdőívek kiértékeléséből kiderült, a kevésbé sikeres dózis-becslések leggyakoribb oka a külső forrásból származó dózis-hatás görbe használata volt. [17]

A DIC assay pontos értékeléséhez 500-1000 metafázis leszámolása szükséges. Nagyszámú minta gyors kezeléséhez 20-50 sejt vagy 30 DIC értékelése javasolt, ami ugyan bizonytalanabbá teszi a becslést, viszont egy második körben lehetséges a ténylegesen sérült személyek mintáinak pontosabb értékelése. Ezen értékelési stratégia alkalmazásával nagy mennyiségű felesleges munka is elkerülhető (amivel például a hamis tüneteket mutató egyének mintáinak pontos értékelése járna). [17]

A RENEB összemérések során bebizonyosodott, hogy a dózis-kategóriák nagyon pontosan kerültek meghatározásra, alacsony és magas dózisra egyaránt. Rendszeres összemérések szükségesek a hálózaton belül a dózis-meghatározások minőségének megőrzéséhez.

A teloméra-centroméra festéses módszer a viszonyítási alapul szolgáló DIC assay által adott eredményeknél megbízhatóbbnak és robusztusabbnak bizonyult. Az eredeti Giemsa/egyszínű kromoszóma-festés esetén kevesebb dicentrikus kromoszómát sikerült azonosítaniuk a partner laboratóriumoknak. A különböző acentrikus töredékek típusának pontos azonosítása a DNS kettős törések számának pontos meghatározását is lehetővé teszik. Még a legmagasabb variációs lehetőséget rejtő teljes test-dózis esetében is csökkent a különböző laboratóriumok által meghatározott dózisok szórása és akár 30%-kal is nőtt a dicentrikusok frekvenciája. Ugyanakkor érdemes megjegyezni, hogy ez esetben a különböző laboratóriumok ugyanazokat a képsorokat elemezték. Egy következő lépés lenne a módszer bevezetése a többi RENEB partner eszköztárába is, amikor is saját készítésű lemezeken és kalibrációs görbén is megismételhetjük az összemérést. Szintén további kísérletek szükségesek a módszer reprodukálhatóságának felméréséhez. [22]

Az OSSKI biodozimetriai laboratóriuma minden esetben a megfelelő triage kategóriába sorolta a vakon értékelt minták dózisát, így a jövőben megfelelő szakmai segítséget képes nyújtani egy radiológiai baleset során. A jelenleg használatban lévő ^{60}Co gamma dózis-hatás görbe enyhén magasabbra becsüli a dózist. Ez valószínűleg a Co gamma sugárforrás alacsony dózis-rátájának tudható be. A közeli jövő feladata az új dózis-hatás görbe elkészítése, a dicentrikus assay teloméra-centroméra festéssel együtt történő bevezetésével.

A baleseti szcenárió gyakorlat célja a résztvevők felkészítése volt olyan hatalmas adatmennyiség kezelésére, amely egy tömegszerencsétlenség alkalmával halmozódhat fel. Minden résztvevő gyakorlatot szerzett úgy a hálózat aktiválásában, mint a kisegítő laboratórium szerepében, az eredmények értékelésében és a nagy adathalmazokat tartalmazó táblázatok

kezelésében. Az európai laboratóriumok készültségi állapotának fontos tükre lett a 27 héten át megismételt információ-begyűjtés. A 28 résztvevő laboratórium válasza a hálózatot aktiváló e-mail-re soha nem haladta meg a 8 órát, ami, figyelembe véve a hálózat globális jellegét és a laboratóriumok számát, nagyon jó idő. [7]

Összességében a RENEB hálózat dozimetriai triage kapacitása egyetlen radiológiai sürgősségi helyzet esetén 4520 páciens, az esetek 40%-ában γH_2A_x módszerrel vizsgálva, amelyet a vizsgálatok számát illetően a dicentrikus assay követ. [6,7,25)

A különböző szcenáriók megítélésének helyessége kiemelkedő volt annak ellenére, hogy számos változótól függött. A gyakorlat hasznosságát mutatja, hogy a kisegítő laboratóriumok a gyakorlat során szemmel láthatóan fejlődtek ezek megítélésében.

A szimulációs gyakorlat folyamán az idő becslése leegyszerűsítve történt, nem vettük figyelembe a minták kiküldésének és a kísérletek elvégzésének idejét. E két tényezőt azonban az összemérési gyakorlatok során teszteltük, amikor is ezen folyamatok 2-5 nap alatt zajlottak le. A hálózat aktiválása és az adatok begyűjtése nem tart két napnál tovább.

A gyakorlat nehézsége, különlegessége számunkra abban állt, hogy pont az augusztus 20-ai hét jutott a koordinálási feladatra. A gyakorlat ezen szakaszában munkatársaink túlnyomó többsége szabadságát töltötte. Az augusztus a nyaralás szempontjából Európa-szerte a legnépszerűbb hónap, ebből kifolyólag a hálózat kapacitása is lecsökkent. Jelentőségét növeli Nemzeti Ünnepünk, hiszen leginkább a fővárosban, de vidéken is jellemzően nagy tömegek gyűlnek össze ünnepelni a szabadban, köztereken és országos szinten szabad nap, ami a terror veszély növekedésével is járhat.

Amennyiben egy partner laboratórium munkatársai bármely téren nem teljesítik sikeresen a hálózat mérési kritériumait, számíthatnak a hálózat támogatására. A RENEB keretein belül a partnerek lehetőséget nyújtanak egymásnak megismerni a gyakorlott, jól működő biodozimetriai laboratóriumok munkáját, ahol tanácsot kaphatnak vagy gyakorlatot szerezhetnek az adott módszerrel kapcsolatosan. A különböző nemzetközi atomenergia szervezetek és nagy gyakorlattal rendelkező laboratóriumok biodozimetriai képzéseket is szerveznek. A hálózat teljesítményének szinten tartására rendszeresen összemérések szervezését tervezzük a továbbiakban is.

KÖVETKEZTETÉSEK

Összességében elmondható, hogy a RENEB tagok készen állnak koordinált választ adni tömeges radiológiai vészhelyzetek esetén. A hálózat egy rugalmasan kezelendő csoportosulás, amely új tagok és új módszerek irányában egyaránt nyitott. Már a hálózat kezdeményezési szakaszában nyolc új tag csatlakozott és négy új módszer került kipróbálásra. Újabb, biodozimetriai potenciállal rendelkező módszerek integrálása is folyamatban van. [6,22] A közeljövő feladata a RENEB hálózat elismertetése a radiológiai sürgősségi helyzetéért felelős nemzeti és nemzetközi hivatalos szervezetek által.

FELHASZNÁLT IRODALOM

[1] *National Strategy for Combating Terrorism, February, 2003* https://www.cia.gov/library/reports/general-reports-1/terrorist_cbrn/terrorist_CBRN.htm (letöltve: 2017.07.21)

[2] https://obamawhitehouse.archives.gov/the-press-office/2016/04/01/nuclear-security-summit-2016-communiqu%C3%A9 (letöltve: 2017.07.21.)

[3] INTERNATIONAL ATOMIC ENERGY AGENCY: *The radiological accident in Goiania. Part IV. Observations and recommendations*. Vienna, Austria. STI/PUB/815, ISBN:92-0-129088-8, pp. 89. 1988.

[4] MÉTIVIER, H. (szerk.): *Chernobyl: assesment of Radiological and Health impacts*. NEA, 2002 https://www.oecd-nea.org/rp/pubs/2003/3508-chernobyl.pdf (utoljára letöltve: 2017.09.13)

[5] OECD: *Nuclear Energy Agency (NEA) activities in follow-up to the TEPCO Fukushima Daiichi nuclear accident*. https://www.oecd-nea.org/pub/nea6888-follow-up-fukushima.pdf (letöltve: 2017.09.13)

[6] VOISIN, P., Et.al..: *RENEB – Realising the European Network in Biological Dosimetry* http://reneb.eu/documents/2012_MP-HFM-223-19.pdf (letöltve: 2017.07.05)

[7] KULKA, U., Et.al.: *RENEB – Running the European Network of biological dosimetry and physical retrospective dosimetry*, International Journal of Radiation Biology, 2017. 93:1, pp. 2-14, DOI: 10.1080/09553002.2016.1230239 2017.07.05

[8] BRZOZOWSKA, B., Et.al.: *RENEB accident simulation exercise*, International Journal of Radiation Biology, 2017, 93:1, pp. 75-80, DOI: 10.1080/09553002.2016.1206230

[9] KÖTELES GY. (szerk.): *Sugáregészségtan.* Medicina Könyvkiadó, Budapest, 2002.

[10] INTERNATIONAL ATOMIC ENERGY AGENCY: *Cytogenetic dosimetry: Applications in preparedness for and response to radiation emergencies.* EPR-biodosimetry, IAEA, Viena 2011.

[11] KULKA, U., Et.al.: *Realising the european network of biodosimetry (RENEB,)* Radiation Protection Dosimetry 2012, pp. 1–5 doi:10.1093/rpd/ncs157

[12] KULKA, U.,Et. al..: *Realising the European network of biodosimetry: RENEB—status quo* Radiat Prot Dosimetry. 2015 Apr; 164(1-2) pp. 42–45. doi: 10.1093/rpd/ncu266

[13] WOJCIK, A., LLOYD D., ROMM, H., ROY L.: *TENEB: Towards a European Network of Excellence in Biological Dosimetry,* http://cordis.europa.eu/pub/fp7/euratom-fission/docs/teneb-final-report_en.pdf (letöltve: 2017.08.10)

[14] MULTIBIODOSE: www.multibiodose.eu (letöltve: 2017.07.25.)

[15] EURADOS: European Radiation Dosimetry Group: *EURADOS Working Group 10: Retrospective Dosimetry.* 2015, http://www.eurados.org/-/media/Files/Eurados/documents/Working_Groups/2015/details/WG10-2015.pdf?la=en&hash=72B77C53F8D550C616FB59E073A39A906CE3FE8A (letöltve: 2017.07.05)

[16] DEPUYDT, J., Et. al.: *RENEB intercomparison exercises analyzing micronuclei (Cytokinesis-block Micronucleus Assay)*, International Journal of Radiation Biology, 2017, 93:1, pp. 36-47, DOI: 10.1080/09553002.2016.1206231

[17] OESTREICHER, U., Et. al.: *RENEB intercomparisons applying the conventional Dicentric Chromosome Assay (DCA)*, International Journal of Radiation Biology, 2017, 93:1, pp. 20-29, DOI: 10.1080/09553002.2016.1233370

[18] TROMPIER, F., Et. al.: *Overview of physical dosimetry methods for triage application integrated in the new European network RENEB, International Journal of Radiation Biology*, 2017, 93:1, 65-74, DOI: 10.1080/09553002.2016.122154518/2009.

[19] WOJCIK, A., OESTREICHER U., BARRIOS. L., VRAL, A., TERZOUDI, G., AINSBURY, E., ROTHKAMM, K., TROMPIER, F., KULKA U. *The RENEB operational basis: complement of established biodosimetric assays*, International Journal of Radiation Biology, 2017, 93:1, pp.15-19, DOI: 10.1080/09553002.2016.1235296

[20] DEPERAS, J., SZLUINSKA, M., DEPERAS-KAMINSKA, M., EDWARDS, A., LLOYD, D., LINDHOLM, C., ROMM, H., ROY, L., MOSS, R., MORAND, J., WOJCIK, A.:. *CABAS: a freely available PC program for fitting calibration curves in chromosome aberration dosimetry*. Radiat Protect Dosim. 2007, 124:115–123.

[21] AINSBURY, E.,A., LLOYD, D.,C.: *Dose estimation software for radiation biodosimetry*.Health Phys. 2010, 98:290–295.

[22] AINSBURY, E., Et. al.. *Integration of new biological and physical retrospective dosimetry methods into EU emergency response plans – joint RENEB and EURADOS inter-laboratory comparisons*, International Journal of Radiation Biology, 2017, 93:1, pp. 99-109, DOI: 10.1080/09553002.2016.1206233

[23] MONTEIRO GIL, Et. al.: *Capabilities of the RENEB network for research and large scale radiological and nuclear emergency situations*, International Journal of Radiation Biology, 2017, 93:1, pp. 136-141, DOI: 10.1080/09553002.2016.1227107

[24] ROMM, H., Et. al. *Performance of the automated dicentric and cytokinesis block micronucleus assays in a recent NATO exercise of established biodosimetry methods* (poster), IRPA, 2012, http://www.irpa.net/members/P02.145.pdf (letöltve: 2017.09.18)

[25] ROMM, H., Et. al:. *Web based scoring is useful for validation and harmonisation of scoring criteria within RENEB*, International Journal of Radiation Biology, 2017, 93:1, pp. 110-117, DOI: 10.1080/09553002.2016.1206228

[26] MULTIBIODOSE - *Final publishable summary report of the project* http://www.multibiodose.eu/News/MBD%20final%20publishable%20summary.pdf (letöltve: 2017.09.18)

HADMÉRNÖK

XIII. évfolyam 3. szám – 2018. szeptember

THE BEHAVIOUR OF NUCLEAR FUEL DURING SEVERE ACCIDENT PROCESSES

NUKLEÁRIS ÜZEMANYAG VISELKEDÉSE SÚLYOS BALESETI FOLYAMATOK ESETÉN

MANGA László

(ORCID ID: 0000-0003-1672-7629)

mangalaci@indamail.hu

Abstract

The issue of safety is paramount for nuclear power plants. The lessons learnt from previous nuclear accidents and the achievements in modern science and technologies drive nuclear professionals to attempt further reducing the already low probability of nuclear accidents.
A significant component of these efforts is to continuously perform risk analyses and model emergency situations on the currently operating power plants, which can contribute to nuclear safety enhancement. In the following I present such an example from the Paks nuclear power plant.
This article highlights the importance of prompt and correct decision-making during different types of emergency situations, and as a result, what is the significance of a well-timed flooding in case of a core-melt accidentt)

Keywords: *accident management, fuel melt, core damage, intervention time, core flooding*

Absztrakt

Az atomerőművek esetében mindig nagyon fontos kérdés a biztonság. Az eddig bekövetkezett nukleáris balesetek tanulságai, a tudomány- és a technika fejlődése arra sarkallja a szakembereket, hogy az eddig is kis valószínűséggel bekövetkező balesetek kockázatát tovább csökkentsék.
Ennek egyik fontos összetevője, hogy a már üzemelő erőműveken is folyamatos kockázatelemzéseket, modellezéseket végezzenek. Ennek köszönhetően tovább növelhető a nukleáris biztonság. A következőkben bemutatok erre egy példát, hogyan működik ez a Paksi Atomerőműben.
A cikk rávilágít arra, hogy a különböző jellegű baleseti szituációkban mennyire fontos a gyors és jó döntés és végeredmény képen, milyen jelentősége van - egy esetleges baleset során - az elárasztás időzítésének.

Kulcsszavak: *balesetkezelés, üzemanyag olvadás, zónasérülés, beavatkozási idő, zóna elárasztás*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.28.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.05.

INTRODUCTION

During the design of nuclear power plants an annual core damage frequency is calculated based on the combinations of different event sequences and operation modes. For the Paks nuclear power plant this number is 5.6·10-5/year [1, 2, 3, 4]. However, other analyses have pointed out that the damage of spent fuel stored outside the reactor core, namely in the spent fuel pool could also cause significant radioactive release. The calculation for the Paks nuclear power plant is 2.27·10-5/year [2, 3, 4). Based on these evaluations it can be deducted, that significant radioactive releases would be attributable to events resulting in the melting of the active core, or the exposure and consequent damage of spent fuel in the spent fuel pool. These special emergency processes will be referred to in the following as accidents.

Even though the frequency of occurrence is fairly low, it cannot be disregarded, as the accident consequences would be substantial [5, 6, 7]. In the following I shall describe the prevention and mitigation measures for potential core or fuel damage as well as managing the accident process.

DEVELOPING EMERGENCY OPERATING PROCEDURES

The Paks nuclear power plant applies Westinghouse type [8] symptom-based emergency operating procedures (ÁOKU) [9, 10]. Table 1 contains the most important characteristics of the Westinghouse accident management system.

<table>
<tr><td></td><td colspan="3">ACCIDENT MANAGEMENT</td></tr>
<tr><td>Event</td><td>Design basis accident</td><td colspan="2">Beyond design-basis accident</td></tr>
<tr><td>Objective</td><td>Remaining within the licensing parameters</td><td>Prevention of core melting, retaining activity in the containment</td><td>Mitigation of core melt consequences</td></tr>
<tr><td>Systems</td><td>Application of operational and safety systems within their design basis limits</td><td colspan="2">Application of all available systems beyond their design limits</td></tr>
<tr><td>Accident management type</td><td colspan="2">Prevention</td><td>Consequence mitigation</td></tr>
<tr><td>Procedures</td><td colspan="2">Event-based accident management
Condition-oriented accident management</td><td>Accident management procedure</td></tr>
</table>

Table 1: The accident management characteristics of the Westinghouse procedure system [11]

Measures can be categorized in two categories: preventions and consequence mitigations. Preventive measures focus on averting and preventing damage to the core, while the measures of the other category aim to prevent or mitigate the consequences of the core damaging processes.

The Westinghouse system covers not only the scope of design basis accidents, but also beyond design-basis emergencies and severe accidents (see figure 1).

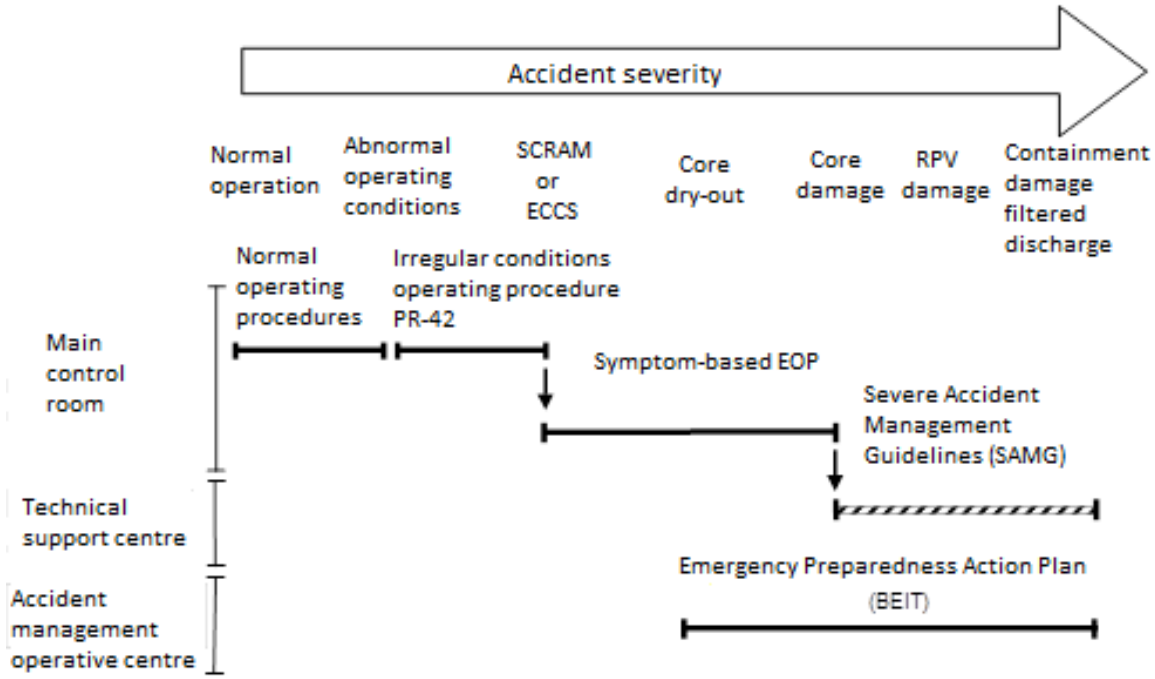


Figure 1: The Westinghouse system for managing the different operating and emergency conditions of a nuclear power plant [12]

For preventive measures the operational and safety systems of the plant are utilized within their design parameters, and the objective is to maintain the processes within the licensing limits applicable for design basis accidents.

For preventive measures also, the application of any piece of equipment can be considered beyond its design basis parameters, which is capable of preventing damage to the core in case of a beyond design-basis accident.

Preventive measures can generally be divided into two categories. The first category is when the emergency event can be clearly identified and the process is well-known; for this category event-based emergency procedures apply. In case of events in the second category only the symptoms of the event can be identified. In such cases symptom-based emergency procedures need be applied, where interventions focus on the recovery of the safety functions. For processes that occur after core damage, only symptom-based emergency procedures can be applied to mitigate the consequences of such processes. To achieve the objective, any system can be utilized beyond its design basis parameters.

The Paks nuclear power plant has implemented the symptom-based emergency operating procedures that cover the scope of preventive measures [13].

During the development of the emergency operating procedures the safety objectives have been defined [9, 10]. The procedures within the strategy aim to fulfil these safety objectives. Table 2 presents these safety objectives.

Safety objective	Function	Damaging process	Procedure
Preventing the melting of the core	Restricting reactivity Maintaining heat removal Maintaining core cooling	Insufficient control Loss of secondary side cooling Loss of primary circuit cooling medium	Primary circuit pressure decrease ECCS recovery
Preventing the damage of the reactor pressure vessel	Reactor pressure vessel integrity	Insufficient cooling	Reactor shaft flooding ECCS recovery
Preventing damage to the containment	Containment integrity	Hydrogen combustion Slow over-pressurization Local high temperature	Ignitors, recombiners Sprinkler, filtered discharge Cooling, door shielding
Preventing the release of radioactive materials	Retaining radioactive materials within the containment	Fission products in the containment	Sprinkler, filtered discharge

Table 2: Safety objectives, functions and procedures recommended to achieve the objectives

In the following I shall describe the strategic steps to achieve the first two safety objectives.

RESTRICTING CORE MELTDOWN, AND PREVENTING THE DAMAGE OF THE REACTOR PRESSURE VESSEL BY INTERNALLY FLOODING THE DAMAGED ACTIVE CORE

The flooding of the reactor pressure vessel (RPV) is such an accident management option, which aims to avert the progression of severe accidents to avoid core damage and to prevent the damage of the reactor pressure vessel. The cooling water injected directly into the rector pressure vessel provides direct cooling for the overheated, or molten core and to reduce residual heat or cool down the core melt and to stabilize its temperature. The cooling water necessary for core flooding can be provided through the recovery of the affected core cooling system, or with the use of special water reserves.

After losing the original core geometry, the conditions for cooling also change significantly, further thermic and chemical reactions can be expected, and the restructuring and possibly the relocation of the core shall also be considered. Different cooling mechanisms may develop, which provide heat removal at different rates. Parallel with the core melt-cooling medium interactions, the core melt also gets in contact with the reactor vessel bottom, that may impair the integrity of the reactor pressure vessel.

Fuel overheating and failure

Figure 3 shows the behaviour of nuclear fuel and its degradation mechanism at high temperatures. The most significant parameter of degradation is the fuel cladding and fuel temperature.

After the core becomes exposed at a high temperature, the expansion of the fuel cladding is to be expected due to the pressure difference on the inside and outside of the fuel assemblies. The expansion, and the consequent rupture of the fuel cladding depends of the pressure difference (figure 3). At higher pressure rate the cladding damage occurs explosively, with a large rupture.

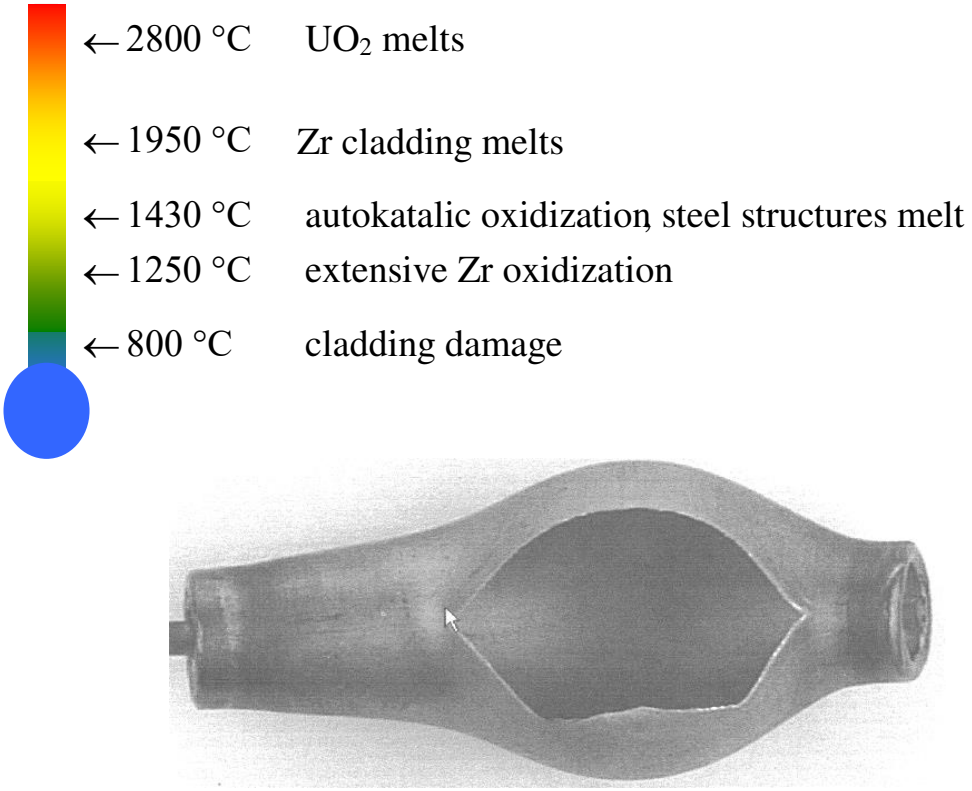


Figure 3: Expansion and rupture of fuel [14]

Consequently, significant zirconium oxidization takes place [15, 16], which also causes temperature increase, and the process becomes self-generating. Due to the oxidization occurring in a water-steam environment and the absorption of hydrogen, the fuel cladding becomes more rigid and the oxide layers start flaking. At approximately 1100°C ferrite-zirconium eutectoid is created, at 1450°C the ferrite components, at 1850°C the zirconium components, then at 2800°C the fuel itself melts down [3, 4, 17].

The core damage process

The Paks Nuclear power plant has modelled in detail the behaviour of fuel and fuel cladding [3, 4] for processes resulting in the loss of the cooling medium. The model was created with the MAAP/VVER program [18]. By following the core damage process in more detail, successful and unsuccessful event sequences could be better distinguished.

To check core damage success criteria, 28 different large diameter pipe rupture cases were considered. According to the divisions applied in probabilistic safety analyses, large diameter pipe ruptures are in the size range of 180mm to 2x492mm. Thus the investigated cases covered four rupture sizes (180, 280, 492 and 2x492 mm) [3, 4].
The program applies the following discrete types for core geometry damage (see figures 4, 5):

Type=0 – fully empty node, from where the active core has been removed,

Type=1 – coolable, rod type geometry,

Type=2 – structurally damaged, debris type node,

Type=3 – partially closed off (candle-like) geometry node,

Type=4 – Completely closed off by melt, uncooled node,

Type=5 – completely molten node.

Based on calculation results, it can be determined that without the hydro-accumulators the only way to avoid the core melting process, if the active core can be flooded in time with a large amount of active cooling medium, which can provide continuous cooling to the core and balance out local overheating. In those cases, when the volume of the active cooling medium is insufficient, local overheating and damage occurs at the core sections where the heat load is the heaviest, and where the cooling of the damaged sections is inadequate.

Figure 4 shows a case for temperature distribution at different times within the active core. It can be seen that in the first few minutes of the process, without cooling medium, the complete core is overheating rapidly.

The injection to the core starts at 330.s, by then the cladding had heated up significantly, and upon the injection of water, the generated steam initiates an explosive, autocatalytic Zr reaction in the hottest regions. The flooding of the core is completed by 600.s, however by then the nodes above the centre line had partially melted and the dripping melt partially or completely closed the lower nodes off from cooling.

These isolated nodes can no longer be cooled; thus the melting process continues within. The continuous melting process causes the structure to lose its integrity and the restructuring and relocation of the upper part of the core begins. As the system contains sufficient amount of cooling water, the moving debris remains in a continuously cooled state, however the melting section slowly moves downwards. 10 hours after the accident the upper 2/3 section of the core is damaged, while the melting process continues in the central nodes of the pile.

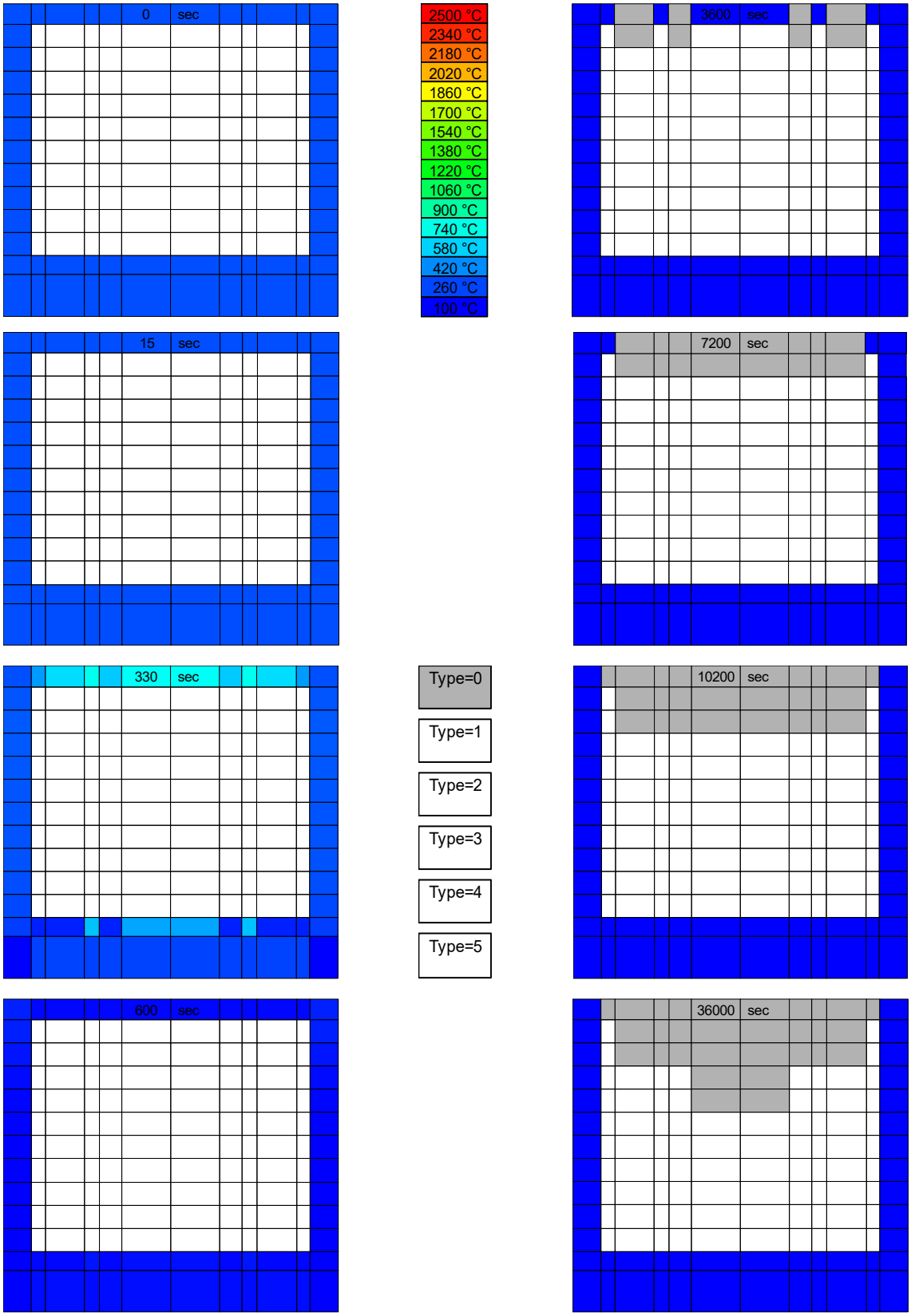


Figure 4: Temperature distribution and the core damage process at different times of an event [3, 4]

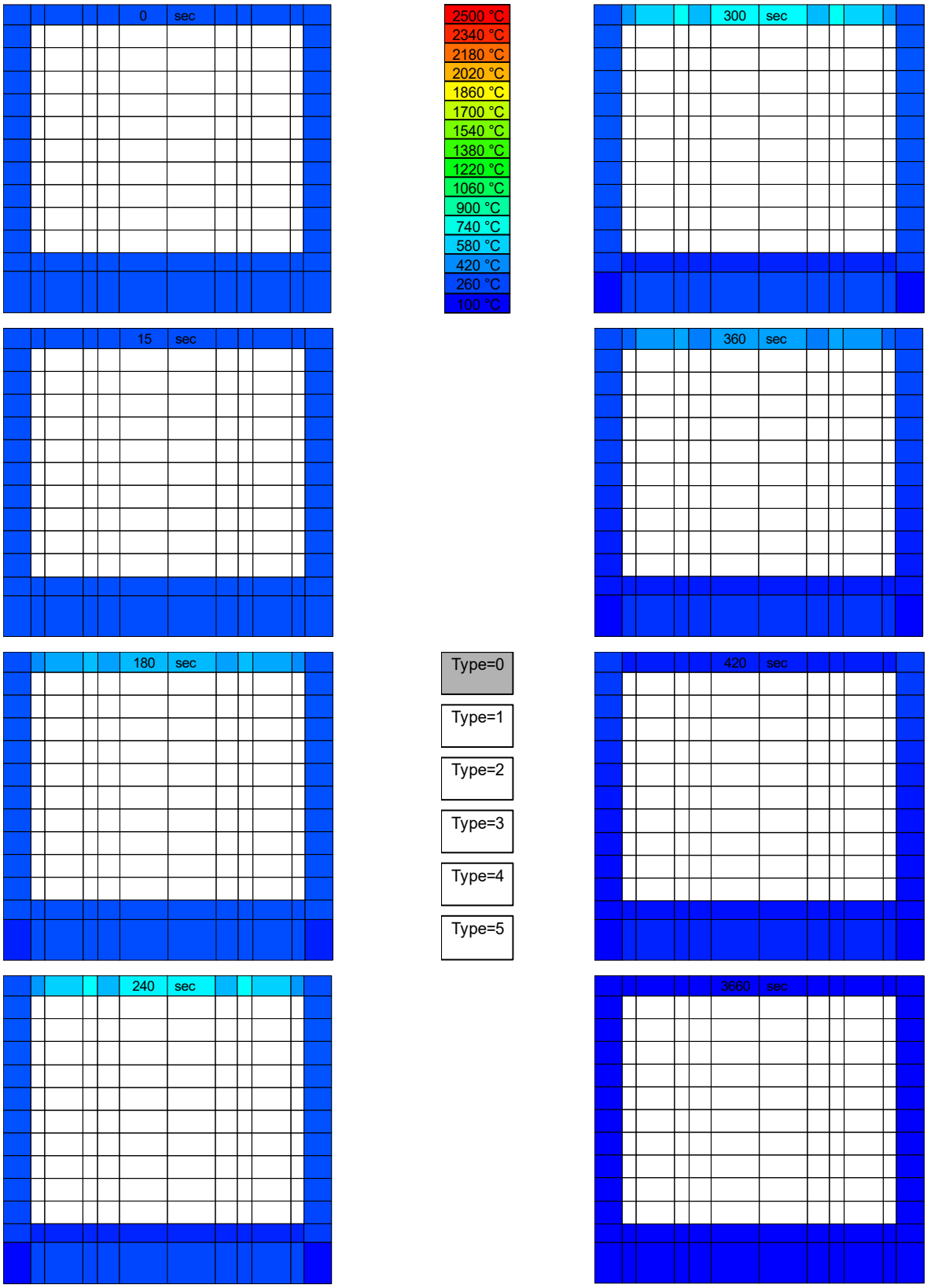


Figure 5: Temperature distribution and core damage process at different times of another event [3, 4]

Figure 5 shows the temperature distribution of another event. In this case refilling occurs earlier, from 240.s, when the core temperature is lower, thus in this case the intense zirconium oxidation does not result in local core melt and the development of uncooled geometry. After complete flooding, all nodes of the active core can cool off. Therefore, even though significant cladding oxidization occurred, the core remained in coolable condition.

Core collapse and core melt behaviour in the reactor pressure vessel

Table 3 contains the timeline of the most important events relating to the melting process [3, 4]. Core collapse occurs fairly soon (2-3 minutes) in case of LOCA (Loss of Coolant Accident) event sequences [19, 20], while in the case of other accident situations this might take up to 30 minutes. The reasons for this phenomenon are the difference in the remanent heat, thermohydraulic parameters, and the differing speed of zirconium-oxidization, which is significantly lower in case of LOEP events.

Event	LBLOCA (minutes)	SBLOCA (minutes)	LOEP (minutes)
Core exposure	15	181	491
Melting commences	30	212	520
Core collapse start	44	224	551
Core collapse finish	46	227	582
Fuel grid heat-up start	44	224	551
Fuel grid failure	73	250	599

Table 3: Timeline of the melting process and the collapse phase for different accident situations

where LBLOCA – large diameter pipe rupture,
SBLOCA – small diameter pipe rupture,
LOEP – complete loss of power.

Following the structural damages of the fuel pile, the core melt and debris sinks to the bottom of the pressure vessel. During the injection the core melt gets into contact with water and is temporarily cooled down. After the damage and meltdown of the structural elements underneath the active core, a debris bed is created at the bottom of the reactor pressure vessel. At the beginning of the injection, the water at the bottom of the pressure vessel boils away, and the debris continues to melt. Figure 6 shows the presumed layout in this status.

The basis of the presumption is that the oxides of uranium and zirconium create a so-called molten pool. Heat removal at the side of the RPV forms a thin crust around the pool. According to research findings, the metal content slowly rises to the surface of the oxide pool. The unmelted debris crates a debris bed above the metal layer. The content of the core melt changes dynamically due to the different heat exchange mechanisms.

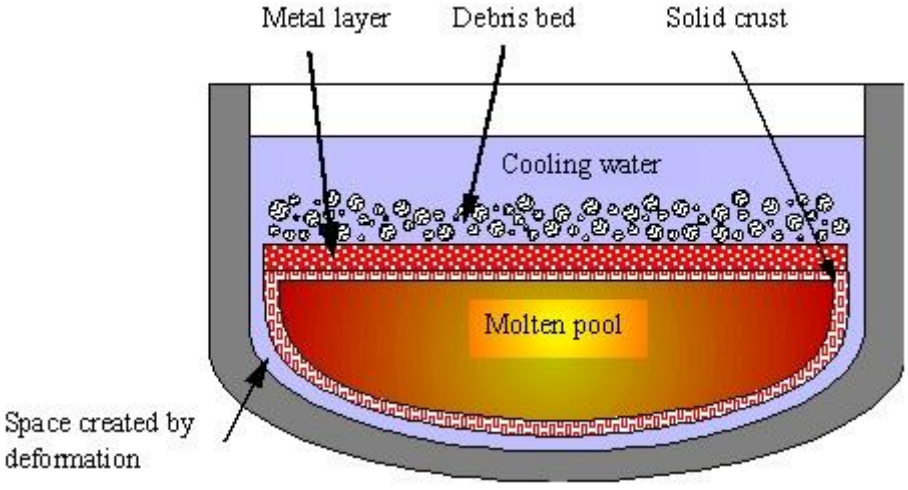


Figure 6: Position of the core melt at the bottom of the RPV [14]

The core melt located at the bottom of the pressure vessel may be cooled to some extent by flooding it with water. Some of the cooling water evaporates as it enters the debris and the cracks in the oxide melt crust. Another potential cooling mechanism is when the cooling water gets into the narrow space between the melt and the reactor vessel wall due to the creeping effect that occurs as the pressure vessel wall heats up. In these spaces heat removal takes place due to the critical heat flux developing in the region. This might provide sufficient cooling for the core melt generating approximately 15 MW energy [3, 4].

Failure of the reactor pressure vessel

The location of the damage is not restricted to the bottom of the RPV, especially if the failure occurs at a higher level (figure 7). In such case only the debris or melt above the failure point escapes to the pit bottom. Without cooling, the melt remaining at the bottom of the pressure vessel continues to overheat, which results in the second, catastrophic damage of the RPV. It is important to note however, that due to the first failure, the pressure vessel is already decompressed.

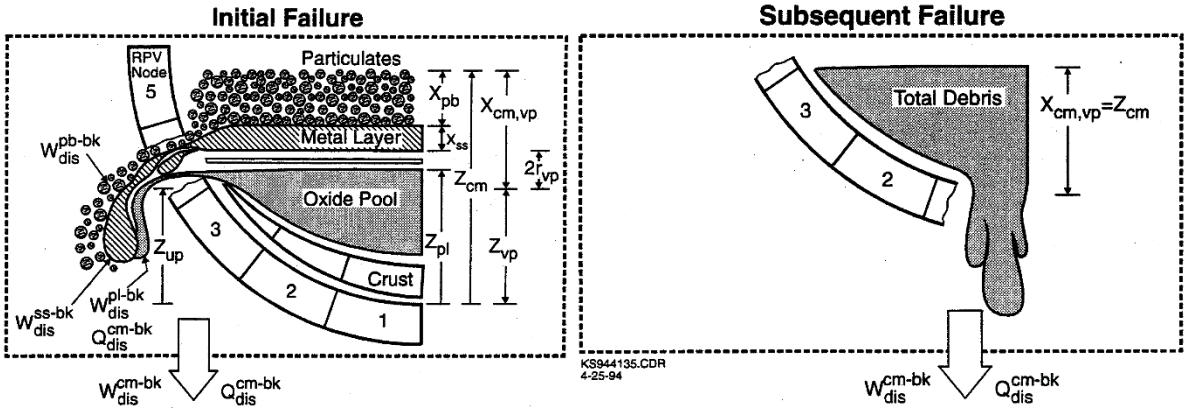


Figure 7: Location of the core melt at the bottom of the reactor pressure vessel [14]

There are no outlets at the bottom of VVER type pressure vessels, therefore only two damage types need be considered: fracture due to creeping and melt-through.

Investigating the potential avoidance of pressure vessel damage

Table 4 presents the calculation results for different size pipe ruptures, in which cases the core damage is due to the loss of the emergency core cooling system (ECCS) [3, 4]. Based on this table the necessity of core flooding is certain.

The first case is the reference case for RPV damage without flooding, the sixth case is the reference case for the process where the melt is flooded. Calculations generally stopped at the appearance of the primary failure on the reactor pressure vessel. Research only considered such loss-of-coolant initial events, where the primary circuit was at least partially depressurized. In case of high pressure, the considered injection options are limited, and the stress on the pressure vessel wall is also more extensive. Calculations were carried out to the point of primary pressure vessel failure, or if no such failure occurred, until 50400s process time. Only cases 2 and 20 contain information on the times when the second, more catastrophic RPV failure occurred [3, 4].

Analyses were carried out with the use of the MAAP program on the coolability of the molten core, and whether reactor pressure vessel failure can be avoided. The calculation results confirmed that with the timely introduction of the sufficient amount of cooling medium the core can be cooled down and stabile conditions can be achieved, while pressure vessel failure can be avoided even when core damage starts before the injection.

In cases without cooling, the time of pressure vessel failure depends on the initial event. The smaller the rupture size, the slower the core dry-out and the melting process. A pressure vessel failure can occur as late as 16 hours from the initial event. In case of larger ruptures this period is reduced to 5-6 hours.

Event	Rupture size [mm]	Start of injection [s]	Rate of injection [kg/s]	Time of pressure vessel damage [s]	End of calculation [s]	Comment
1	100	-	-	21600	+1000	
2	100	-	-	21600 (25700)	50400	
3	20	-	-	59000	+1000	
4	20	54000	10	-	100800	
5	20	58000	10	58500	+1000	
6	100	4250	10	-	50400	
7	100	4250	5	-	50400	
8	100	7250	10	-	50400	
9	100	7250	5	-	50400	
10	100	7250	3	14600	+1000	
11	100	9000	10	-	50400	
12	100	9000	5	13700	+1000	
13	100	10000	10	-	50400	
14	100	11000	10	11900	+1000	11 bars
15	100	11000	15	11600	+1000	16 bars
16	100	11000	30	11400	+1000	24 bars
17	100	12000	10	13800	+1000	
18	100	12000	10	14400	+1000	2xSV+RV
19	100	20000	10	20600	+1000	
20	100	22000	10	21600 (-)	50400	
21	200	-	-	18500	+1000	
22	200	13000	10	-	50400	

Table 4: Start of pressure vessel failure based on injection parameters

The emergency cooling systems must be recovered or other sources of cooling medium must be utilized within these timeframes to prevent pressure vessel failure. Due to the intense heat generation of the zirconium-steam reaction that occurs immediately after the damage of the active core, the recovery of cooling cannot prevent the melting of the core.

When the core melt at the pressure vessel bottom is flooded, depending on the initial rupture size, pressure increase develops. If the pressure vessel wall is overheated by the time flooding starts and cooling is slow, it is possible that the flooding itself will cause the pressure vessel failure. The point of such failure generally occurs not on the bottom of the RPV, but at least one metre higher, thus only part of the core melt can escape the damaged pressure vessel. Continuous cooling ensures that the catastrophic failure of the reactor pressure vessel does not happen. For larger rupture sizes the pressure increase is more moderate, therefore there is a better chance that the intervention is successful. In case of smaller rupture sizes, the pressure vessel wall heats up slower, due to less remanent heat in the core melt and the extended hydro-accumulator injection.

Based on the calculations, pressure vessel failure can be prevented with 10 kg/s injection rate within the following intervention times (table 5) [3, 4]:

Rupture size	Intervention time
20 mm	15.0 hours
100 mm	2.6 hours
200 mm	3.6 hours

Table 5: Pressure vessel failure prevention times at 10 kg/s injection rate

SUMMARY

During emergency situations when core cooling is lost and the fuel overheats, the integrity of the RPV is lost as a result and wall failure occurs. After the extensive overheating of the reactor vessel wall, flooding will also damage the reactor, causing further inhermeticity. The process results in the release of gaseous fission products into the primary circuit. However, the activity of the wall cracks is lower by an order of magnitude than the activity of the gasses remaining in the fuel matrix. Naturally, the objective is to prevent the damage of the fuel pellets, which is only possible with the flooding of the core.

The timing of the flooding is important. As there is no information available about the actual physical conditions of core behaviour during an accident, only indirect calculations, flooding must occur as soon as possible to prevent fuel meltdown.

The prompt flooding of the core must be part of any accident management strategy, even if fuel meltdown cannot be avoided, as pressure vessel integrity can only be maintained with cooling.

REFERENCES

[1] INSAG (International Nuclear Safety Advisory Group (1988): *Basic Safety Principles for NPPs.* Safety Series No. 75-INSAG-3, IAEA, Vienna. https://www-pub.iaea.org/MTCD/Publications/PDF/P082_scr.pdf (date of download: 2018.05.12).

[2] Hungarian Atomic Energy Authority: *National Assessment Report (Convention on Nuclear Safety).* 2012. http://www.haea.gov.hu/web/v3/OAHPortal.nsf/2DB98A2D49EF15A1C1257BEB002FAF6D/$FILE/CNS_extra_magyar.pdf (date of download: 2018.05.12).

[3] VEIKI Rt.: S*afety assessment report of the Paks nuclear power plant from the aspect of large volume radioactive releases. Management of the occurrence probability and uncertainty of physical processes.* June 2002.

[4] KFKI-AEKI, VEIKI Rt.: S*afety assessment report of the Paks nuclear power plant from the aspect of large volume radioactive release.* Extended study. May 2003.

[5] ANTAL Z., VASS Gy., KÁTAI-URBÁN L.: *Atomerőmű létesítés tűzvédelmi követelményeinek vizsgálata.* Védelem Tudomány, II. évfolyam, 1.szám (2017), ISSN 2498-6194 17-30. p. http://www.vedelemtudomany.hu/articles/02-antal-vass-kataiurban.pdf (date of download: 2018.05.12).

[6] MANGA L., KÁTAI-URBÁN L., *Nukleáris balesetkből levonható tanulságok – a tudomány állása I. rész,* Bolyai Szemle, XXV. évfolyam, 2016/4 szám ISSN 1416-1443, 120-136. p. https://folyoiratok.uni-nke.hu/document/uni-nke-hu/bolyai-szemle-2016-04.original.pdf (date of download: 2018.05.12).

[7] MANGA L., KÁTAI-URBÁN L., VASS Gy.: A Paksi Atomerőmű nukleárisbaleset-elhárítási rendszerének sugárvédelmi célú értékelése. *Védelem Tudomány,* II. évfolyam, 1. szám (2017), ISSN 2498-6194 152-162 p. http://www.vedelemtudomany.hu/articles/12-manga.pdf (date of download: 2018.05.12).

[8] Westinghouse: http://www.westinghousenuclear.com/About/News/Features/View/ArticleID/812 (date of download: 2018.05.12).

[9] KFKI-AEKI: *Preparations for developing an accident management procedure system*. 2003.

[10] VEIKI Rt.: *Determining the accident management procedure groups*. 2002.

[11] Bastien R. et al.: *Westinghouse Approach to Implement Post-Accident Recovery,* ENS TOPNUX'93, The Hague, Netherlands, April 25-28, 1993

[12] VÉGH J.: *Az atomerőmű biztonságos üzemeltetésének támogatása on-line folyamatinformációs rendszerek alkalmazásával.* Phd. értekezés, KFKI Atomenergia Kutatóintézet, BME Nukleáris Technikai Intézet, Budapest 2003.. http://dept.phy.bme.hu/phd/dissertations/vegh_disszertacio.pdf (date of download: 2018.05.12).

[13] Lenkei I.: *Westinghouse-type symptom-oriented procedures.* Guide for Paks NPP's operators, Paks (1995).

[14] Paksi Nuclear power plant: *Fuel behaviour during emergency and severe accident processes.* Training material, Paks 2004.

[15] DOBOR J.: *Iparbiztonság fizikai és kémiai alapjai.* Nemzeti Közszolgálati Egyetem, Budapest, ISBN 978-615-5491-06-1, 2014. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/8589/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y (date of download: 2018.05.12).

[16] PÁTZAY Gy.: *Atomenergetika és nukleáris technológia.* Egyetemi tananyag, Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest, ISBN 978-963-279-468-6, 2011. http://www.kankalin.bme.hu/Dok/Konyvek/Atomenergia/Atomenergetika_animaciok%20nelkul.pdf (date of download: 2018.05.12).

[17] DOBOR J., KOSSA Gy., PÁTZAY Gy.: *Atomerűvi balesetek és üzemzavarok tanulságai 1*. Hadmérnök. XII. évfolyam, 1. szám (2017) ISSN 1788-1919, 58-71 P. http://hadmernok.hu/171_06_dobor.pdf (date of download: 2018.05.12).

[18] Fauske & Associates: Engineering & Testing Services / Nuclear / MAAP – Modular Accident Analysis Program, https://www.fauske.com/nuclear/maap-modular-accident-analysis-program (date of download: 2018.05.12).

[19] KÁTAI-URBÁN L., KISS B.: Nukleáris erőművek, mint veszélyes technológiai és az országos nukleáris balesetelhárítási rendszer. *Hadmérnök,* IX. évfolyam, 3. szám (2014) ISSN 1788-1919, 80-97 p. http://www.hadmernok.hu/143_07_kataiul.pdf (date of download: 2018.05.12).

[20] C. Queral, J. Gondzález-Cadelo, G., Jimenez, E. Villalba: *Accident management actions in an upper-head small-break loss-of coolant accident with high-pressure safety injection failed,* Universidad Politécnia de Madrid, C/Alenza 4, 28003 Madrid, Spain http://oa.upm.es/11398/2/INVE_MEM_2011_104764.pdf (date of download: 2018.05.12).

HADMÉRNÖK

XII. Évfolyam. 3. szám – 2018. szeptember

A TŰZOLTÁSVEZETŐ FELADATAINAK VIZSGÁLATA KÁRESETNÉL, AZOK HATÁSA, KOMPLEXITÁSA, ÉS IDŐFÜGGÉSE SZEMPONTJÁBÓL

EXAMINATION THE TASKS OF THE LEADER OF THE FIRE FIGHTING AT AN EVENT; IN THE VIEW OF THE EFFECTS, THE COMPLEXITY AND THE TIME

NAGY László; RÁCZ Sándor

(ORCID: 0000-0002-2999-6847); (ORCID: 0000-0001-9955-924X)

nagyla63@gmail.com; racz.sandor@uni-nke.hu

Absztrakt

A tűzoltásvezető munkavégzésének eredményessége káresetek felszámolásakor szorosan függ a beosztottak, és a beosztott vezetők gyakorlatorientált felkészítésétől. A vezetői feladatok delegálása függ az egyének képességétől, tudásszintjétől, valamint gyakorlatától. A végrehajtók szintjén, az elméleti tudás mellett a begyakorolt mozdulatok készségszintű alkalmazása elengedhetetlen. A képzés gyakorlatias megközelítése különösen fontos ebben a szakmában. Az automatizmus csökkenti a bizonytalanságot, valamint több kipróbált módszer, és azok egymáshoz viszonyított hatékonyságának a vizsgálata növeli azoknak a mintáknak a számát, amelyekből a tűzoltók választhatnak a valós események kezelésekor. A tűzoltásvezető által létrehozott tűzoltási szervezet szintjeinek kialakításának, kohéziójának, és azok egymásra hatásának vizsgálata segíthet a vezetőre nehezedő feladatok racionalizálásában.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében a Nemzeti Közszolgálati Egyetem felkérésére, a Concha Győző pályázat keretében készült.

Kulcsszavak: *hatékonyság, összehasonlítás, gyakorlat*

Abstract

The effectiveness of the work of the leader of the firefighting depends on the practice-oriented preparation of the subordinates and the subordinate leaders. The delegation of leadership tasks depends on the people's ability, level of knowledge and practice. In addition on the executor level, the theoretical knowledges, and the skilful applications of the rehearsed move are indispensable. The practical approach of the training is very important in this job. Automation reduces uncertainty, and the more tested methods and their relationship to the effectiveness increases the number of samples that firefighters can choose during an intervention. Examining the design, the cohesion, and the interplay of the organization made by the leader of the firefighting can help to rationalize some leadership tasks.

The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016- 00001 titled „Public Service Development Establishing Good Governance” in the Concha Győző Program.

Keywords: *efficiency, comparison, practice*

A kézirat benyújtásának dátuma (Date of the submission): 2018.06.02.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.25.

BEVEZETÉS

Komplex tevékenység a tűzoltás taktika feldolgozása, hiszen egy művelet alatt hozott döntéseket, és azok hatásait kell elemezni, mind eredményességi, mind pedig biztonsági szempontból. Az eredményességet pedig a jogszabályoknak megfelelés, és a hatékonyságvizsgálat szempontjából kell tovább bontani. Megfelelhetünk a fő elvnek, az élet védelmének, mind a bajba jutottak, mind pedig a beavatkozó tűzoltók szempontjából, de megfelelhetünk egyszerre a tárgyak mentésének, és a biztonságnak is, de kockázatvállalás nélkül jellemzően nem tudjuk a feladatunkat elvégezni. [1] A kockázatvállalás sajnos velejárója a tűzoltó hivatásnak, viszont a fölöslegesen vállalt veszély természetesen nem. Mindenki, aki egyszer már látott tűzoltó tevékenységet, esetleg őt is mentette tűzoltó, tisztában van vele, hogy a tűzoltóknak valódi veszélyek között kell munkát végezniük, amelyek akár azonnali, élet kioltására alkalmas hatást fejthetnek ki az ott lévőkre. A tűzoltó munkát nem lehet virtuális térben végezni, ahol sebezhetetlenek vagyunk (vagy kapunk egy új életet, mint egy számítógépes játékban), és sokszor nem is lehet a hibánkat kijavítani, mint egy elgépelt papírlap újranyomtatását egy adminisztrációs tevékenységnél. Elvárt dolog, hogy a tűzoltó gyors, szakszerű, hatékony munkát végez, és ezen felül nem állítja meg semmi, valamint minden váratlan helyzetre van egy gyors, alkalmazható válasza. Hogyan lehetséges, hogy ilyen magas elvárás alakult ki a társadalomban ezzel a szakmával kapcsolatban? A tűzoltó szakma empirikus szakma, ahol a korábban jól működő eljárások honosodtak meg, és nem tűrt meg olyan metódust, ami nem vezet eredményre. Tehát a bajba jutottak azzal szembesülnek rendszerint, hogy az érkező mentő egységek ”tudják mit csinálnak”. Ez a szakszerűség természetesen a korábban kipróbált elemekre épül, és a technika fejlődésével, az eszközök modernizációjával vált egyre hatékonyabbá. A fejlesztési irányok, a jogalkotó szándékának megfelelően a biztonság garantálására épülnek. Ennek feltételei egyrészt technikai, technológiai természetűek, másrészt szervezeti struktúrát érintenek, valamint szerves része ez utóbbinak a felkészülés, oktatás, kiképzés gondolatköre. A tűzoltó beavatkozások elemzése is erre épül, azaz képesek legyünk felismerni a hibáinkat, azokból következtetéseket levonni, és a későbbiekben új megoldási lehetőségeket kidolgozni. A szerzők feltételezése alapján szükségszerű a korábban működő eszközök, eljárások hatékonyságát vizsgálni, és kipróbálni a helyzetek megoldására még hatékonyabb eszközöket, eljárásokat, módszereket vagy új vezetési elveket. Ehhez kapcsolódóan esetleg az oktatással kapcsolatos, mind elméleti, mind gyakorlati módszereinket is fejleszthetjük. Tehát folyamatosan vizsgálnunk kell az eszközeinket, és az eljárásainkat is. A szervezet működése, működtetése viszont a leginkább érzékeny pont, amelyet szükséges folyamatosan „finomhangolni”. Az optimalizálás, mert lényegében erről van szó, a cikk témáját tekintve a tűzoltói beavatkozás különböző szintjein keletkező feladatok végrehajtásáról, valamint azok célszerű szervezéséről szól.

A szerzők véleménye alapján a tűzoltók igyekeznek egyszerűsíteni, és a lehető legkevesebb elemi mozdulatból a lényeget érintő hatást kicsikarni. A szükséges minimum, de azt gyorsan, vagy az elérhető maximum, de azt csak később között, a szerzők véleménye alapján az előbbi stratégiát részesítik előnyben. Szokták mondani, hogy „*a tűzoltás szabályait vérrel írták”.* A racionális feladat-végrehajtás sok évszázados, vagy inkább évezredes tapasztalat alapján alakult ki a kollektív tudatban, és a szabályzókban. Egy tűzoltó, amennyiben rendelkezik 3 információval (pl.: ég valami, az helyileg hol van, hogy lehet megközelíteni) az elég az elsődleges feladatok meghatározásához. Ezek alapján már döntést fog hozni, és elkezdi a beavatkozás előkészítését, majd részletekbe menően igyekszik további információval felvérteznie magát a szakszerű végrehajtás érdekében. [2]

Egy „egysúlypontos káresetnél”, ahol lényegében egy konkrét területhez köthető a felhasznált erők, eszközök „könnyen” lehetséges végigkísérni a feladatokat, de ahol komplex feladatrendszer várható, területileg elkülönülő helyszíneken, ez csak a feladatok kiszervezésével, azokat delegálva, megbízásos módszerrel lehetséges. Az ilyenkor átruházott feladat alapján „lecsorog” a végrehajtás egy vezetői szintet, és inkább koordináló szerep jut a kárhelyszín parancsnokának.

Talán senki nem gondolt bele abba, hogy egy komplex káresetnél mekkora mennyiségű információ zúdul az irányító személyre, mindenesetre már vizsgálták azt az információmennyiséget, amellyel még képes megbirkózni az emberi agy. Körülbelül 6-8 közötti elemi információt képes feldolgozni az emberi agy egyszerre, és ebbe beletartoznak az információkkal végzett műveletek, tehát az elvonatkoztatás, halmazokba való csoportosítás, egymásra hatások vizsgálata is. [4] A mentális, vagy kognitív térképnek ki kell fejlődnie, meg kell erősödnie egy tűzoltóban, hogy biztonságosan, higgadtan tudjon döntéseket hozni. A cikk témáját tekintve, olyan gyakorlatban végrehajtható folyamatokat dolgoz fel, amely ennek a kognitív térképnek a kialakulását segíti.

Gyakorlati példákon keresztül lehet rávilágítani a kognitív térkép fejleszthetőségének a kérdéskörére. Egy lakóépületben keletkezett tűzesetnél a feladatok gördülékeny végrehajtása a képzettségre, a rutinra, és az összeszokottságra épül, valamint ezek koordinációjára, különös tekintettel az életmentéssel kapcsolatos épületátvizsgálást, és a cikk további részében feldolgozásra kerülő szerelési eljárásokat. Kipróbált, jól működő eljárások, valamint átélt sikeres helyzetek erősítik ezt a fejlettségi állapotot. A tűzoltásvezető által adott utasítás nem zárja ki az állomány kezdeményezőkészségét, amennyiben harmonizál az alapcél elérése érdekében hozott alapvető tűzoltásvezetői elképzeléssel. Ezek az önálló gondolatok, a mentális felkészültségünk a korábbi sikeresen végrehajtott legnagyobb előnyt ígérő fogásokból, eljárásokból állnak tehát.

PROBLÉMÁK AZ ELJÁRÁS KIVÁLASZTÁSÁBAN

Az alkalmazott eljárás kivitelezése tehát begyakorolható, viszont a helyszínhez alkalmazott legcélravezetőbb módszer már csak korábbi döntéseink, emlékeink, sikereink alapján kerülnek kiválasztásra, összhangban a szabályzókban előírtakkal. [5] Amit már korábban csináltam, és jól működött azt fogom választani, még ha adódhatna egy hatékonyabb módszer is, de ahhoz további felderítésre van szükség, mint például lakóépületek száraz, vagy nedves felszálló vezetékeinek az alkalmazhatósága, nem kockáztatok annak próbájával. [2] Ezért mindenképpen célszerű egzakt mérésekkel, próbákkal igazolni a választható módszerek egymáshoz viszonyított sikerességét, hogy a legelőnyösebb megoldást választhassuk.

A jogszabályok, belső szabályzók csak az elvárt feladatokat határozzák meg, tehát a „mit kell elvégeznem?” kérdésre adnak választ, a hogyanra nem. [3] Az eljárásoknak a begyakorlása folyamatos, hiszen begyakorló, és szerelési gyakorlatok javítanak ezeknek a minőségén. A gyakorlatok rendszerét belső szabályzó előírás határozza meg amely egyik fő gondolata szerint „*A gyakorlatokat úgy kell tervezni és végrehajtani, hogy azok során az állomány megfelelő ismeretet, jártasságot, valamint készséget szerezzen. A gyakorlatok tervezésénél, végrehajtásánál a tűzesetek és műszaki mentések, továbbá a korábbi gyakorlatok tapasztalatait is hasznosítani kell.”*[1]

[1] 60/2016. számú BM OKF főigazgatói intézkedés 2. számú melléklet

A gyakorlatok fajtái a tűzoltósági szakterületen a következőek:

Felkészítő gyakorlatok:

- vezetési gyakorlat;
- szerelési gyakorlat;
- tűzoltótechnika kezelői gyakorlat;
- helyismereti foglalkozás;
- szituációs begyakorló gyakorlat;
- tűzoltási gyakorlat.

Ellenőrző gyakorlatok:

- helyi szintű ellenőrző gyakorlat;
- területi szintű ellenőrző gyakorlat.[2]

A felkészítő gyakorlatoknak alkalmasnak kell lenniük többek között a szerelési készség fejlesztésére, az egyes feladatok különböző megoldási módszereinek kipróbálása, gyakoroltatása, a legjobb módszer kiválasztása érdekében, valamint a határozott, magabiztos, magas fokon szervezett beavatkozásra való felkészítés, a felmerült hibák és pozitívumok feldolgozása, a tapasztalatok levonása révén is. [8] Ezt az elvárást továbbgondolva a szerzők, a gyakorlatok egymásra épülésével kapcsolatban fejlesztési lehetőséget látnak, amely a készségszintű végrehajtási eljárásaink javítását eredményezhetik. [6]

Az alap szerelési eljáráson túl, de még a végleges komplex feladatvégzésen belül kell végrehajtási lehetőségeket kidolgozni, mégpedig azok egymáshoz viszonyított eredményességével. [9] Ez a típusú, összehasonlító gyakorlat végrehajtás még nem honosodott meg Magyarországon, de több alkalommal foglalkoztatta már a tűzoltókat. [10] [11] A végrehajtható eljárások egymáshoz viszonyított sikerességén, azok mérhető (időbeni) paraméterein, és az azokba befektetett energia alapján történő szelekción alapuló „mintagyűjtés” a szerzők véleménye alapján hatékonyabbá tennék a tűzoltói beavatkozásokat. Ez a kreatív szemléletű módszertanilag folyamatosan javítható, gyakorlati képzési forma lenne, amely által a variációs lehetőségeinket bővíteni tudjuk. A gyakorlatok során kialakítható automatizmus, különösen a mérés alatti végrehajtás esetében, már közelíthet ahhoz a „munkatempóhoz”, amely káreseteknél szükséges. Ez a megerősítési folyamat segítségünkre lehet, amikor a tűzoltónak, a káresetek felszámolásakor, megemelkedik a stressz szintje, és emiatt akaratlanul is beszűkül a látóköre. További pozitív hatása van a versenyszellemnek, amely jelen van a tűzoltói mentalitásban, ezért ez is motiváló erő a mozdulatok tökéletesítése érdekében racionalizált mozdulatok, mozdulatsorok kidolgozásánál.

Megvizsgálva a lakóépületekben, tűzoltók által kialakítandó oltóvízhálózatokat (szerelés), valamint összehasonlítva ezeket megállapíthatjuk, hogy ez később egy módszertani segédlet alapja lehet, amely összhangban az alap szerelési eljárásokkal, de azt továbbgondolva, eredményesebbé teheti a tűzoltó munkát. [12] A szerelési szabályzat[3] korábban meghatározott alapmozdulatokra építve, valamint azokat folyamatosan fejlesztve, ad kereteket a szakszerű munkavégzéshez, azonban például társasházakban, ezek különbözőképpen hajthatóak végre. A témát érintve a néhány szerelési lehetőség vizsgálata történt meg, valamint lett hozzá javaslat megfogalmazva.

[2] 60/2016. számú BM OKF főigazgatói intézkedés 2. számú melléklet
[3] BM OKF 3/2015. számú Főigazgatói utasítása a tűzoltóságok Szerelési Szabályzatáról

Szerelési szintidők

A szerelési szabályzat — ellenőrzött körülmények között végrehajtva — meghatározott időintervallumokat állapít meg típusos feladatokhoz (1. számú táblázat). Ezek az időintervallumok káresetnél nem biztos, hogy tarthatóak, de lehetséges a rövidebb végrehajtás is a körülmények függvényében. Különösen nem életszerű épített környezetben, például különböző lakóházak esetében felsőbb emeletekhez szerelt tűzoltó alapvezetékek[4], és a tűz oltására alkalmazandó sugár[5] megszereléséhez szükséges időt meghatározni. A vizsgálatok azt mutatják, hogy javíthatóak ezek az idők különböző módszerek élő helyszínen való gyakoroltatásával.

Az oltással kapcsolatos előkészítő folyamatok többszörösen megismétlődhetnek a tűzeset alakulásával, valamint egyéb bontási, vágási, behatolási feladatokat is kell végezni. [13] Ezzel együtt, és éppen ezért ezek a folyamatok minden esetben nagyobb erőt igényelnek, mint maga az oltási létszámigény a tűzoltás korai szakaszában, és a szerzők megállapítása alapján önálló vezetést is. [14] Emellett, ebben a szakaszban, a tűzoltásvezetőnek pontosan le kell határolnia feladatrészeket a végrehajtók számára.

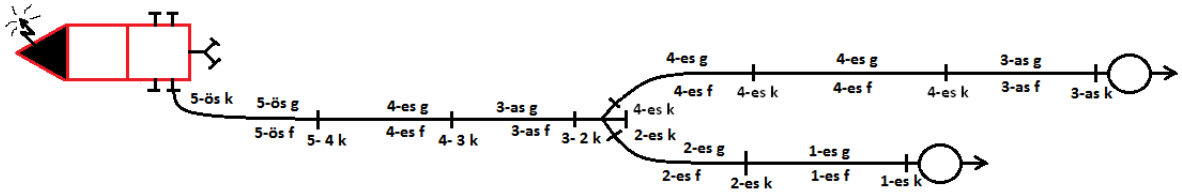
Sorszám	Szerelési feladat megnevezése	Végrehajtási szintidők /sec/
		Megfelelő
1.	Sugár szerelése 2 db tekercstömlővel	50
2.	Sugár szerelése 3 db tekercstömlővel	75
3.	Táplálás szerelése szívótömlővel	200
4.	Táplálás szerelése tűzcsapról, (föld feletti) 2 fővel (1 tömlő távolság esetén)	90
5.	Gépjárműfecskendőről osztott sugár szerelése tekercstömlővel, táplálás szívótömlővel (tömlőhosszabbítás nélkül)	320
6.	Gépjárműfecskendőről osztott sugár szerelése tekercstömlővel, táplálás (föld feletti) tűzcsapról 2 fővel (1 tömlő távolság esetén)	230

1. számú táblázat Szerelési szintidők (Forrás: 3/2015. BM OKF Utasítás szerelési szabályzat)

Az alap struktúra az 1. számú ábrán látható, amelyet épített környezetben természetesen a lakóház, vagy a terep adottságai miatt másképpen kell elképzelni. [15] A szabályzat — a későbbiekben látható módon — a végrehajtás főbb módozatait, és a módszereket előírja, azonban a módszerek helyszínenként nem egyformán célravezetőek.

[4] Tűzoltó tömlők egymáshoz kapcsolásával kialakított vízhálózat, amely egyik végén a tűzoltó gépjármű által rendelkezésre álló nyomás alatti vízmennyiség áll, míg a másik oldalán egy víz elosztására alkalmazott úgynevezett osztó (jellemzően 3 ágú) áll.

[5] Tűzoltó tömlők egymáshoz kapcsolásával kialakított vízhálózat, amely egyik végén az osztó áll, míg a másik végén a sugárcső (a víz kijuttatását szabályzó tűzoltó szakfelszerelés) áll.



1. **ábra** Alapvezeték, és osztott sugár sematikus ábrája síkban fektetve, betűjelekkel a szerelést végzők számkódja, és az általuk végzett tevékenység6

(Forrás: 3/2015. BM OKF Utasítás szerelési szabályzat)

A szerelési szabályzat külön meghatározza, hogy milyen módozatokat lehet alkalmazni a végrehajtáshoz :

1. Osztóval szerelt alapvezeték megkötése felhúzáshoz a sugárcsőkötél zárkapcsos végével
2. Osztóval szerelt alapvezeték megkötése felhúzáshoz a sugárcsőkötél kötél orsó felhasználásával.
3. Tömlővezeték megkötése felhúzáshoz a sugárcsőkötél zárkapcsos végével
4. Tömlővezeték megkötése felhúzáshoz a sugárcsőkötél kötél orsó felhasználásával [12]

Az első probléma az alapvezeték felhúzásánál jelentkezik, hiszen a lakóházak nem mindegyike rendelkezik megfelelő, tűzoltó gépjármű által megközelíthető oldala felőli lépcsőházból elérhető megfelelő ablakkal, vagy egyszerűen egy előtető a bejáratnál nehezíti meg ezt a folyamatot. Ezután rögtön jelentkezik a második probléma, ami az osztó kikötésével kapcsolatos.

A magasban végzett munka megköveteli, hogy visszaesés ellen is biztosítsuk a kiépített oltóvezetékeinket, amely több eszköz igénybevételével is történhet:

a. Alapvezeték osztóval kikötése sugárcsőkötél zárkapcsos végével
b. Tömlővezeték kikötése tömlőtartó kötéllel
c. Alapvezeték osztóval kikötése tömlőtartó kötéllel

Ezek a problémák jelentkezhetnek is a lakóházak tüzeinél, és értékes időt használunk arra, hogy kiválasszuk az optimálisnak vélt megoldást. [16] A gyakorlatok rendszere a tűzoltóságok tekintetében lehetőséget ad arra, hogy szerelési foglalkozások keretében fejlesszék a készségszintjüket a végrehajtók. Természetesen ez előírás is a szakszerű végrehajtás érdekében, de az „élő” helyszínen (különböző lakóépületek a városokban p.: Larsen-Nielsen házak, sávházak, pontházak, függőfolyosós bérházak) történő szerelés nem elterjedt. A parancsnok (Hivatásos tűzoltóság parancsnoka, vagy a szolgálatban lévő állomány szolgálatparancsnoka) szervezheti úgy ezeket a szerelési foglalkozásokat, hogy a hivatásos tűzoltóparancsokság működési területén, önkormányzati tűzoltóságok esetében az elsődleges műveleti körzetén belül végigjárják a különböző típusú és adottságú építményeket, és kidolgozzák az oltáshoz legjobban alkalmazható módszereket. [17]

[6] 3/2015 BM OKF Főigazgatói Utasítás szerelési szabályzat jelmagyarázat az ábrához: g= gurít; f=fektet; k=kapcsol

Alkalmazott szerelési feladatok típusos helyszíneken

Két konkrét példán keresztül tudjuk megvilágítani ezt a lehetőséget, amely Budapesten, és Dunaújvárosban került végrehajtásra. Nem egyedi kezdeményezések ezek, azonban a mért eredmények nem kapnak széleskörű publicitást. A tűzoltók általában a tapasztaltabbaktól szerzik be azt a tudást, amely a legjobb „fogás" alkalmazását fogja számukra jelenteni. Az összehasonlító elemzés ezért ritka, mert a legtöbb alkalmazott eljárás (akár mozdulatszintű fogás) már meghonosodott, és lényegében célravezető is, hiszen egy már korábbi sikeres végrehajtáson alapszik. Kijelenthetjük azonban, hogy a tűzoltók a másodpercekkel küzdenek a káresetek felszámolásánál, és a továbbiakban látható, hogy a gyakorlatot vezető parancsnok szemlélete az, hogy megállapítást tesz az esetleges nyerhető időre, azaz maradt-e idő a szerelésben.

Összehasonlító, alkalmazott, szerelési gyakorlat I.

A gyakorlat helye: Budapest, XX. kerület Ady Endre u. 100.
A gyakorlat ideje: 2013. október 11. 9^{00}-tól 12^{00}-ig
A gyakorlat formája: Szerelési gyakorlat (összehasonlító, alkalmazott: a szerzők)
A gyakorlat célja:

1. A középmagas épületekben történő beavatkozás gyakorlása különös tekintettel az alapvezeték és a sugárszerelés vonatkozásában.
2. A különböző szinteken az eltérő alapvezeték szerelési módok kipróbálása, összevetésük a hatékonyság és gyorsaság tekintetében.
3. A különböző szintek eléréséhez szükséges tömlők megállapítása.
4. A szükséges taktikai megoldások kialakítása.

A feladat egyik részét, nevezetesen az alapvezeték felhúzását tárgyalja a szerelési szabályzat, viszont a lépcsőkaron történő tömlőfektetést nem, és nem is támogatja más[7] belső utasítás sem, mégis ez is egy lehetséges megoldási forma, amelyet vizsgálni érdemes, és nem ritkán alkalmazásra kerül a tűzoltói beavatkozásoknál. A szabályzat általi alapvezeték felhúzási mód esetében részletesen meg vannak határozva a feladatokat, így ennek a végrehajtása utasítás szerint történt. A gyakorlat végrehajtásának időpontja 2013-ban történt, és más eljárási szabály[8] volt érvényben, viszont lényeget érintő részletekben nem tér el a mostani hatályban lévőtől[9].

A gyakorlat helyszíne egy Budapesten (XX. kerület) található panelépület, amelynek egyik főbejárata, illetve szilárd útburkolattal rendelkező utcafrontja az épület Nyugati oldalán található (1. számú kép). A lépcsőház kialakításából adódóan a lépcsőkarok mellett található a lift, közvetlenül mellette a szemétledobó helyiség. A lépcsőkarok két oldalán egy-egy üvegajtóval elválasztva loggián keresztül tudjuk az adott szinten lévő lakásokat megközelíteni. Az alapvezeték felhúzásnál ezt a loggiát használták a szerelést végzők, és az ellenkező oldali lakáshoz szerelték a sugarat.

[7] 6/2016. BM OKF Utasítás
[8] 102/2012. BM OKF Intézkedés a tűzoltóságok Szerelési Szabályzatáról
[9] 3/2015. BM OKF Intézkedés a tűzoltóságok Szerelési Szabályzatáról

1. kép. A panelház nyugati oldala (forrás: Vincze Zsolt Készült: Budapest, 2013.október 11.)

A gyakorlaton a negyedik, hatodik, és nyolcadik emeleten lehetett a feladatokat végrehajtani. A szerelési feladatok mindhárom szinten ugyanaz voltak:

a. Sugár szerelése, alapvezeték felhúzással. (szerelési szabályzat)
b. Sugár szerelése lépcsőkaron fektetett alapvezetékkel.

Alapvető célkitűzés az volt, hogy a két módszer közötti végrehajtási időkülönbséget mérhetővé tegyék, és ennek alapján, a későbbi éles beavatkozás alkalmával megfelelő döntéseket tudjanak hozni a parancsnokok.

A 6/2016 BM OKF Utasítás alapján megszerelhető az alapvezeték az orsótéren[10] keresztül is, de ebben a lépcsőházban orsótér nem állt rendelkezésre ezért ez a feladat nem került végrehajtásra.

Minden szerelés a gépjármű fecskendőből indult, a szükséges tömlők a fecskendő mellett elhelyezve (a feladat egységes mérhetősége érdekében). A szerelést végrehajtók a légzőkészüléket készenlétbe helyezve (hordhelyzetben, nem használva) viselték. A szerelést egy teljes raj (5 fő) hajtotta végre, de táplálásszerelésre[11] nem került sor. Az első „B" tömlő végén minden esetben osztó volt elhelyezve, amely praktikus a beavatkozók szempontjából, és két célt szolgálhat. Ennek egyik funkciója, hogy könnyedén leengedhető a beavatkozás végén a vízmennyiség a gravitáció segítségével, illetve műszaki probléma esetén kiváltható vele a használt gépjárműfecskendő. Az idő mérése a fecskendőből való kiszálláskor indult és az adott szinten a sugár megszerelését követően ért véget. [10]

[10] Lépcsőkarok közötti, lakóházakban eltérő nagyságú rés, amely alkalmas lehet tűzoltó tömlő elvezetésére (a szerzők)

[11] a tűzoltó gépjárműfecskendő folyamatos vízutánpótlására megszerelt vízhálózat, amelyet épített, városi környezetben jellemzően utcai, föld alatti, vagy föld feletti tűzcsapokról szerel a végrehajtó állomány (a szerzők)

A szerelési feladatok végrehajtása
Alapvezeték felhúzása külső falsíkon[12] a 8. emeletre:
Az egyes és kettes beosztásban[13] lévő sugárfelszereléssel a lépcsőkaron a szerelési szintre felhatolt, az alapvezetéket mentőkötél[14] segítségével felhúzta, az osztót kikötötte, a sugarat megszerelte.

Végrehajtási idő: 4 perc 58 másodperc.
Alapvezeték hossza: 3db „B" tömlő

A szerelést vezető parancsnok megállapítása: Az osztó, illetve az alapvezeték kikötése nem a szerelési szabályzat szerint történt (a szerelést végzők más kikötési módot használtak a gyorsítás érdekében), valamint utólagos értékelésével megállapította, hogy célszerűbb lett volna az osztót a lépcsőházban elhelyezni.

Alapvezeték szerelése a lépcsőkaron 8. emelet.
Az egyes és kettes sugárfelszereléssel felhatol a 8. emeletre. Az alapvezetéket a hármas és négyes szereli légzőkészülékben. Mindketten két-két darab „B" tömlőt visznek magukkal (többet nem tudnak a súlya, és a hordozhatósági nehézségek miatt). Az elgondolás az volt, hogy a tömlőket nem gurítják ki, hanem a felső kapocsnál fogva kihúzzák, miközben a másik előremegy. A tömlő állandóan beakadt, többször vissza kell menniük, megigazítani. A négy tömlő a hatodik emelet után elfogy, vissza kell menniük plusz tömlőkért.

Végrehajtási idő: 8 perc 34másodperc.
Alapvezeték hossza: 6 db „B" tömlő

A szerelést vezető parancsnok megállapítása: A szerelés a külső falsíkon történő felhúzáshoz képest majdnem kétszer annyi ideig tartott. Sok időt elvett, hogy vissza kellett menni plusz tömlőért. Amennyiben lett volna bevonható létszám a végrehajtásra, rádión kérhettek volna plusz tömlőket, amely összességében csak egy- másfél perccel rövidítette volna meg a szerelést. A tömlők kifektetése a fal mellett megfelelő volt, sehol nem volt beszorulva. A felhasznált 6db „B" tömlővel a 9. szint is elérhető lett volna.

Alapvezeték felhúzása külső falsíkon a 6. emeletre.
Az egyes és kettes beosztásban lévő sugárfelszereléssel a lépcsőkaron a szerelési szintre felhatolt, az alapvezetéket mentőkötél segítségével felhúzta, az osztót kikötötte, a sugarat megszerelte.

Végrehajtási idő: 4 perc 02 másodperc
Alapvezeték hossza: 2db „B" tömlő

A szerelést vezető parancsnok megállapítása: Az osztó a lépcsőházban lett kikötve (az előzőekben tapasztaltak figyelembe vételével).
Alapvezeték szerelése a lépcsőkaron 6. emelet

[12] „a sugarak működtetéséhez szükséges alapvezetéket lehetőség szerint az orsótérben vagy a külső falsíkon felhúzással kell szerelni" (BM OKF Intézkedés)
[13] a szerelési szabályzat számozással különbözteti meg a végrehajtók feladatkörét, amely a tűzoltó gépjárműveken betöltött szolgálati beosztásokra utal.(a szerzők)
[14] életmentésre, és egyéb feladatok végrehajtására rendszeresített kötél, amely 30 méter hosszúságú (a szerzők)

Az egyes és kettes sugárfelszereléssel felhatol a 6. emeletre. Az alapvezetéket a hármas és négyes szereli légzőkészülékben. Mindketten két-két darab „B" tömlőt visznek magukkal. Az elképzelés ugyanaz volt, mint az előzőekben azzal a különbséggel, hogy a társ nem megy előre, hanem együtt húzzák a tömlőket.

Végrehajtási idő: 3 perc 23 másodperc
Alapvezeték hossza: 5db „B" tömlő

A szerelést vezető parancsnok megállapítása: A gyors végrehajtás ellenére a nem gondos tömlőfektetés következményeként a száraz tömlők (nem voltak víznyomás alatt) a lépcsőfordulókban a korlát alá szorultak. Ennek következtében, ha nyomás alá helyeztük volna a tömlőket a víz nem tudott volna az osztóig eljutni. Kiszabadításuk nyomás alatt a parancsnok megállapítása szerint nem kivitelezhető. Megoldásként felmerült még a szerelés után a végrehajtók végigmennek a szinteken és kiszabadítják, kifektetik a tömlőket, amely további egy- másfél percet vett volna igénybe. A negyedik tömlővel az 5. emelet feletti fél emeletig ért el a szerelés. Tehát ismét szükség lett volna plusz tömlőre, amennyiben a BM OKF utasítás szerinti elvet *„Amennyiben lehetséges, az osztó helye az égő szinten, vagy afelett legyen meghatározva"*. A szerelést végzők, szabályosan eljárva, eltértek ettől, mert a tűzoltás sikerességét nem befolyásolta volna ez a különbség.

Alapvezeték felhúzása a 4. emeletre.
Az egyes és kettes beosztásban lévő sugárfelszereléssel a lépcsőkaron a szerelési szintre felhatolt, az alapvezetéket mentőkötél segítségével felhúzta, az osztót kikötötte, a sugarat megszerelte.

Végrehajtási idő: 3perc 43 másodperc
Alapvezeték hossza: 2db „B" tömlő.

A szerelést vezető parancsnok megállapítása: A végrehajtás során sok idő elment az osztó kikötésével, amely előfordulhat, mert egy kötéltechnikával végrehajtott mozdulatsorban „benne van" ennyi hibaszázalék, ezen kívül a szerelést végzők, úgy döntöttek, hogy 2db „C" tömlőből szerelik meg a sugarat. A kiértékelésnél a parancsnok felhívta a figyelmüket, hogy ez nem szükséges. Ezeket figyelembe kb. 30 mp. „benne maradt" a szerelésben.

Alapvezeték szerelése a lépcsőkaron 4. emelet
Az egyes és kettes sugárfelszereléssel felhatol a 4. emeletre. Az alapvezetéket a hármas és négyes szereli légzőkészülékben. Mindketten két-két darab „B" tömlőt visznek magukkal. A szerelés a szerelési szabályzattal összhangban, azaz a lépcsőn fentről lefelé, a tömlőt gurítva került végrehajtásra. A hármas az első tömlőjét másfél emeletről gurította, eközben a négyes a harmadikról tette ugyanezt.

Végrehajtás: 2 perc 12 másodperc
Alapvezeték hossza: 4db „B" tömlő

A szerelést vezető parancsnok megállapítása: A szerelés során mindkét alapvezetéket szerelő tűzoltó, az első tömlő kigurítása után a fent maradó kapocsra rátette a második tömlőjét, így a kifektetéskor azt nem húzta magával. Az alapvezeték szépen kifektetve a fal mellett volt megszerelve.

A gyakorlat végén, bár a lépcsőház nem volt rá tökéletesen alkalmas, megvizsgálták a végrehajtók, hogyan hajtható végre a szerelés, ha az alapvezetéket az orsótérben kézben felhúzva juttatják el a beavatkozás szintjére.
A szerelést vezető parancsnok megállapítása: Bár időmérés nem történt, és a tömlő is beszorult egyszer, az alapvezeték kevesebb, mint egy perc alatt a hatodik emeleten volt. Egy „B" tömlővel a lépcsőkar aljától a hatodik emelet érhető el. Egyértelműen ez a megoldás a legcélravezetőbb, a külső falsíkon történő felhúzás mellett, de a helyszín adottságai nem minden esetben engedik meg a legbiztonságosabb, és leggyorsabb megoldás alkalmazását. Előfordul, hogy mégis a lépcsőkaron szerelnek a tűzoltók, amelyet később életmentés céljából használni is kell, ezáltal a mentés körülményessé válik. Ez a megoldás csak akkor jöhet szóba, amennyiben a helyszínen tapasztaltak kizárják valamilyen okból a többit, vagy indokolatlanul hosszabb időt vesz igénybe a szerelés azokkal a módozatokkal.

2. kép A korlát alá szorult tömlő (forrás: Vincze Zsolt Készült: Budapest, 2013.október 11.)

Összefoglalva a gyakorlat tapasztalatait

Számos tapasztalat született a szerelési gyakorlat alatt, amely a későbbiekben segítheti az ilyen feladatvégrehajtást. Az egyértelművé vált, hogy a hatodik emelet felett a külső falsíkon történő alapvezeték szerelés gyorsabb, mint a lépcsőkaron szerelés. A hatodik emeletig viszont a lépcsőkaron történő alapvezeték szerelés gyorsabb, vagy közel azonos idejű a felhúzással. Az alapvezeték szerelésével foglalkozó 3-as, és 4-es beosztású, csak a hatodik emeletig tud plusz tömlő nélkül alapvezetéket szerelni a lépcsőházban. Mindeközben az is beigazolódott, hogy a lépcsőkaron szerelt alapvezeték akadályozza a mentést, és az épület kiürítését. További energia befektetését igényli, hogy a lépcsőkaron szerelt alapvezeték gondos fektetést igényel, mert a beszorult tömlők miatt az oltóvíz nem jut el az osztóig (2. számú kép).

A legbiztosabb módszer a lépcsőkaron fektetésnél, továbbra is a fentről lefelé történő gurítás. Ha a lépcsőkaron a tömlőket húzzuk, akkor plusz időt vesz igénybe a megfelelő kifektetésük. További praktikus tapasztalt, hogy egy tömlő biztonságosan másfél emeletet ér el a lépcső aljától. Tehát a gurítási pontok a „másfeledik", a harmadik, a „négy és feledik", a hatodik emeletek.

Az orsótér használata esetén, a leghatékonyabb megoldásnak, a tömlő, az orsótérben kézzel való felhúzása tűnik. Alkalmazható ott is ahol az orsótér olyan szűk, hogy a tömlőt felhúzni nem lehet, viszont nem alkalmazható ott ahol legalább 5cm nincs a két lépcsőkar között. Orsótérben kézzel felhúzás esetén egy tömlő a lépcsőkar aljától a hatodik emeletig ér el.
Mindezeket összefoglalva, a káreseti szerelési eljárások kiválasztásánál a következőket kell a vezetőnek mérlegelnie káresemény felderítő szakasza után, tudva, hogy a szerelési utasítása kiadása után már nincs idő jellemzően újabb verzió kidolgozására:

1. felhúzható-e az alapvezeték külső falsíkon?

2. nyitható-e ablak, megfelelő-e a mérete a tömlőfelhúzás kivitelezéséhez?
3. van-e orsótér?
4. van-e akadályozó tényező a külső falsíkon?
5. megtelepíthető-e magasból mentő
6. milyen rögzítési lehetőségek vannak?

Ezeknek a körülményeknek az ismeretében, a gyakorlatokon mért időeredmények alapján könnyebb lehet a hatékony módozat kiválasztása. A leghatékonyabb módozat kiválasztása csak mérések általi, összehasonlító, alkalmazott, élő helyszínen végrehajtott szerelési, vagy szituációs gyakorlatok alkalmával fejleszthetőek! [18]

Összehasonlító (szituációs) szerelési gyakorlat II.

A gyakorlat, egy olyan társasház területén került lefolytatásra, ahol a társasház, a tűzvédelmi hatóság engedélyével átalakította a meglévő száraz felszálló tűzvízvezeték rendszerét, úgy, hogy vízkivételi helyek csak a hatodik és fölötte minden második emeleten kerültek kialakításra. Egy zárt szekrényben elhelyezett csatlakozócsonkokkal került biztosításra a vízkivitel ezeken a szinteken. A gyakorlat megtervezésében, megszervezésében, segítséget nyújtott a Fejér Megyei Katasztrófavédelmi Igazgatóság Dunaújvárosi Katasztrófavédelmi Kirendeltség Hatósági osztályvezetője, aki a szituációs gyakorlat során részt vett az eredmények rögzítésében és kiértékelésében is.[11]

A gyakorlatot a Fejér Megyei Katasztrófavédelmi Igazgatóság Dunaújvárosi Katasztrófavédelmi Kirendeltség Dunaújváros Hivatásos Tűzoltóparancsnokság „A” szolgálati csoportja 10 fővel hajtotta végre.

A végrehajtás (kísérlet) ideje : 2018. április 12-én 9:00 óra.

A gyakorlat helyszíne: 2400 Dunaújváros, Köztársaság út 10-12. szám alatti társasház

A gyakorlat egy szituációs feltételezéssel indult, amely szerint 7. emeleti szemétledobó helyiségben keletkezett tűz, amely veszélyezteti a szinten élőket. Az állománynak a feladatot teljes védőfelszerelésben légzőkészülékkel (hordhelyzetben) kellett végrehajtania.

A gyakorlat során a következő feladatok kerültek meghatározásra:

a. táplálás és alapvezeték szerelése felhúzással (lépcsőházon belül, a lépcsőkarok közötti térben), osztó az 6. szinten, majd két darab „C” sugár szerelése,
b. földszintről táplált, beépített szárazfelszálló vezetékrendszer használatával két darab „C” sugár működtetése. A szárazfelszálló vezeték betáplálási pontja a földszinten volt.

A táplálás és alapvezeték szerelése felhúzással feladat végrehajtása a következőképpen valósult meg:

1. alapvezeték szerelés: 3 fő (5-ös, 4-es, 3-as beosztás), 1 db osztó a 6. emeleten
2. táplálás szerelés: 1 fő (5-ös beosztás), 1 db osztó a földszinten
3. első sugárszerelése a 6. emeletről: 2 fő (1-es, 2-es beosztás). Második sugár szerelése a 8. emeletre (3-as, 4-es beosztás). A feladathoz szükség volt egy teljes rajra.

A földszintről táplált, beépített szárazfelszállóról megszerelt vezetékrendszer kialakítása következőképpen valósult meg:

a. szárazfelszálló vezeték betáplálási pontjára csatlakozás 1 fő (5-ös beosztás) – osztó elhelyezése a betáplálási pont előtt
b. táplálás szerelés: 1 fő (5-ös beosztás),
c. alapvezeték szerelés: nem volt szükség
d. sugárszerelés: 2 fő (1-es, 2-es beosztás) 6. emeletre, 2. sugárszerelés a 8. emeletre (3-as, 4-es)

Mindkét gyakorlati feladat háromszor került mérésre, és minden esetben 1 teljes raj hajtotta végre. Egy raj ugyanazon beosztások mellett kétszer hajtotta végre a feladatokat.

3. kép: Szituációs gyakorlat – (Forrás: Somogyi Gábor, Szili István, Készült: Dunaújváros 2018.április 12.)

Mért eredmények osztófelhúzással:

1. A két sugár működtetéséhez leggyorsabb esetben is 6 perc 51 másodperc szükséges.
2. Az első sugár működtetéséhez 5 perc 01 másodperc, míg a második sugár működtetéséhez átlagosan 6 perc 59 másodperc szükséges.

Mért eredmények szárazfelszálló vezeték használatával:

Az első sugár működtetéséhez szükséges legjobb idő 1 perc 48 másodperc volt, míg a második sugár működtetéséhez 2 perc 46 másodpercre volt szükség.

Következtetések:

A mért eredmények egyértelműen a száraz felszálló vízhálózat használatának hatékonyságát erősítették, amely valószínűsíthető is volt a kevesebb munkaelem miatt. Az előnye a másik módszerhez képest viszont az, hogy 3 fő is elegendő volt az első sugár működtetéséhez a korábbi 5 fővel szemben. A hatályos belső szabályzó rendelkezik is ennek a módszernek az alkalmazási lehetőségének a vizsgálatáról a beavatkozás felderítési szakaszában, azonban sok társasház — különösen a régebbi építésűek — nem fordítanak kellő figyelmet ezek működőképesen tartására. Sok esetben megrongált, hiányos állapotban, szabálytalan módon, elzárva találhatóak ezek. Ezt a körülményt ismerve, a tűzoltók, nem szívesen szerelnek ezen beépített eszközök segítségével oltóvíz hálózatot, hanem inkább a saját kiépítésben bíznak. Az első sugár rendelkezésre állása, kulcsfontosságú a beavatkozás sikerességének szempontjából, mert a zárt téri tűzfejlődések esetében akár 4-6 perc alatt kialakulhat a helyiség teljes égése. A nyerhető több mint 3 perc, és az így optimalizálható létszámigény az életmentésbe bevonható személyek tekintetében is hatékonyabb végrehajtást biztosít. A második sugár szerelése

biztonsági szempontból kerül elrendelésre a hatályos belső szabályzó előírása miatt [3], a felső szintekre történő tűzterjedés megakadályozása miatt, azonban amennyiben nem szükséges az üzemeltetése, a felszabaduló létszám azonnal átcsoportosítható életmentésre.

4. kép: Szerelés a szárazfelszálló vezeték használatával – (Forrás: Somogyi Gábor, Szili István, Készült: Dunaújváros 2018.április 12.)

ÖSSZEGZÉS

A szerzők által megállapítottak alapján fontos lenne olyan alkalmazott eljárások módszertani kézikönyv, vagy segédlet elkészítése az alkalmazható módszerekről, valamint azok használhatóságáról, amely típusos helyszíneken megvalósítható módozatokat tartalmaz, összehasonlítva azokat egymással időfüggés, és befektetett energia alapján, kiemelve azok előnyeit, és hátrányait. A szerelési szabályzat általi „iskolaszerelési eljárások”, és a végrehajtás lehetőségei nem ugyanazt jelentik. Egy esetleges környezeti változó kizökkenti a végrehajtót, és improvizálnia kell valamit, amely hasonló eredményt hoz. A tűzoltó folyamatosan gordiuszi csomókat vág át azért, hogy a hatékonyságát megőrizze. Szükségszerű lemodellezni folyamatokat, és mérhetővé tenni a nyereséget, az eljárások között. Az ilyen típusú gyakorlat alatti empirikus folyamatok és a közvetlen értékelés növeli a problémamegoldó képességünket. A mérések által átélt minimális stressz szint is hasznossá válhat, hiszen kis mértékben modellezi a beavatkozások légkörét. További megállapítás ilyen helyszínek esetében, hogy szigorúbb hatósági szankciókkal, pontosabb nyilvántartással a beépített száraz, és nedves felszálló vezetékek alkalmazhatóságát biztosíthatnánk a beavatkozó tűzoltók részére, hiszen egyértelmű a mért értékek alapján az időnyereség ezek használatával.

Ezeknek a módozatoknak a kidolgozása, és abból készségszintű választás a közvetlen vezető szintje (személyes vezető). Elengedhetetlen, hogy a kárhelyszínen döntési helyzetben lévők szakmai kompetenciája alulról, tehát a végrehajtás szintjétől épüljön fel. Azok, akik a mozdulatszintű végrehajtást már begyakorolták számos környezetben, megfelelő döntési alternatívákhoz jutottak, amelyre már lehet egy személyes vezetői szintet építeni. Azok, akik ezt a szintet megfelelő időtartamig gyakorolták, azoknak célszerű személyes vezetői, majd irányítói szintre lépniük. Mindezek alapján, kimondható, hogy a tűzoltás vezetésének a folyamata eltér a szervezeti vezetői folyamatoktól, ezért nem szükségszerűen kompatibilisek egymással.

A tűzoltásvezetői szinthez legerősebben a koordináció kapcsolódik, amely a szerzők véleménye szerint vertikálisan magasabb szintet jelent a vezetési struktúrában.

A közleményben leírtak alapján, kimutattam a Katasztrófavédelem tűzoltókat érintő képzési rendszerében rejlő további lehetőségeket, amely leginkább abban rejlik, hogy a leggyorsabban

végrehajtható alternatívát adja a vezető kezébe. A feldolgozott gyakorlatokból következtethetően, a hatályos szervezési elvek alapján nem biztonságos olyan többsúlypontú esemény felszámolása, ahol a tűzoltásvezető egyrészt személyes vezetésre, másrészt közvetett irányításra is kényszerül, hiszen a figyelmét más kérdések megválaszolása köti le.

Annál az eseményrészletnél, ahol a tűzoltásvezető nem tud primer információkhoz jutni szükségszerűen le kell azokat határolni, és önálló súlypontként kezelni, önálló erő, eszköz, és létszám hozzárendelésével, személyes vezető jelenléte mellett. Nem elvárható ezáltal, megfelelő alternatíva kiválasztása olyan személytől, aki nem kap vizuális megerősítést a körülményekről. A folyamatot, és lehetséges választható megoldásokat ismernie kell, de csak a célértékről való eltérésnek kell visszakerülnie az ő szintjére. Az alacsonyabb szintű beosztott vezetőnek is rendelkeznie kell a szükséges megoldási minta készlettel, és csak a lényegi, stratégiai lépéseket befolyásoló eseményekről kell a magasabb vezetői szintet értesítenie.

További megállapítás, hogy a tűzoltás szervezetének kialakítását, és különösen a komplex feladatok végrehajtása érdekében létrehozott — tűzoltásvezetői munkát segítő — különleges beosztások szervezését, és alkalmazását is szükségszerűen gyakoroltatni kell a tűzoltás vezetésére jogosult állománnyal. A szerzők későbbi kutatása, ezen elvek mentén arra irányul, hogy milyen összehasonlító módszerek alkalmazhatóak a tűzoltás szervezetének hatékonyabb kialakításának vizsgálatához, amely a feladatok gyorsabb pontosabb lehatárolásához, a vezetői szintek célszerű kialakításához vezethet, beleértve az egyéb kialakítható segítő beosztások kialakításának fontosságát.

FELHASZNÁLT IRODALOM

[1] 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról;

[2] 39/2011. (XI. 15.) BM rendelet a tűzoltóság tűzoltási és műszaki mentési tevékenységének általános szabályairól;

[3] 6/2016. (VI.24) BM OKF Főigazgatói utasítás a Tűzoltás-taktikai Szabályzat kiadásáról

[4] RESTÁS Á.: A tűzoltásvezetők döntéseit elősegítő mechanizmusok; Védelem - Katasztrófa- Tűz- És Polgári Védelmi Szemle 20:(5) (2013) 11-14. o. ISSN 1218-2958 http://www.vedelem.hu/letoltes/ujsag/v201305.pdf?6 (letöltve: 2017.12.12.)

[5] RESTÁS Á.: Alkalmazott tűzoltás; Egyetemi jegyzet, Nemzeti Közszolgálati Egyetem, 2015; ISBN 978-615-5527-23-4

[6] PÁNTYA P.: Lehetőségek a katasztrófavédelmi, tűzoltói beavatkozó biztonság növelésére, Szerk.: POKORÁDI L. Műszaki Tudomány az Észak-kelet Magyarországi Régióban 2014. Debrecen: MTA Debreceni Akadémiai Bizottság, 2014. 214-222. o. http://store1.digitalcity.eu.com/store/clients/release/mtekmr_2014.pdf (letöltve: 2017.12.08.)

[7] PÁNTYA P.: A katasztrófavédelem és a tűzoltóságok hazai és nemzetközi tevékenysége, a beavatkozások keretei, a biztonság és hatékonyság megjelenése Hadmérnök 12:(2) (2017) 201-213.o. http://www.hadmernok.hu/172_16_pantya.pdf (letöltve: 2018.03.11.)

[8] 60/2016. számú BM OKF Főigazgatói intézkedés a készenléti jellegű szolgálatot ellátó tűzoltó állomány napi továbbképzésének, valamint a tűzoltósági szakterület által tartandó gyakorlatok rendszerének szabályairól

[9] PÁNTYA P.: What could help for the firefighting, technical rescues? In: STEFAN G., ANDREA M., BORIS T. (szerk.) ANDREA M., BORIS T. Advances

in Fire, Safety and Security Research 2015. Bratislava: Fire Research Institute of the Ministry of Interior Slovak Republic, 2015. 60-65.o. ISBN:9788089051199

[10] Vincze ZS.: Alapvezeték szerelés középmagas épületnél (szerelési gyakorlat Budapesten 2013. feljegyzés a gyakorlatról, a szerző engedélyével)

[11] SZILI I.: Középmagas és magas épületek megelőző tűzvédelme BSC szakdolgozat 2018. NKE

[12] 3/2015. számú BM OKF Főigazgatói utasítás a tűzoltóságok szerelési szabályzatáról

[13] BODNÁR L.: Az erdőtüzek oltásának logisztikai problémái valós példák alapján BOLYAI SZEMLE XXIV: (4) (2015) 86-99. o.

http://archiv.uni-nke.hu/uploads/media_items/bolyai-szemle-2015-04.original.pdf (letöltve: 2018.04.09.)

[14] RESTÁS Á.: A tűzoltásvezetők döntései – elméleti szempontból; Védelem - Katasztrófa- Tűz- és Polgári Védelmi Szemle 20:(3) (2013) 5-10. o. ISSN 1218-2958 http://www.vedelem.hu/letoltes/ujsag/v201303.pdf (letöltve: 2018.03.17.)

[15] BODNÁR L., DEBRECENI P., PELLÉRDI R.: Az erdőtűz kockázatának csökkentési lehetőségei Magyarországon. Védelem Tudomány Katasztrófavédelmi online tudományos folyóirat 2:(2) (2017) 1-11. o.http://www.vedelemtudomany.hu/articles/01-debreceni-bodnar-pellerdi.pdf (letöltve: 2018.04.09.)

[16] RESTÁS Á.: A tűzoltásvezetők döntéseinek modellezése és működése a gyakorlatban, Védelem - Katasztrófa- Tűz- és Polgári Védelmi Szemle 20: (4) (2013) 9-12. o. http://www.vedelem.hu/letoltes/ujsag/v201304.pdf (letöltve: 2018.04.09.)

[17] MARTIN Z., ANDREA M., IVETA M., PÁNTYA P.: The Proposal of Methodology to Investigate the Passenger Cars Fires Bolyai Szemle 26:(2) (2017) 45-56. o. https://www.uni-nke.hu/document/uni-nke-hu/Bolyai_Szemle_2017_02_kesz.pdf#page=45 (letöltve: 2018.04.09.)

[18] PÁNTYA P.: Eredmények a tűzoltók beavatkozói készségének növelésében Bolyai Szemle XXIV:(4) (2015) 172-180. o. http://archiv.uni-nke.hu/uploads/media_items/bolyai-szemle-2016-04.original.pdf#page=172 (letöltve: 2018.04.11.)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

KEVERŐK ALKALMAZÁSA A BIOLÓGIAI SZENNYVÍZTISZTÍTÁSBAN

USE OF MIXERS IN BIOLOGICAL SEWAGE TREATMENT

PAPP Tamás

(ORCID: 0000-0001-5574-8508)

papp.tamas@uni-nke.hu

Absztrakt

A keverők alkalmazása a szennyvízkezelésben elengedhetetlen a lebegő biomassza homogenizálásához. Anaerob vagy anoxikus reaktorokban nincs levegőztetés, ezért keverőket kell alkalmazni. A keverés teljesítménye a keverő geometriáján, a forgási sebességen, az elhelyezésén és a folyadék tulajdonságain, például a sűrűségen és viszkozitáson alapul. A keverési hatékonyság értékeléséhez általában helyszíni méréseket végzünk (például nyomjelző vagy gyorsasági mező), amely erőforrás igényes lehet. A numerikus számítások hatékony eszköz lehetnek a megbízható költséghatékony megoldások megszerzéséhez, és különböző szimulációs alternatívákat lehet összehasonlítani. Ebben a kutatásban két lapátkeverővel ellátott anoxikus tartályt vizsgáltam a keverők eltérő fordulatszámaival. A keverők az edény aljától 1 és 2 lapátátmérőnyi távolságra helyeztem el. Az eredmény az volt, hogy a legalacsonyabb forgási sebességű keverő nem biztosított elegendő keverést, a nagy forgási sebességű nagy sebességeket okozott, amelyek lebonthatják a flokkokat és alacsonyabb tartózkodási időt eredményezhetnek.

Kulcsszavak: *keverő, szennyvíz, folyadék, anaerob, anoxikus, áramlás, fordulatszám*

Abstract

Application of mixers in wastewater treatment is essential to homogenise the suspended biomass. In anaerobic or anoxic reactors there is no aeration, thus mixers should be applied. Performance of mixing is based on the mixer geometry, rotational speed, the location and fluid properties such as density and viscosity. For evaluation of the mixing efficiency, generally field measurements are performed (e.g. tracer study or velocity field) which can be resource demanding. Numerical calculations could be an effective tool to gain reliable cost-effective solutions and various simulation alternatives can be compared. In this research an anoxic tank with two mixers were examined at different rotational speed of the mixers. In this research I examined anoxic reservoir with two mixer mixers with different speeds of mixers. The mixers were placed at a distance of 1 and 2 scaffolds from the bottom of the bowl. The outcome was that the scenario with the lowest rotational speed did not provided sufficient mixing, the high rotational speed caused high velocities which may break down the flocs and results lower residence time.

Keywords: *mixers, wastewater, fluid, anaeribic, anoxic, flow, simulations, rotation speed,*

A kézirat benyújtásának dátuma (Date of the submission): 2018.06.03.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.16.

BEVEZETÉS

Napjainkban egyre nagyobb hangsúlyt kell fektetni a szennyvíztisztításra, mert rohamosan csökken az édesvíz készletünk, amelyben nagy szerepet játszik, hogy a felhasználásra kerülő tiszta víz 80%-át mindenféle tisztítás nélkül szennyvízként visszaengedjük a természetbe, ez nagy pocsékolás, és a környezetünket is szennyezzük vele. A WHO (Egészségügyi Világszervezet) egy tanulmánya szerint egyetlen csésze kávé előállításához 140 liternyi vízre van szükség, 1 kg marhahúséhoz pedig 16 ezer literre. [1]

Számunkra természetes, hogy ha kinyitjuk a csapot, mindig tiszta és egészséges ivóvíz folyik rajta. De sajnos számos olyan ország is található, ahol a lakosság édesvíz igény meghaladja a rendelkezésre álló vízkészletet. Ezen országok népessége az ezredfordulón 2,5 milliárd volt, amely a kutatások szerint 2025-re 3 milliárdra emelkedhet. Az Éghajlatváltozási Kormányközi Testület (IPCC) előrejelzése szerint 2080-ra 2,3 milliárdan nem jutnak majd ivóvízhez, 2020-ra 75-250 millió afrikai szenved majd vízhiányban. Nemsokára eljön az időszak, amikor a legnagyobb harc nem az olajért vagy az aranyért folyik, hanem a tiszta és egészséges ivóvízért, a „kék aranyáért”. [1]

Azt már korán megtanultuk, hogy a Föld vízkészleteinek csupán 2,7%-a édesvíz, aminek ráadásul 77%-a jéghegyekbe és gleccserekbe fagyva található. Ez a kevés készletet is, amellyel gazdálkodnunk kell, rengeteg veszélynek van kitéve. Ezen veszélyek nagy többségét mi emberek idézzük elő. A népesség gyarapodásával, az ipar tevékenységével és a mezőgazdasági öntözés növekedésével egyre nő a víz iránti igény. Globálisan a vízfogyasztás 80%-áért a mezőgazdaság felelős. Ugyanakkor világszerte csökkennek az elérhető készletek. Több mint harminc ország szenved vízhiányban, és a kereslet kielégítése érdekében egyre növekszik a felszín alatti víz kitermelése is. [2] Ha az emberiség az értékes vízkészletek kiaknázását utánpótlás vagy visszatöltődés nélkül folytatja, a vízválság egyre súlyosbodni fog. A folyóvizek folyamatos utánpótlást biztosítanak, ezek a vizek azonban erőteljesen szennyezettek is lehetnek, mivel a társadalom által termelt szennyvizek 80%-a jut vissza kezeletlenül a természetbe. Ennyi víz megy veszendőbe, és ami rosszabb, hogy a környezetet is szennyezi. Jelenleg 663 millió ember szenved vízhiányban a Földön, ebből 1,8 millióan szennyvizet fogyasztanak ivóvíz helyett. Ezek a hatalmas, és elkeserítő számok indokolják a szennyvíztisztítás fontosságát. [3]

Szennyezésből származó károk:

- Közvetlen:
  - Felhasználásuk korlátozott
  - Felhasználása költséges
- Közvetett:
  - Hatással van a környezetre, és a vízi élővilágra
  - Egészségügyi károkat okoz
  - Sportolási, vízparti pihenések lehetőségének csökkentése [4]

Megfelelő kezeléssel, újra tiszta kezelt vizet lehet előállítani, melyhez lebegő biomasszát alkalmazunk, a biomassza alkotója olyan mikroorganizmus csoport, mely képes szennyvízben található, szerves anyag, tápanyag lebontására. Reaktortérben ez a biomassza lebegő állapotban van, kitölti a teljes reaktor térfogatot, kihasználva a teljes medence kapacitást.

Mindenképp indokolt tehát, hogy a szerves mikroszennyezők esetében a terjedést minél pontosabban lehessen számítani, hogy a kockázatbecslésnél elkerülhessük az olyan túlzásokat, amelyek az ivóvízminőség javító program során korábban már előfordultak.

A hazai viszonyok kapcsán ki kell még emelni a hálózatok túlméretezettségéből és a vízigények csökkenéséből származó magas vízkort, amely elsősorban a fertőtlenítési melléktermékek keletkezésnek kedvez az elosztórendszerben. Ez körülmény kombinálva a

tisztítási technológiák felújítása során nagy számban alkalmazott töresponti klórozással előrevetíti, hogy a fertőtlenítési melléktermékek hálózatban való terjedését szükséges lesz tanulmányozni. Ez nem csak a kockázatbecslés érdekében, hanem a napi üzemeltetés fejlesztéshez is − melynek a klóradagolás meghatározó eleme − szükséges lesz. [2] Ennek a kutatásnak az első lépése maguknak a fertőtlenítőszereknek, jelen esetben a leggyakrabban alkalmazott aktív klórformák terjedésének vizsgálata. Ezen ismeretek birtokában válik majd lehetségessé a mikroszennyezőkkel kapcsolatos vízminőségi modellezés. A klór átalakulásnak leírására rendelkezésre álló összefüggések után egy vízelosztó hálózat hitelesített hidraulikai modelljén szemléltetésre kerül a vízminőségi modellezés érzékenysége, azaz hogy a klór átalakulását leíró paraméterek bizonytalansága milyen mértékben képes befolyásolni a végeredményt.

A biomassza lebegésben tartásához is mechanikus keverőket alkalmazunk (levegőztetett medencékben a levegő áram keltette vízmozgás is segít). A tisztítási folyamatok egy része igényli, a külső oxigén bevitelét (pl. nitrifikáció), azonban léteznek olyan folyamatok melyhez kémiailag kötött oxigént alkalmazunk, vagyis külső levegőztetésre nincsen szükség, ilyen például a denitrifikáció, melyhez a nitrátban lévő oxigént hasznosítja. Ez esetben, levegőztetés hiányában még nagyobb hangsúlyt kap a mechanikus keverés.

A keverés célja a kiegyenlítés, azaz az összekevert anyagok hőmérsékletének, viszkozitásának, sűrűségének eloszlása egyenletesen a kevertetett tartály teljes térfogatában. [5] A keverés hatékonyságát a keverési index %-ban mutatja. A tökéletes elegyítés értéke 100%, mely a valóságban nem elérhető. [6] De mindenképpen törekedni kell rá, mert minél jobb a kevertetés hatékonysága, annál több vegyszert, időt, és energiát spórolhatunk meg. A keverő berendezések az iparban a leggyakrabban alkalmazott műveleti egységek, de ezek a berendezések legtöbbször egy működő technológia részei, ezért kísérleti információk nehezen szerezhetők be, valamint egy modell felépítéséhez szükséges adatok összegyűjtése hosszú időbe telik. Megoldást jelenthetnek a félüzemi kísérletek, de ezekben az esetekben a méretnövelés jelenthet problémát, ugyanis ez jelentősen befolyásolhatja a berendezésben kialakuló áramlási képet. A méretnövelés már egy külön tudományággá nőtte ki magát. Kezdetben a dimenziómentes számok rendszerén keresztül bonyolult módon történtek a számítások, ma azonban széles körben alkalmazható tervezőprogramok állnak rendelkezésre ezen a tudományterületen is. [7] Így a keverők teljesítményszükséglete a hasonlóságelmélet segítségével, pontosabban a dimenzióanalízis alkalmazásával általánosan is leírható. Tapasztalatok szerint a keverő teljesítményszükséglete a keverő és a tartály méreteitől, a keverő fordulatszámától, a kevert folyadék sűrűségétől és viszkozitásától függ. Ha a keverőtartályban folyadéktölcsér keletkezik, akkor még a nehézségi erő is befolyásolja. [8]

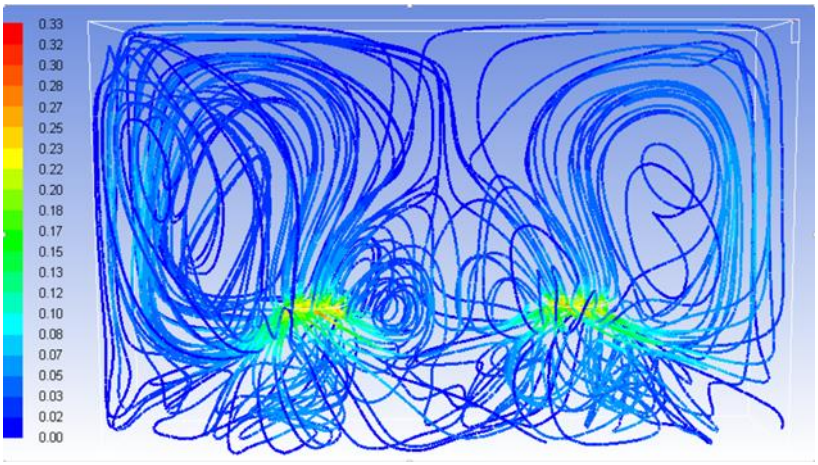
ANYAG ÉS MÓDSZER

A numerikus számítások hatékony eszközök lehetnek a megbízható költséghatékony megoldások megszerzéséhez, és különböző szimulációs alternatívákat lehet összehasonlítani. Ezen programok fejlesztésénél a legfontosabb ösztönző az volt, hogy nemzeti problémák megoldására is fel lehessen használni. [9] Ebben a kutatásban két keverővel ellátott anoxikus tartályt vizsgáltam a keverők eltérő fordulatszámaival. A kísérletet az Ansys nevű szimulációs programmal végeztem el, hatáskeresztmetszet modellel, melybe nyomásnövekedést és perdület változás megadható az áramlási tér valamely felületére, így könnyebben modellezhető az áramlástani gépek pl. a keverők körül kialakuló sebességmegoszlás. [10] A vizsgálandó térben a program rácspontokat vesz fel, és a rácspontok elmozdulásából számolja ki a kevert folyadék sebességét, és irányát. Minél sűrűbben helyezkednek el a rácspontok annál pontosabb eredményt kapunk. [11] A nagy örvényes szimuláció (LES) teszi lehetővé, hogy minden nagy léptékű turbulens örvényt kiszámoljunk, és csak kis turbulens örvényeket alakítunk ki alrácsmodell segítségével. [12]

A hipotézisem, hogy minél nagyobb keverési intenzitást alkalmazunk, egyre jobb áramképet kapunk, egyre kisebb holt térrel, úgy hogy a kívánt tartózkodási idő elegendő a denitrifikáció végbemeneteléhez, mely 2 maximum 3 óra. Tehát a keverőlapátok forgási sebességének növelésével a biomassza kevertetése hatékonyabb lesz.

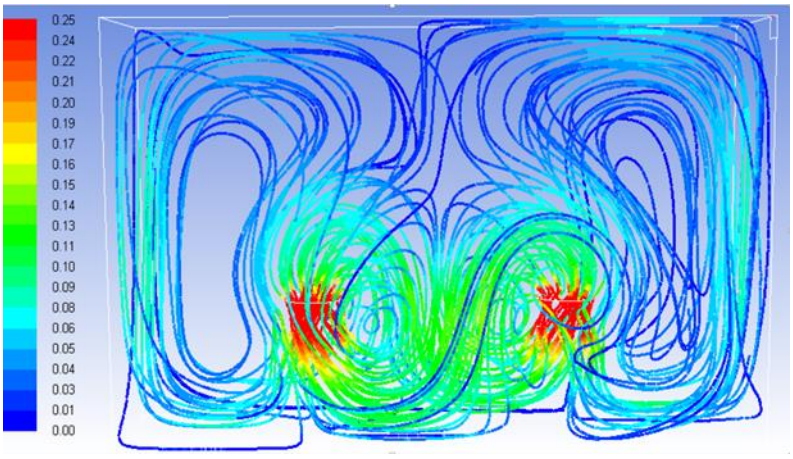
Szimuláció 2 lapátátmérőnyi távolsággal

Az kiindulási modellnél a keverők fordulatszáma 100 1/min. A 1. ábra az áramvonalak sebességét, sűrűséget és stagnáló zónákat mutatja. Az áramvonalak először felfelé, majd lefelé indulnak, ez egy függőleges keverési minta, ami meglehetősen zavaros. Ennél a fordulatszámnál, a teljes elkeveredéshez túl sok időre van szükség, tartályban a tartózkodási idő meghaladta a maximális 3 órát.



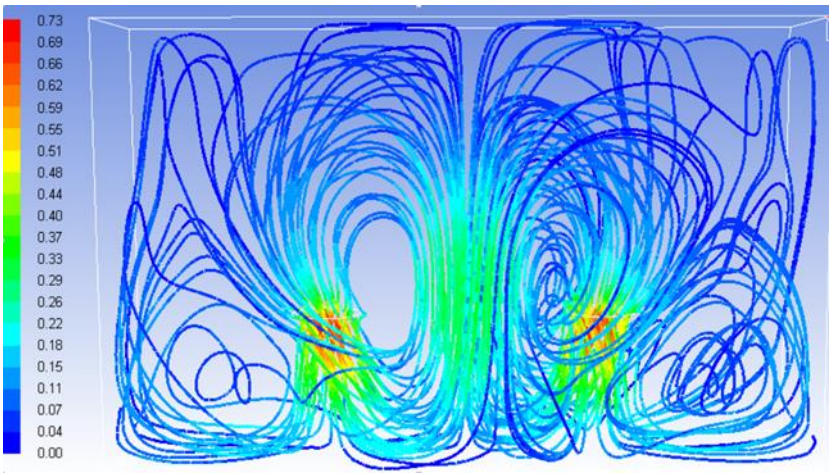
1.ábra Áramvonalak sebességi ábrája 100 1/min-nél (saját szerkesztés)

A második szimulációnál a keverők sebessége 400 1/min. A 2. ábrán jól látható, hogy a sebesség nem csökken le nemkívánatos mértékben a fal mellett sem, jól megfigyelhető, hogy kisebbek lettek a pangó zónák, és az áramvonalak is szabályosabbak lettek. A fokozott fordulatszám lecsökkentette a tartózkodási időt a kívánt időintervallumra.



2.ábra Áramvonalak sebességi ábrája 400 1/min-nél (saját szerkesztés)

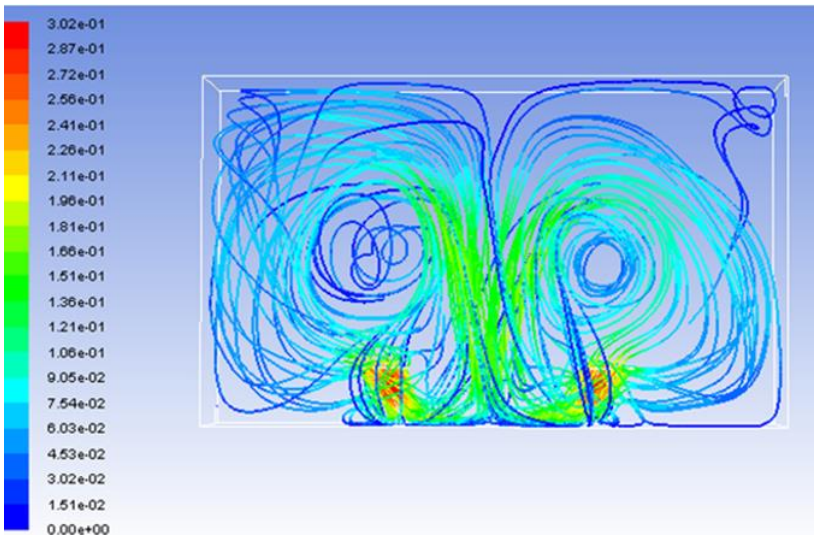
A harmadik szimulációnál a keverők sebessége 900 1/min. A 3. ábrán megfigyelhetjük, hogy az áramvonalak iránya már nem szabályos, és a nagy sebesség miatt a pangó zónák mértéke is növekszik, és a két keverő már összedolgozik. A folyadék tartózkodási ideje a nemkívánatos szint alá csökkent.



3.ábra Áramvonalak sebességi ábrája 900 1/min-nél (saját szerkesztés)

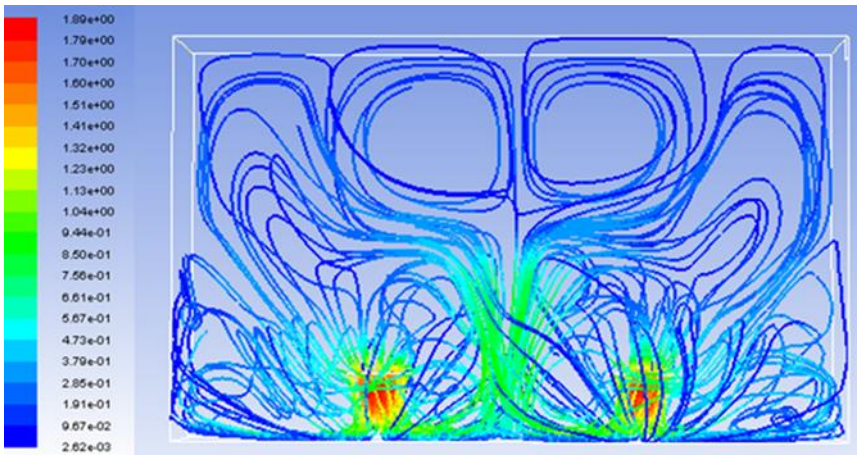
Szimuláció 1 lapátátmérőnyi távolsággal

A negyedik szimulációnál, már 1 lapátátmérőnyi a keverő, és az edény alja közötti távolság. Keverőlapátok forgási sebessége 100 1/min. Az 4. ábrán jól megfigyelhető, hogy az áramvonalak szabályosabbak, mint az 1. ábrán, de a holtterek mérete lényegesen nagyobb.



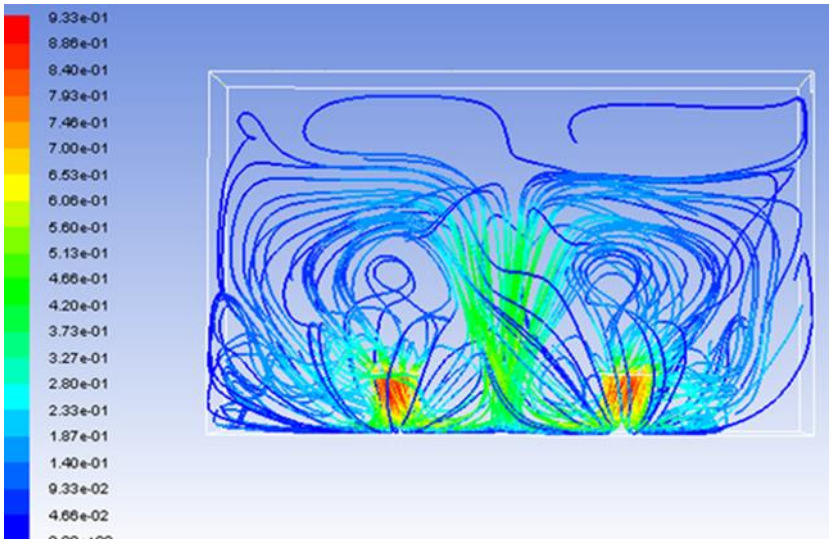
4. ábra Áramvonalak sebességi ábrája 100 1/min-nél (saját szerkesztés)

Az ötödik szimuláció során a keverők sebessége 400 1/min. Ebben az esetben az áramvonalak jelentősen szabálytalanabbak (5. ábra), mint a 2. ábrán látható, és a sebesség is lecsökken, ezért a tartály felső részében a folyadékon nem keveri át a megfelelő mértékben.



5. ábra Áramvonalak sebességi ábrája 400 1/min-nél (saját szerkesztés)

A hatodik szimuláció esetében a fordulatszám 900 1/min (6.ábra). A fokozott fordulatszámnak köszönhetően, a kiinduló sebesség megfelelőnek tűnik, de mivel az edény alja meglehetősen közel van a keverőlapátokhoz, ezért az áramlás iránya túl merőlegesen érkezik, és jelentős mértékben lelassul. Az alacsony sebesség miatt, megnövekedett a tartály felső részén az át nem kevert folyadék mennyisége.



6. ábra Áramvonalak sebességi ábrája 900 1/min-nél (saját szerkesztés)

KÖVETKEZTETÉSEK

Az első sorozat eredménye, hogy a legalacsonyabb forgási sebességű keverő nem biztosított elegendő keverést, a nagy forgási sebességű nagy sebességeket okozott, amelyek lebonthatják a flokkokat, és alacsonyabb tartózkodási időt eredményezhetnek. Az eredmények azt mutatták, hogy optimális művelet érhető el az áramlási szimulációk alkalmazásával. Ezért a hipotézisemet elvetettem, mert a számítások nem azt igazolták. Ez alapján módosítom a kiindulási állításomat: a keverési hatékonyság, nem lineáris a keverő teljesítményével.

A második sorozatnál a legalacsonyabb fordulatszámú keverés bizonyult a legmegfelelőbbnek, annak ellenére, hogy a pangó zónák méretei nem ebben az esetben voltak a legkisebbek, de az áramvonalak itt a legszabályosabbak, és a keverő lapátok sem dolgoznak egymás ellen, ezért kevesebb az energiafelhasználás is.

ÖSSZEGZÉS

A számszerű adatokat a szimulációból kaptam (1.táblázat), melyekből arra lehet következtetni, hogy a keverő magasság megfelezésével, hiába értem el nagyjából kétszeres folyadék átlagsebességet, mégsem tudja kellő képpen átkeverni, mert túl merőlegesen érkezik a tartály aljára a folyadék, ami miatt lelassul, és túl magas a keverők feletti vízoszlop. A második szimuláció bizonyult a leghatékonyabbnak, ebben az esetben legszabályosabbak az áramvonalak, az áramlás sebessége sem lassul le nemkívánatos módon, és energiafelhasználás szemszögéből is megfelelőnek tűnik, mert ebben az esetben a keverőlapátok nem dolgoznak egymás ellen.

Keverők sebessége (1/min)	2 keverőnyi magassággal a kevert folyadék átlagsebessége (m/s)	1 keverőnyi magassággal a kevert folyadék átlagsebessége (m/s)
100	0,037	0,07
400	0,054	0,14
900	0,109	0,28

1.táblázat Különböző forgási sebességekhez, és keverőmagasságokhoz tartozó adatok (saját szerkesztés)

FELHASZNÁLT IRODALOM

[1] PAPP T: *Parti szűrés és reverze osmosis szűrés elméleti, és gyakorlati oktatása.* Dunaújváros 2016.

[2] KÁRMÁN K: A parti szűrésű vízbázisok és jelentőségük. *Magyar tudomány* 174.11. (2013) 1300. oldaltól-1301. oldalig.

[3] SZABÓ E.: *Szennyvizet ivóvíznek?*, 2017. www.gasztrohos.blog.hu/2017/03/22/szennyvizet_ivoziznek A (letöltés ideje: 2017.10.02.)

[4] BEREK T., DÉNES K.: *Vízbázisok védelme, különös tekintettel a katonai táborok vízellátására*. 2015. Műszaki Katonai Közlöny XXV: (1) pp. 121-130.

[5] VARGA I.: *Keverés.* 2014. www.slideplayer.hu/slide/2133443/ (A letöltés ideje: 2017. 09. 14.)

[6] BÁRÁNY ZS. B.: *A keverés.* 2014. www.bzsb.hu/aloldalak/oktatasi-anyagok/Automatika/Keveres.pdf (A letöltés ideje: 2017.09.15.)

[7] EDEGY A.: *Vegyipari berendezések áramlástechnikai vizsgálata, CFD szimulációs példák kidolgozása.* 2011, www.pr.mk.uni-pannon.hu/disszeminacio/keveres.html#alkalmaz (A letöltés ideje: 2017.09.31.)

[8] FONYÓ ZS. FÁBRY GY.: *Vegyipari művelettani alapismeretek*. Digitális Tankönyvtár, 2011, www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_519_44580_Vegyipari_Muveletten/ch02s05.html (A letöltés ideje: 2017.09.19.)

[9] BRACKBILL J. U. .: *Introduction to Harlow's scientific memoir.* 2003. www3.nd.edu/~gtryggva/CFD-Course/JCP-Harlow-2004.pdf (A letöltés ideje: 2017. 10.03.)

[10] KRISTÓF G.: *Áramlások numerikus modellezése*, Budapest: BME Áramlástan Tanszék, 2011, www.ara.bme.hu/~kristof/CFDjegyzet/ (A letöltés ideje: 2017.10.01.)

[11] BAKKER A.: *Applied Computational Fluid Dynamics.* Canonsburg: ANSYS, 2002. www.bakker.org/dartmouth06/engs150/07-mesh.pdf (A letöltés ideje: 2017.09.26.)

[12] BAKKER. A.: *Large Eddy Simulation.* 2000. www.bakker.org/cfm/webdoc16.htm (A letöltés ideje: 2017.09.27)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

A TELEPÜLÉSEK VÍZGAZDÁLKODÁSI HELYZETÉNEK HATÁSA A BELVÍZI VÍZKÁRRAL SZEMBENI ÉRZÉKENYSÉGRE

THE EFFECTS OF THE WATER MANAGEMENT SITUATION ON THE SENSITIVITY OF THE INLAND WATER HARVEST IN THE CITIES

(A CIKK DOI azonosítója)

PRIVÁCZKINÉ HAJDU Zsuzsanna

(ORCID: 0000-0002-8599-1215)

prizsuzsa@gmail.com

Absztrakt

A klímaváltozással együtt járó szélsőséges vízgazdálkodási helyzetek erősödése a települési vízgazdálkodásban is szemlélet-váltást sürget. Az Alsó-Tisza-vidéki Vízügyi Igazgatóság (ATIVIZIG) működési területén tapasztalható, hogy a belterületeken a burkolt felületek ugrásszerűen megnőttek, a mélyfekvésű területek beépülnek, ezzel növelve a település belvízi kitettségét. A szakirodalmi kutatások és az igazgatóság adatainak elemzésével kimutatható, hogy az antropogén hatások, a víziközművek fejlődése milyen tendenciákat mutat és ez milyen hatást gyakorol a települések belvízhelyzetére. A globális klímaváltozás a Dél-Alföld vonatkozásában az aszályveszély erősödését vetíti előre. A szennyvíz és csapadékvíz-hálózatok „elvezetés-központú" kiépítésével a települések alatti terület vízhiányos időszakban fokozottan vízhiányban fog szenvedni, egyidejűleg a külterület-belterület határán a csúcsidejű vizek befogadása miatt fokozott belvízi helyzet kialakulása várható. A települési vízgazdálkodásban a komplex szemléletű megoldások, valamint a csapadékvíz-gazdálkodás megvalósítása egyéni és önkormányzati szinten is szükségszerűvé válik.

Kulcsszavak: *települési csapadékvíz-gazdálkodás, antropogén hatás, belvíz veszélyeztetettség*

Abstract

The strengthening of extreme water management situations associated with climate change also calls for a change of attitude in municipal water management. In the area responsibility of ATIVIZIG the paved surfaces in the settlements have been increased, deep-seated areas are become built-in, thus increasing the inland excess water threat of the settlements. By studying the literature and analyzing available data of ATIVIZIG it is possible to show the trends of the anthropogenic impacts, as example the development of the water utility works and their impact on the inland excess water situation in the settlements. Global climate change is predicting growth of the drought risk in the South Great Plain. By establishing a "drain-centered" water networks, the ground under the settlements will suffer from a water scarcity in water deficiency period. Simultaneously there is expected an increased worse situation of inland excess water where peak waters from downtown are led into the regional water-systems and capacity problems occurs.

The implementation of complex approaches gets important in urban water management and the rainwater management becomes necessary at individual and municipal level.

Keywords: *water-management in settlements, anthropogenic effects, inland excess water hazard*

A kézirat benyújtásának dátuma (Date of the submission): 2018.04.05.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.29.

BEVEZETÉS

Magyarország földrajzi helyzete miatt vízkároknak kitett, mivel a Kárpát-medence sajátos vízrajzi helyzettel bír. [1: 417–419. o.] Területén a szélsőséges időjárás gyakran okoz vízbő időszakokban árvizet, belvizet, csapadékhiányos időszakban aszályt is, amelyek évről évre jelentős kárt okoznak nemzetgazdasági szinten is. Ezen okok miatt a vízkárok elleni védekezés hazánkban történelmi távlatokra tekint vissza. Az állami szerepvállalás jelentős, jogrendszerünk több száz éves múltra tekint vissza ezen a téren[1], így a védekező szervezetek nagy hagyományokkal rendelkeznek. [19]

Magyarország területének 55 %-a dombvidéki, 45 %-a síkvidéki terület. Hazánkban közel 3200 település van, amelyek közül mintegy 1000 síkvidéki, 2200 dombvidéki területen található. [2] A belvíz elleni védekezés a síkvidéki települések sajátossága is, amelyet a települések vonatkozásában helyi vízkárelhárításnak nevezünk, ami alapvetően a belvízi helyzetben történő beavatkozásokat és intézkedéseket jelenti. A belvíz megfogalmazására, leírására számtalan szakmai meghatározás született az elmúlt évszázadban/évtizedekben, amely pl. a károkozás volumenétől, az elöntés nagyságára, tartósságára vonatkozóan, stb. terjesztette ki a belvíz definícióját. [1] [12] A belvíz időszakos jelenség, a kis felszínesésű területeken a vízbő időszakok sajátossága, amely hidrológiai helyzet hatására alakul ki (csapadék, hőmérséklet függő); tartós, nagy kiterjedésű elöntéssel együtt járva kárt okoz külterületen és belterületen is. A belvíz a mezőgazdaság szempontjából más értelmezéssel bír, mint például a települések szempontjából: a mezőgazdasági területen a telített talaj már „belvízi elöntésnek” számít (kárt okoz), viszont a téli időszak elöntései számottevően kisebb kárt okoznak, mint a tenyészidőszakban. [1] A településeken azonban évszaktól függetlenül is nagy kárt okozhat a belvízi elöntés, vagy a megemelkedett talajvízszintből származó elöntés.

Jelen írás a Dél-Alföldi területek síkvidéki települései kapcsán foglalkozik az utóbbi évek változásainak tükrében a települések megváltozott vízgazdálkodási helyzetével, amely befolyásolja a települések belvízi kockázatát is. A körülmények ismerete különös jelentőséggel bír a várható globális klímaváltozás tükrében, amelyet a település fejlesztési irányok kapcsán fontos figyelembe venni.

Jelen cikk célja, hogy bemutassam, a belvízképződésre hatással lévő különböző tényezők hogyan változtak meg az elmúlt időszakban a települések belterületének és külterületeinek vonatkozásában. Ehhez a vonatkozó szakirodalom elemzését végeztem el, valamint konkrét elemzésekkel támasztom alá a megállapításokat, amelyek Alsó-Tisza-vidéki Vízügyi Igazgatóság (ATIVIZIG) adatbázisában fellelhető adatok, valamint a KSH[2] adatok alapján készültek: az ivóvízhálózat fejlődés és ivóvíz-fogyasztás, a szennyvízcsatorna-hálózat és szennyvíztisztítás közel egy évtizedes statisztikai adatszolgáltatásának elemzésével[3].

Célom, hogy írásommal felhívjam a szakemberek és a döntéshozók figyelmét arra, hogy a várható globális klímaváltozás tükrében mely tényezők kapcsán kell különös figyelmet fordítani a települések fejlesztése során arra, hogy a tervezők a vízgazdálkodás elemeit komplex módon vizsgálva tervezzenek és mérlegeljenek, a belvíz kialakulását a megvalósuló fejleszté-

[1] A vizekkel kapcsolatos *rendszerezett* jogalkotásra elsőként a kiegyezést követően találunk példát; konkrétan a vízjogról [sic!] szóló 1885. évi XXIII. törvénycikket. A terület szabályozásának előzményei már az 1807, 1836-os törvényi rendelkezésekben is fellelhető. [19]

[2] KSH: Központi Statisztikai Hivatal

[3] A vizsgálatot a KSH 2000-2016 időszak adataira, az ATIVIZIG-nél digitális települési adatsoros adatbázisban fellelhető 2005-2016 időszakra végeztem el, amikortól a statisztikai adatgyűjtések évi gyakorisággal elérhetőek.

sekkel ne elősegítsék, hanem okszerű intézkedésekkel és beavatkozásokkal a belvízveszélyt csökkentsék.

A BELVÍZ KIALAKULÁSÁT BEFOLYÁSOLÓ TÉNYEZŐK

A belvíz kialakulását *természeti* és *antropogén*[4] hatások okozzák. A belvíz kialakulása bonyolult folyamat, leginkább a helyi viszonyok vannak rá hatással. Kölcsönhatásaik révén szükséges vizsgálnunk a kialakulására hatással lévő különböző tényezőket.

A természetes adottságokat tekintve két nagyobb csoportot határozhatunk meg: [1: 85–87 o.]

- a meteorológiai viszonyok,
- a vízgyűjtő terület adottságai.

A *meteorológiai* viszonyok közül legnagyobb hatása a lehullott *csapadék* nagyságának, térbeli és időbeni eloszlásának van, ideértendő a hóolvadékból keletkező lefolyást is. Ha talaj telítődik a csapadékból, akkor vízbefogadó-képessége, vagy vízelvezető-képessége kimerül, belvíz képződik. A *hőmérséklet* is alapvető fontossággal bír, a fagyott talaj úgy viselkedik, mint a vízzel telített talaj, nem tudja a vizet befogadni. A hirtelen hóolvadás is belvizet okoz, de a magasabb hőmérsékletnek a párolgás révén jelentős a belvíz-csökkentő hatása.

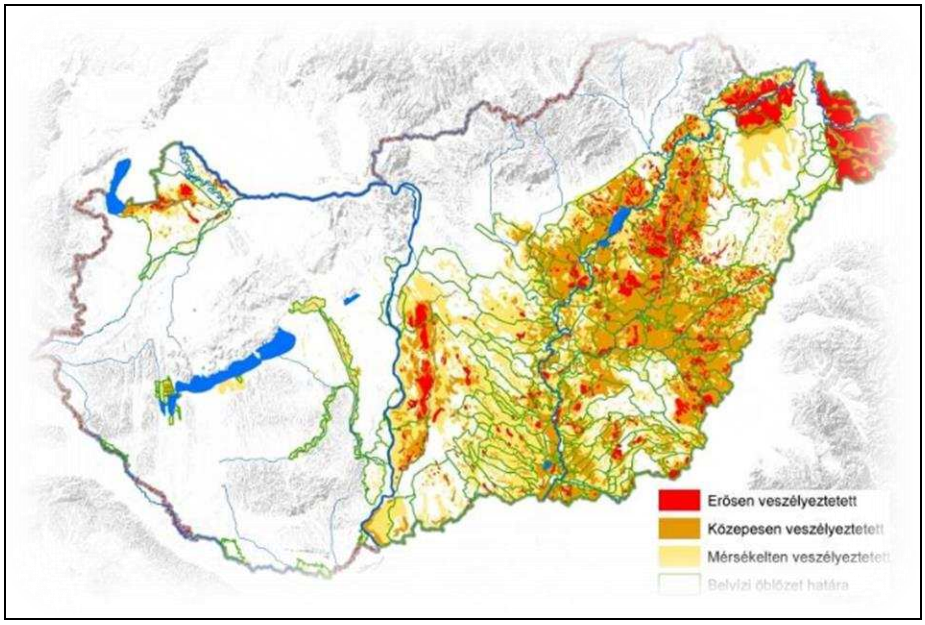
A vízgyűjtő terület jellemzői közül talán a legfontosabb kiemelnünk *domborzati* viszonyokat. A kis terepesés, ami az alföldi területeket jellemzi, ideális a belvízképződésre. A mikro-domborzat a belvíz kialakulását, a makro-domborzat a belvíz lefolyását és elvezetését befolyásolja. A *talaj-adottságok* kapcsán elsősorban a talaj kötöttsége (vízgazdálkodási tulajdonságai) és vastagsága (tározótérfogat) alapvető fontosságú a belvízképződésben. A laza, homokos talajok jobban vízáteresztők, mint a kötött agyagtalajok, belvízképződésre kevésbé érzékenyek. A *talajvíz* helyzete jelentős hatással van a belvízképződésre, ha magas, akkor a talaj telítettsége miatt a lehulló csapadékvíz nem tud a mélyebb rétegek felé leszivárogni, belvíz keletkezik. A vízgyűjtőterület nagysága és alakzata is befolyásolja a belvízképződést. A nagyobb területekről nagyobb belvízhozammal kell számolnunk, a hosszanti elnyúló vízgyűjtőkről az összegyülekezési idő hosszabb, így fajlagosan kisebb vízhozam éri el a befogadót, mint a kisebb vízgyűjtőkön. [1]

Az emberi tevékenység hatására mára megváltozott az alföldi sík tájak vízgazdálkodása: mezőgazdaságilag művelt területek, burkolattal ellátott területek, települések, utak, vízrendezési művek, csatornák, szivattyútelepek létesültek, a melioráció segítségével vízjárta területeket csapoltak le, megváltozott a táj arculata. Az antropogén hatások közül elsősorban a talajhasználatot említem meg, amely több szempontból is hatással van a belvízképződési folyamatokra. [20] A mezőgazdasági talajművelés, az agrotechnika, a talaj víztározó-képességére és vízelvezető-képességére van hatással, a szakszerűtlen talajműveléssel a kötöttebb talajok esetén kialakuló eketalp réteg meggátolja a vizek mélyebb rétegek felé történő beszivárgását, ezzel elősegíti a belvizek kialakulását. Az egyes művelési ágak is befolyásolják a belvízképződést: az erdők csökkentő hatással bírnak, a növényzettel nem benőtt területek elősegítik a belvízképződést. A növényzet a párologtatás révén nagyban hozzájárul a belvizek csökkentéséhez. A burkolt területek meggátolják a talajba történő beszivárgást, ezért elősegítik a belvíztömeg növekedését, ezzel a belvízképződésben is negatív hatással bírhatnak. Az öntözött területeken nagyobb a belvízképződés kockázata a folyamatos vízzel telített talajréteg miatt. [3] A települések vízhasználata a nem csatornázott területeken talajvíz dombok kialakulásához vezetett.

[4] emberi tevékenység által okozott

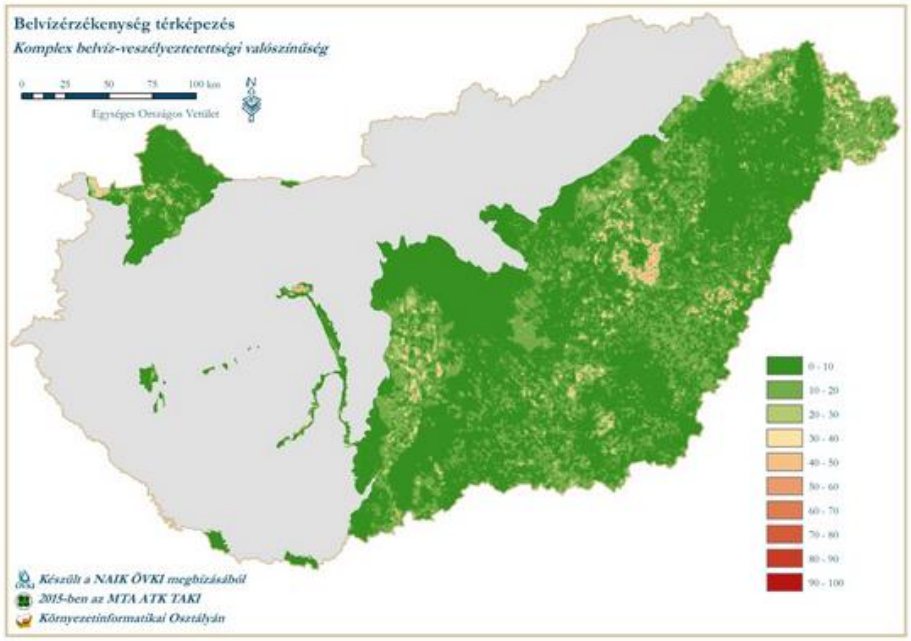
A TERÜLET BELVÍZ-VESZÉLYEZTETETTSÉGE

Egy-egy terület belvíz-veszélyeztetettségének meghatározása, majd a térképi ábrázolása, elsősorban a természeti adottságok és az addigi elöntések gyakoriságát feldolgozva készül el. A belvízgyakoriság elemzésével a gyakori elöntések okait elemezve feltárhatjuk annak előző fejezetben taglalt okokat. [3] A veszélyeztetettség térképi megjelenítésével bemutatható Magyarország belvíz-veszélyeztetettsége, amely hazánk közel 60 %-át érinti, a síkvidéki területeket. Ennek a térképnek máig használatos formáját Pálfai és társai dolgoztak ki és tettek közzé 2002-ben. [1: 145–151] Egy-egy területet adottságai alapján (természeti adottságok és a belvízgyakoriság alapján) 1–4 osztályba soroltak be a belvíz-veszélyeztetettség alapján: alig, mérsékelten, közepesen és erősen veszélyeztetett területeket határoltak le. Az akkori technikai színvonal lehetősége természetesen egészen más, mint a mai korszerű, térinformatikai rendszerek által nyújtott lehetőségek. A belvíz-veszélyeztetettségi térkép az alföldi sík területekre értelmezhető, ezt mutatom be az 1. ábrán.



1. ábra: *Magyarország síkterületeinek Pálfai-féle belvíz-veszélyeztetettsége* [1: 1. melléklet]

A belvíz-veszélyeztetettség térképi meghatározásában a számítástechnikai fejlődés, valamint a Víz-keretirányelv és kapcsolódó Árvízi kockázati térképezési EU-irányelv végrehajtása adott nagy lökést a 2002. évet követően. [2] Az átdolgozott Komplex Belvíz-veszélyeztetettségi térkép három kategóriát különböztet meg Magyarországon: átlagos, fokozott és nagyfokú veszélyeztetettséget. A térkép 2015-ben készült el Magyarország vonatkozásában. A két féle belvíz-veszélyeztetettségi térkép háttérmunkálatainak és eltérő ábrázolásának összehasonlítását jelen cikkben helyhiány miatt nem tárgyalom, ez egy következő írás témája lehet.



***2. ábra**: Magyarország belvízérzékenység térképe.* [5]

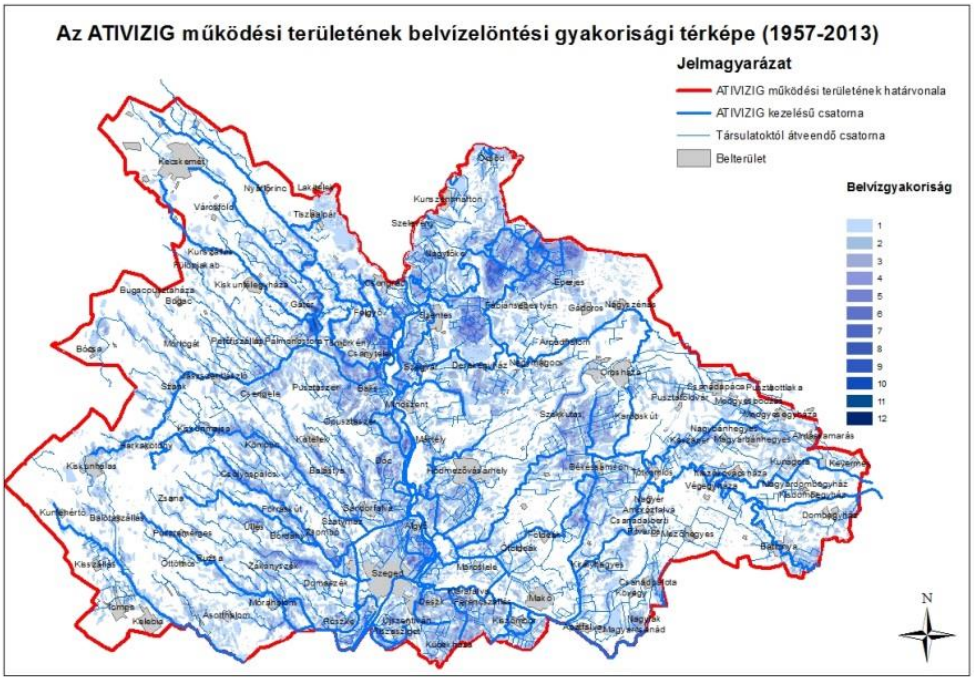
A kutatók kisebb léptékben számos területen foglalkoztak egy-egy terület kapcsán a belvíz-veszélyeztetettség árnyaltabb (több tényező figyelembevétele, térinformatikai elemzések stb.) kimunkálásával, ezen publikációk és szakirodalom bőségesen fellelhető szakirodalmi és az internetes szakirodalomban publikált forrásokban. [6] [20]

A belvíz-veszélyezettség térképezéshez és a belvíz-képződés jelenségének jobb megértéséhez, kutatásához kínál remek lehetőséget a SANITEL–2 műhold által készített felvételek elemzése és térinformatikai rendszerekkel történő összekapcsolása, amely kutatás most indul a vízügyi ágazatban. Ez várhatóan lehetőséget ad majd arra vonatkozóan is, hogy a több évtizeden át a vízügyi szolgálat által empirikus úton gyűjtött elöntési adatok helyett valóságos, mért elöntési adatok álljanak rendelkezésre a kutatók és szakemberek számára. Ez egyúttal lehetőséget adhat a belvíz-képződés és belvíz-mentesítés időbeni lefolyásának megfigyelésére is. [7]

A belvíz-veszélyeztetettségi térképek a *települések belterületének vonatkozásában nem értelmezhetők*, a belterületek vonatkozásában az antropogén hatás olyan jelentős, hogy a belvízképződés általános, területi megállapításai nem használhatóak! A települések kapcsán, mint az azokat körül ölelő természeti környezet veszélyeztetettsége, természetesen szerepet játszik, de mint olyan sokszor bebizonyosodott a korábbi védelmi helyzetekben, egy-egy rosszul kivitelezett kapubejáró, betemetett csatornaszakasz egész utcák elöntését okozhatja még akkor is, ha nincs kiterjedt belvízhelyzet a vízgyűjtőn.

Az ATIVIZIG a 12 vízügyi igazgatóság közül a Dél-Alföldi területeken látja el a magyar állam nevében a vízgazdálkodási feladatokat, amelynek része a vízgazdálkodás, az ár- és belvízvédelem is. Működési területe lefedi Bács-Kiskun megye K-i és Békés megye Ny-i felét, Csongrád megye teljes egészét, valamint Jász-Nagykun-Szolnok megyéből Öcsöd és Kunszentmárton településeket. Összesen 114 település tartozik a területhez. Ezen települések víziközmű-fejlődésének elemzése készült el.

A működési terület térképi megjelenítését és a jellemző belvízgyakoriságot [18] az alábbi ábrán mutatom be.



***3. ábra**: Az ATIVIZIG működési területe és a belvízgyakoriság* [18]

A GLOBÁLIS KLÍMAVÁLTOZÁS HATÁSA A BELVÍZKÉPZŐDÉSRE

A globális klímaváltozás belvízképződésre várható hatását a következtetések kapcsán feltétlenül vizsgálnunk kell.

Hazánkban az átlagos éves csapadék 600–650 mm, de szélsőséges időjárás körülmények között akár 203 mm is lehet (Szeged, 2000-ben), de 2010-ben egy rendkívüli csapadékos időszakban 1000–1200 mm volt az átlag csapadék. A Dél-Alföldön az országos átlagnál némileg kisebb, 500–550 mm a sokéves átlag csapadék. Az aszály és árvíz mellett a terület legjelentősebb környezeti veszélye a belvíz, amely 2–4 évente okoz károkat a mezőgazdaságban, 10 évente nagy károkat is. [12] Az elöntött területek nagysága változó, ezzel együtt az okozott kár is. Az ATIVIZIG működési területén az átlagos belvizes években 20–40 ezer ha, míg a 2000-ben mért legnagyobb elöntés 108 ezer ha volt. [18]

Különös hidrológiai sajátosság, hogy a vízbő és vízhiányos időszakok egymást követő évben, vagy akár egy éven belül is megjelenhetnek, ezzel együtt a belvizek és az aszályok is egymást követő években szélsőséges mértékben is testet ölthetnek. Így történt meg pl. az 1999–2000. és a 2010–2011 esztendőkben, ahol a nagy területi elöntéssel járó belvízvédekezési időszak az ATIVIZIG működési területén gyakorlatilag egy évnél hosszabban is elhúzódott. Egyidejűleg 2000-ben és 2011-ben aszályos időszak is volt. Így 2011. márciustól kezdődően a fennsíki területek már öntöző vizet igényeltek, miközben a mélyfekvésű területeken még folyt a területek belvízmentesítése. [18]

A globális klímaváltozás várható hatásaival számos tanulmány foglalkozott, a hazánkban várható hatások kapcsán az előzetes elemzések megszülettek. [13] [15]

Az Alföldre vonatkozóan a Szegedi Tudományegyetem [12] készített különböző szcenáriókat és vizsgálta meg a globális klímaváltozás hatását az aszály, a belvíz és árvíz-veszélyekre vonatkozóan az alföldi területeken. A belvíz kapcsán az előrejelzés bizonytalanságát emelném ki, és erre a tanulmányban a szerzők is felhívták a figyelmet, hiszen a belvízképződés vonatkozásában a helyi tényezők és sajátosságok jelentősek, ezért sok bizonytalanságot hordoz. Mezősi és tsai. tanulmányának megállapításai alapján az evapotranspiráció növekedése és a fagyos napok számának növekedése a belvízképződésre csökkenő tendenciát jelent, míg

az intenzívebbé váló csapadékesemények, a nyári-tavaszi elöntések a belvízi események növekedéséhez járulhatnak hozzá. A modell eredmények alapján összességében a belvízveszély kismértékű változását jelzik előre az Alföldön. [12]

A fenti tanulmány összefoglaló megállapításai alapján az Alföldi területek vonatkozásában az éghajlati szélsőségek fokozódásával kell számolni, a belvíz továbbra is számottevő természeti veszély marad, azonban az aszály-veszély várható intenzív növekedésével kell számolnunk.

A TELEPÜLÉSEK BELVÍZHELYZETE ÉS A VÍZGAZDÁLKODÁS ELEMEINEK KAPCSOLATA

A belvízi elöntés fogalmán általában külterületi, mezőgazdasági területek elöntését értjük, s a belvíz definíciói közül egyik sem foglalkozik a belterületi elöntéssel. [1: 172] A belvízi elöntés azonban ugyanúgy veszélyezteti a belterületi ingatlanokat és a külterületeken a tanyás ingatlanokat, esetenként sokkal nagyobb károkat okozva, mint a külterületeken. Az alföldi sík területeken jellemzően a magas talajvíz miatt alakulnak ki a belterületi elöntések. Ez származhat a folyók menti településeken az árvizek alkalmával megduzzadó talajvízszint miatt, de a csapadéktevékenység, vagy hóolvadásból származóan is kialakulhat a telített talaj, amely már nem tud több vizet levezetni a mélyebb rétegek felé.

Külön említem meg a földárja[5] jelenséget, amely az alföldi területeken több ízben okozott a belterületeken is tartós, nagy kárt okozó elöntéseket, pl. Orosházán és a Maros-hordalékkúp településein 1979-ben[6] [8: 155–171].

A települések belterületi belvízi elöntés elleni védelme kapcsán helyi vízkárelhárításról beszélünk, amelynek jogszabályi háttere a felelősségi és döntési jogköre jól szabályozott. [2] [4] Azonban a jogszabályi környezet folyamatos változása miatt folyamatos alkalmazkodást kíván a védelmi szervezetek részéről, ennek tárgyalására a cikk terjedelme miatt nem ad lehetőséget.

Az alábbi elemzés mindazon szakemberek figyelmébe ajánlom, akik döntési helyzetben vannak egy-egy fejlesztés előkészítésében, engedélyezésében, vagy megvalósításában: polgármester, önkormányzati műszaki felelős, tervező, engedélyező hatóság szakembere, vízügyi igazgatóság szakembere, fejlesztési irányvonalat meghatározó szakember.

Vizsgáljuk meg a települések belvízkár-érzékenységének szempontjából a tényezőket! A legfontosabb tényező a belterületi belvíz kialakulásának szempontjából a talajvíz szintje. A településeken a földtani és domborzati adottságok alapján a térségre jellemző talajvízszintek alakulnak ki, de attól jelentősen eltérő helyzetek is kialakulhatnak az antropogén hatások következtében.

Szükséges megismernünk, hogy a területi adottságokon túl milyen antropogén hatást gyakorolhat a belterületeken a települési víziközmű[7] helyzete, hogyan befolyásolhatják egyes elemei a talajvízszint alakulását, ezzel milyen hatást gyakorolnak egy-egy település belvízérzékenységére.

---

[5] A „földárja” a talajfelszínre is feltörő elöntés, amely a jelentős mértékben megemelkedő talajvíz hatására alakul ki, mely időnként és helyenként a felszín fölé jut, s itt rendszerint keveredik a csapadékból és hóolvadásból közvetlenül képződő és a helyi mélyedésekben, mély vonulatokban összegyűlő belvízzel.

[6] A 2006-ban és 2010-ben kialakult kiterjedt belvízi helyzet elemzései külön nem vizsgálták ebben az időszakban a földárja jelenség hatását, ami valószínűsíthető ezekben az időszakokban is.

[7] A víziközmű - szolgáltatás magyarországi tartalma két fő alaptevékenységet jelent, vezetékes ivóvízellátást és közműves szennyvízelvezetést.

1. Az ivóvíz-hálózat és az ivóvíz-felhasználás volumenének növekedése – a vezeték-rendszer állapota miatti veszteség a talajvízszintre növelő hatással van - a belvíz szempontjából negatív hatást gyakorolhat
2. a szennyvízkibocsátás növekedő tendenciája - a belvíz szempontjából negatív hatást gyakorolhat
3. a szikkasztott szennyvíz növeli a talajvíz szintjét – a belvíz szempontjából negatív hatást gyakorolhat (szükséges a terület általános talajvízszint adottságait és a talajtani adottságokat is együttesen vizsgálni),
4. a szennyvízhálózat fejlődése a fentiek alapján kedvező tendenciát jelent a belvíz-helyzetre,
5. a szennyvíztisztító telepek koncentrált, pontszerű terhelésként jelennek meg a belvízcsatornákon – a folyamatos terhelés a belvízelvezető-kapacitás fenntartása szempontjából káros hatást gyakorol,

A települések víziközmű helyzetében az elmúlt közel 10 évben[8] végbement változásokat az ATIVIZIG működési területére vonatkozóan mutatom be az igazgatóság rendelkezésre álló adatbázisai alapján, amely a közmű üzemeltetők különböző statisztikai bevallásain alapszik a 2005–2016 időszakra vonatkozóan. A változási trend bemutatására a KSH 2000-2016 időszak adatsorait mutatom be.

Ivóvíz-ellátó hálózatok és ivóvíz-fogyasztás (1. pont kapcsán): Az ivóvízbázist a Dél-Alföldön a mélységi vizek, ún. rétegvizek biztosítják, a sekély porózus vízrétegek vízminőségi állapotuk miatt már nem alkalmasak ivóvíz célú hasznosításra. A közműves ivóvízellátás az 1960-as évek óta folyamatos fejlődés révén érte el a mai állapotot. Összességében az ivóvíz-hálózatok mára kiépültek, jelentős változás a lakossági vízfelhasználásban nem várható. [10] [17] Egy-egy ipari beruházó megjelenésével, vagy megszűnésével, vagy a helyi turizmus fejlődésével várható lokálisan változás.

Magyarországon minden település rendelkezik közműves vezetékes ivóvíz-hálózattal, a háztartások 95%-a bekötéssel rendelkezik a hálózathoz. Az éves mintegy 440 millió köbméter vízfogyasztás háromnegyede lakossági felhasználáshoz köthető. Az egy főre eső napi átlagos vízfogyasztás 90–100 liter. [10]

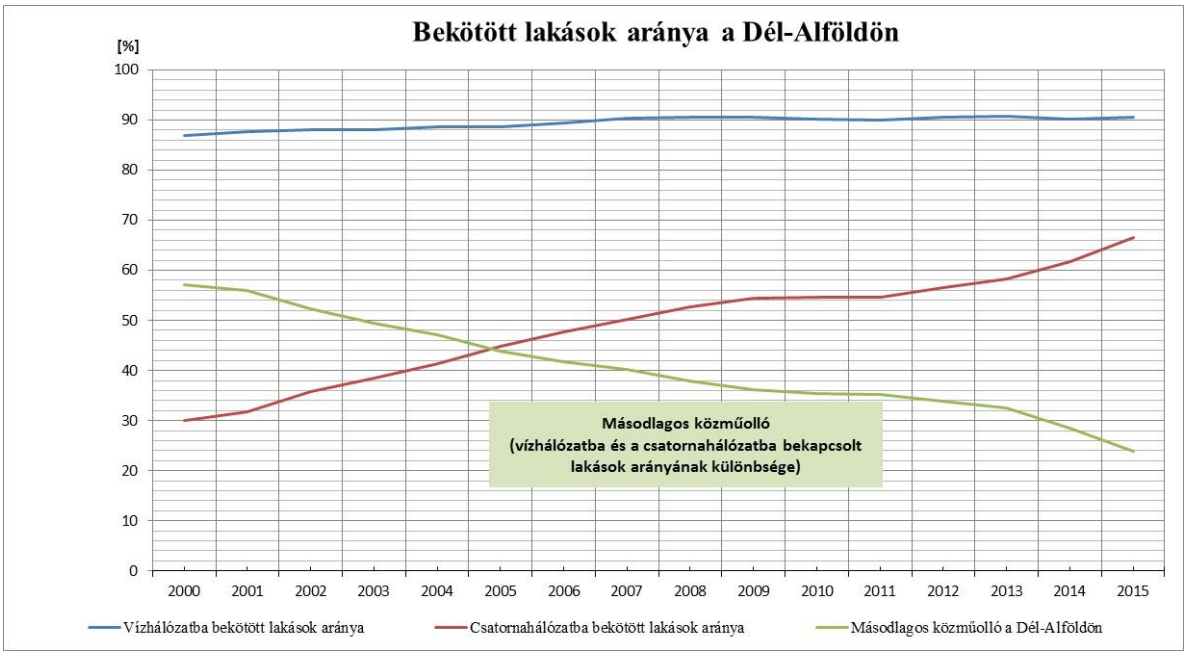
Az ivóvíz-hálózat és az ivóvíz-felhasználás volumenének növekedése a belvízhelyzetre negatív hatással lehet, mert ezzel együtt a szennyvíz-kibocsátás volumene is nő. Másik fontos probléma az ivóvízhálózatok kapcsán, hogy a meglévő, jellemzően 60–70-es években kiépült korszerűtlen ivóvízhálózatok jelentős hálózati-veszteséggel működnek.[9] Ezen hálózati veszteség 20–40 %-ra is tehető a szakértői becslések alapján. Ez a víz-elszivárgás a talajvízkészletet gyarapítja, a belvízképződést viszont elősegítheti azzal, hogy a talaj vízfelvevő képességét rontja, a talaj telítettsége miatt a beszivárgási folyamatokat lassítja.

A változások érzékeltetésére mutatom be a 4. ábrán a közműolló 2000–2015 időszak KSH adataiból szerkesztett grafikont, amely az ivóvízhálózatra és szennyvízhálózatra kötött lakások számát mutatja be, amelyet másodlagos közműollónak is nevezzük. Ebből jól látható, hogy az ivóvíz bekötések száma, azaz a közműves hálózatra bekötött lakásszámok száma, jellemzően stagnál az elmúlt évtizedben, 87%-ról indulóan elérte a 90%-ot, majd évek óta

[8] Az EUs csatlakozás kapcsán Magyarországon többlet források álltak rendelkezésre a víziközmű fejlesztésekre, valamint az áruház építési „boom” is körülbelül ekkor vált jelentős tényezővé a burkolt felületek kapcsán.

[9] Orosháza esetében szakértői becslés alapján 73 mm/év-re becsülték 1988-ban a szikkasztott szennyvíz mennyiségét, 15 mm/év mennyiségre az ivóvíz hálózati veszteség értékét. A sokéves átlag 550 mm csapadékmennyiséghez képest ez a 90 mm többletterhelés igen jelentős érték. [4. Pálfai, 1988]

stagnál. Ebből azt a következtetést vonhatjuk le, hogy az utóbbi évtized változásai közül az ivóvízfogyasztás változása nem releváns. Ezzel együtt a kibocsátott szennyvíz mennyisége sem változott számottevően. [21] Abban viszont jelentős változás történt, hogy ezen szennyvizek szikkasztással a település alatti sekély porózus víztestet terhelik-e, avagy a szennyvízgyűjtő hálózat fejlesztésével egyre több szennyvíz került be a szennyvíztisztító telepekre.



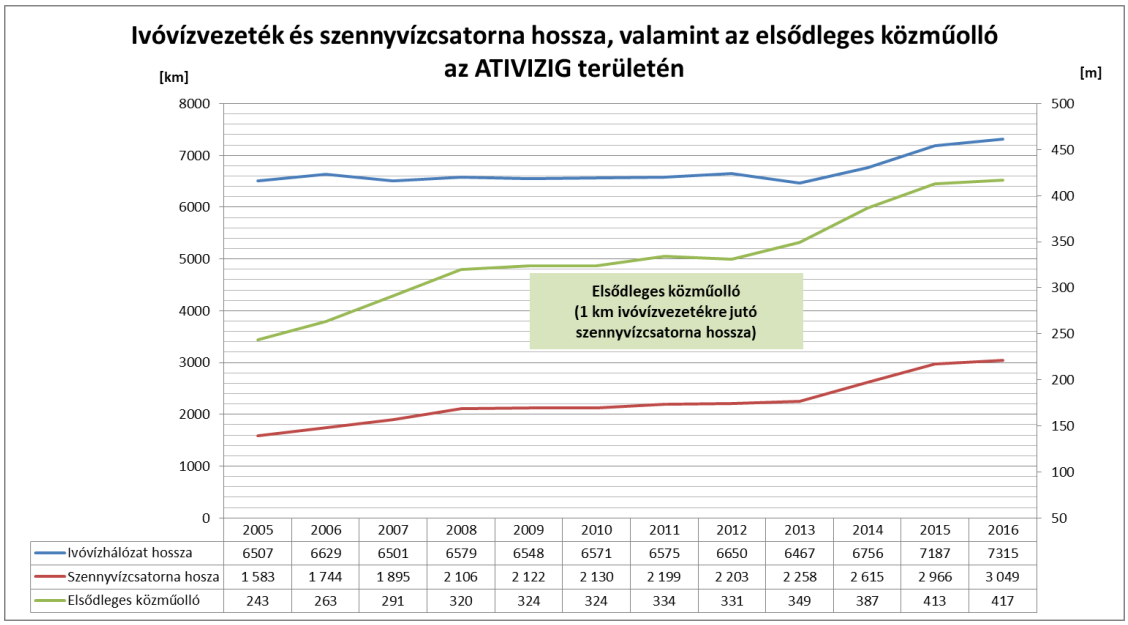
4. ábra: *Ivóvízhálózatra és a szennyvízhálózatra kötött lakások száma 2000-2015 időszakban, valamint a másodlagos közműolló*
(Szerkesztette a szerző KSH-adatok alapján) [21]

Szennyvíz-csatorna hálózatok és szennyvíztisztító telepek: A 4. ábrán fent bemutatott közműolló változásának adataiból egyértelmű, hogy a szennyvíz-csatornahálózatok jelentős fejlődésen mentek keresztül az elmúlt évtizedben, számottevő változást tapasztalunk a szennyvízbekötések, azaz a szennyvízhálózatra rákötött lakások számában, növekedés tapasztalható. A Nemzeti szennyvízprogramnak[10] köszönhetően a 2013–2015 időszakban arányaiban nagyobb növekedési tendencia tapasztalható.

A szennyvíz-csatornahálózat fejlettsége évtizedeken át jelentősen elmaradt az ivóvízhálózatok fejlődésétől. A településeken a 90-es évek végéig jellemzően a szikkasztásos szennyvíz-elhelyezés volt jellemző, a vezetékes ivóvízhálózatok kiépülését követően ugrásszerűen megnövekedett a szikkasztott szennyvíz mennyisége is. A települések alatt szennyvízdombok[11] alakultak ki, [11] amelyek rendkívül kedvezőtlenül befolyásolták a települések belvízhelyzetét: az elszikkasztott szennyvizek folyamatosan magasabb szinten tartották a belterületek alatt a talajvízszintet, csökkentve ezzel a talaj víz-áteresztő képességét, egyúttal növelve a belvízi elöntések kockázatát.

[10] Magyarország településeinek szennyvízelvezetési és –tisztítási helyzetéről, a települési szennyvízkezeléséről szóló 91/271/EGK irányelv Nemzeti Megvalósítási Program

[11] szennyvízdomb: vezetékes ivóvízellátás kiépülésével egyre több szennyvíz keletkezik, amit korszerűtlen módon elszikkasztanak. Sok szikkasztó sok elszikkasztott szennyvize folyamatosan magasan tartja a talajvizet a települések alatt, gyakorlatilag egy domb képződik. Ráadásul elszennyezi a talajvizet.

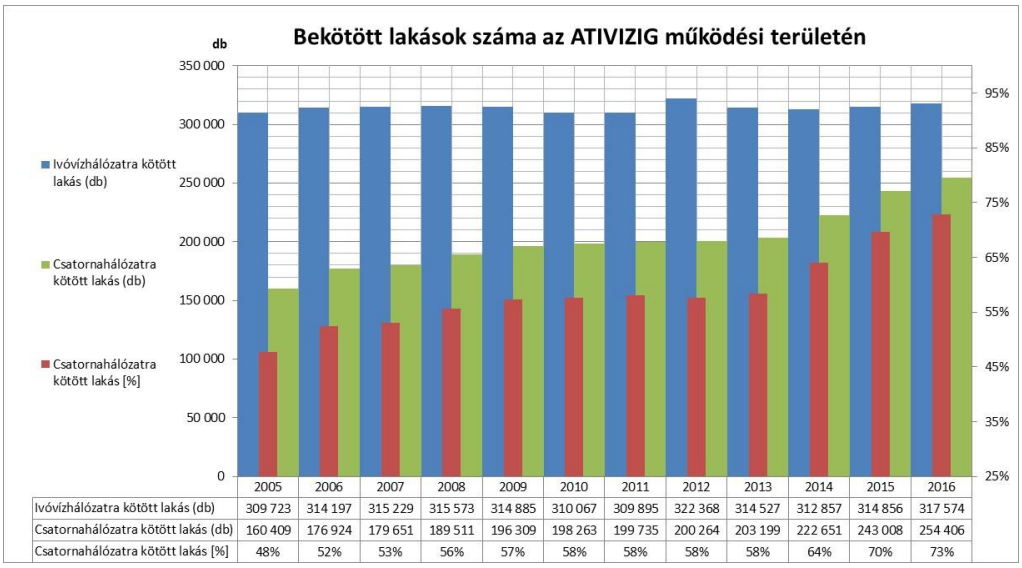


	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Ivóvízhálózat hossza	6507	6629	6501	6579	6548	6571	6575	6650	6467	6756	7187	7315
Szennyvízcsatorna hosza	1 583	1 744	1 895	2 106	2 122	2 130	2 199	2 203	2 258	2 615	2 966	3 049
Elsődleges közműolló	243	263	291	320	324	324	334	331	349	387	413	417

5. ábra: *Ivóvízvezeték és csatornahálózat fejlődése az ATIVIZIG működési területén, elsődleges közműolló* (szerkesztette a szerző *[17]*

A Nemzeti Szennyvízprogramnak köszönhetően, az EU-elvárásnak megfelelően, a 2000 LE[12] települések esetében gyakorlatilag 2015-re megvalósult a szennyvíz-csatornahálózatok kiépítése és megvalósult a szennyvíztisztítás is. A szennyvízhálózatba bekötött lakások számának további növekedésével a javulási tendencia is nő, amely jelentősen javítja a települések belvízi helyzetét. Illusztrációnak bemutatom az 5. ábrát, amelyen az ATIVIZIG működési területén lévő településein a szennyvízhálózatra és ivóvízhálózatra bekötött lakásszámokat ábrázolja. Az adatok alapján megállapítható, hogy az elmúlt több mint 10 év alatt a csatornahálózatra kötött lakások aránya 2005-ben még 48% volt, amely 2016. évre 73%-a nőtt, amely jelentős arányú növekedés. Ezzel együtt, mint már említettem, az ivóvízbekötések száma gyakorlatilag nem változott. [17]

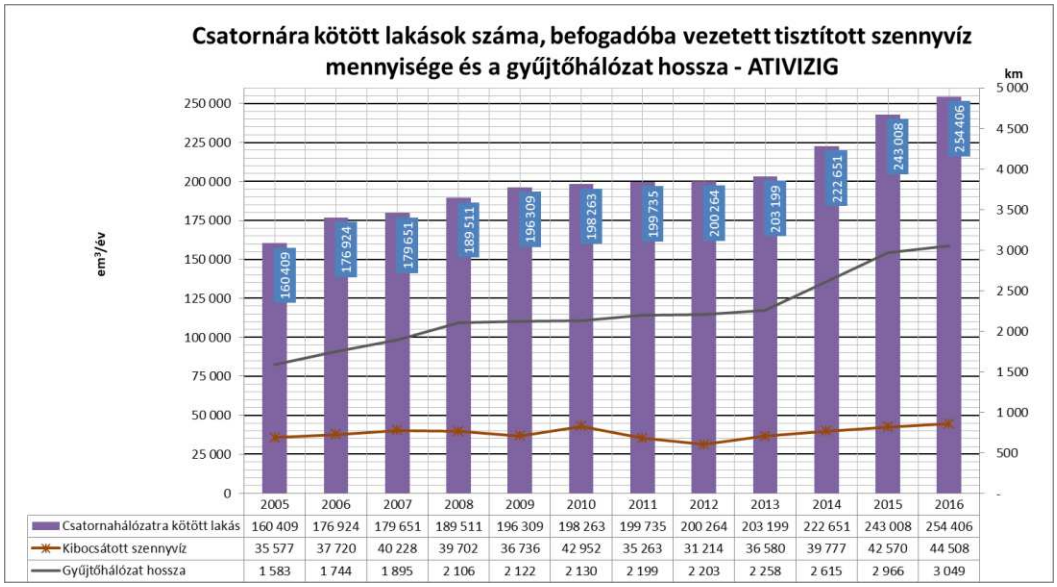
[12] lakos-egyenérték



	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Ivóvízhálózatra kötött lakás (db)	309 723	314 197	315 229	315 573	314 885	310 067	309 895	322 368	314 527	312 857	314 856	317 574
Csatornahálózatra kötött lakás (db)	160 409	176 924	179 651	189 511	196 309	198 263	199 735	200 264	203 199	222 651	243 008	254 406
Csatornahálózatra kötött lakás [%]	48%	52%	53%	56%	57%	58%	58%	58%	58%	64%	70%	73%

6. ábra: *Vezetékes ivóvízhálózatra és szennyvízhálózatra bekötött lakásszámok az ATIVIZIG működési területén.* (szerkesztette a szerző ATIVIZIG adatok alapján) *[17]*

Mit jelenthet ez a belvízképződés szempontjából? A kiépült rendszerek esetén a természet regenerálódó képességétől függően a szennyvízdombok megszűnése várható. Ahol nincs kiépített szennyvízcsatorna-hálózat, vagy a lakosság továbbra is szikkasztót használ,[13] ott a meglévő szennyvízdombok tovább-táplálása valósul meg, amely elősegítheti a belvíz kialakulását a korábban tárgyaltak alapján (lsd. 2. pont). Ezen hatás ritka beépítésű területeken, ill. jó vízáteresztő-képességű (homokos) altalajok esetében természetesen kisebb mértékű, akár elhanyagolható hatás is lehet.

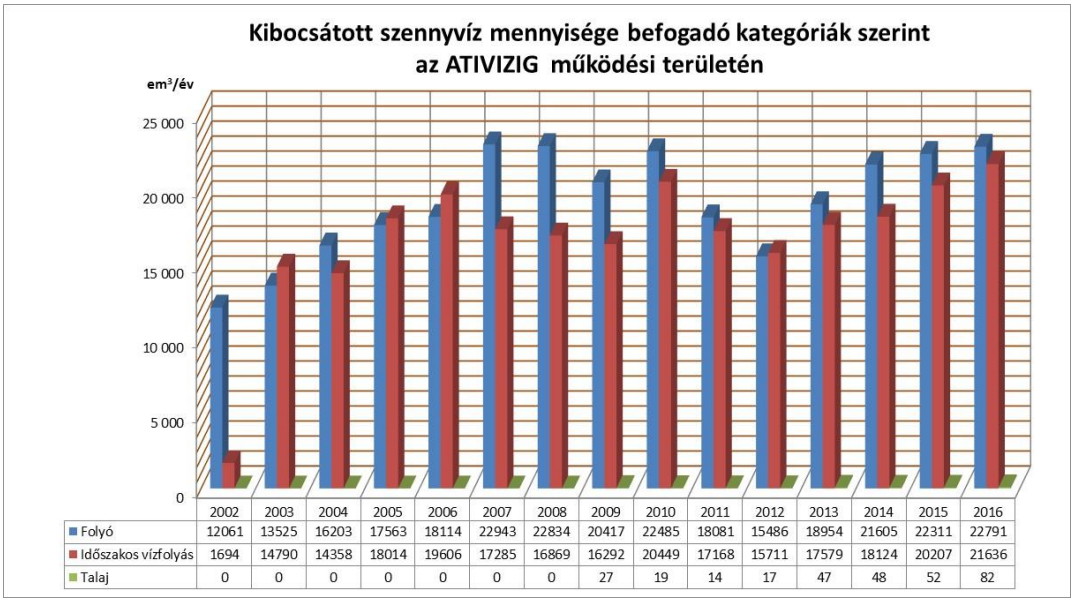


	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Csatornahálózatra kötött lakás	160 409	176 924	179 651	189 511	196 309	198 263	199 735	200 264	203 199	222 651	243 008	254 406
Kibocsátott szennyvíz	35 577	37 720	40 228	39 702	36 736	42 952	35 263	31 214	36 580	39 777	42 570	44 508
Gyűjtőhálózat hossza	1 583	1 744	1 895	2 106	2 122	2 130	2 199	2 203	2 258	2 615	2 966	3 049

7. ábra: *Csatornára kötött lakások és a befogadóba vezetett szennyvíz mennyiségének változása az ATIVIZIG működési területén (*szerkesztette a szerző) [17*]*

[13] A hatályos jogszabályoknak megfelelően a szikkasztókat egyedi oldó-medencés szennyvíztisztító kisberendezésekkel kell felváltani. A Nemzeti Szennyvízprogram végrehajtásával gyakorlatilag a 2000 LE településeken megvalósult a szennyvízcsatornázás és szennyvíztisztítás.

A 4. pontban írtak, miszerint a szennyvíz-elvezető rendszerek és szennyvíztisztító telepek fejlődése viszont egy másik problémát eredményezett, amely a működési területünk sajátossága: a tisztított szennyvizek bevezetése a tisztítótelepekről az addig csak időszakosan vizet szállító belvízcsatornákba történik (természetesen kivételt képeznek a folyó menti települések, ahol közvetlenül a folyóba kerülnek elvezetésre a tisztított szennyvizek). Ezzel a csatornák egy állandó vízterhelést kapnak, a tisztított szennyvíz a bejuttatott tápanyag miatt a csatornában a növényzet túlburjánzását is okozza. Továbbá ezen terhelés a csatorna eredeti méretezése során nem került számbavételre, a belvízi időszakban – és tulajdonképpen egész esztendőben - ez többlet terhelést jelent a belvízrendszer (csatornák és szivattyútelepek) számára. A dél-alföldi területeken egy-egy csatorna nem ritkán 60–90 km távolságból szállítja a vizet a befogadó folyókig. Ezzel a külterületi vízrendszerek terhelése növekedett – itt említve meg azt a sajnálatos tényt, hogy a termálvíz-felhasználás ugrásszerű növekedése a visszasajtolási kötelezettség megszűnése miatt szintén ugyanezen belvízcsatorna-hálózatot terheli a csurgalékvizek elvezetése miatt, valamint a fürdő-fejlesztések kapcsán jelentkező elfolyó vizek szintén ezen rendszereken kerülnek elvezetésre. Összefoglalóan a belvízelvezető vízrendszerek többletterhelése miatt nőtt a települések belvízi kockázata.

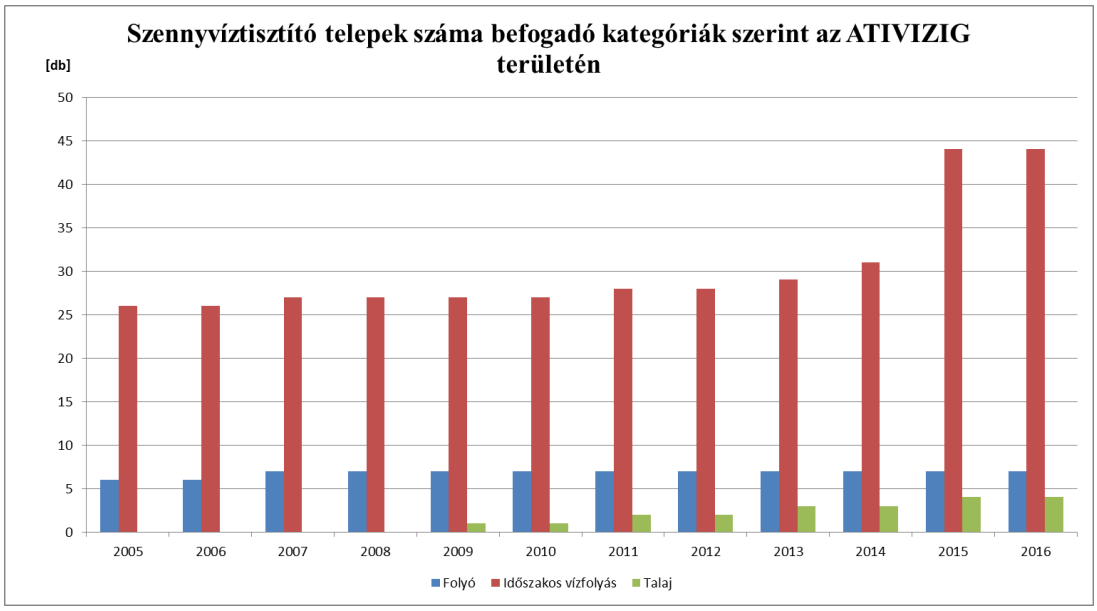


	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Folyó	12061	13525	16203	17563	18114	22943	22834	20417	22485	18081	15486	18954	21605	22311	22791
Időszakos vízfolyás	1694	14790	14358	18014	19606	17285	16869	16292	20449	17168	15711	17579	18124	20207	21636
Talaj	0	0	0	0	0	0	0	27	19	14	17	47	48	52	82

8. ábra: *Szennyvíztisztító telepek által kibocsátott szennyvíz mennyisége*
(szerkesztette a szerző ATIVIZIG adatok alapján [17])

A 6. ábrából kiemelem, hogy míg 2002-ben 1 964 ezer m^3/év tisztított szennyvíz került a belvízcsatornákba (az ábrán időszakos vízfolyásként szerepel), addig 2016-ra 21 636 ezer m^3/év, ami 12-szeres növekedést jelent[14]! (Az adatokat itt hosszabb időintervallumban vizsgáltam, hogy jól látható legyen a változás trendje.) [17]

[14] Ezzel együtt fontos felhívni a figyelmet arra a tényre is, hogy a szennyvíz-elvezetés mennyisége (azaz a tisztított szennyvíz mennyisége) jelentősen függ egy adott terület csapadékától is. Azaz aszályos időszakban jóval kevesebb, belvizes esztendőben jóval több lehet a szennyvízmennyiség!



9. ábra: *Szennyvíztiszító telepek számának növekedése* (szerkesztette a szerző ATIVIZIG adatok alapján) [17]

A területhasználat megváltozása, burkolt felületek növekedése is jelentős hatással van a települések belvíz-veszélyeztetettségére. Ez ugyan nem víziközmű témához kötött közvetlenül, de a belterületek kapcsán feltétlenül tárgyalni kell, mert jelentősen befolyásolja a belvízképződést. A burkolt felületen nem tud beszivárogni a csapadék, összegyűjtést követően befogadóba vezetik el. A burkolt felületekről gyorsabb az összegyülekezés, nagyobb az elvezetendő vízhozam is, úgynevezett csúcsterhelés fog jelentkezni a pontszerű bevezetésnél. Gyakori probléma, hogy a befogadó csatorna ezen csúcsterheléseket nem tudja fogadni, ezért ezen a bevezetési helyen és környékén folyamatosan elöntés-kiöntés fog jelentkezni. Hasonló problémával szembesülünk a belterületről kivezetett csapadékvízzel, amely eltérő méretezési alapelvek alapján megépült területi vízhálózatok esetében jelentkező csúcsterhelések, melyet a rendszer közvetlenül nem tud fogadni. [16]

A burkolt felületek növekedésére vonatkozó egzakt adatot a cikk írásának időtartama alatt nem találtam. Az viszont közismert tény, hogy számtalan bevásárlóközpont épült, hatalmas burkolt parkolók létesültek, a belterületi utak burkolása is az elmúlt évtizedekben rohamosan fejlődött, de a külterületi úthálózat is (elkerülő utak, autópályák), ipari parkok létesültek nagy burkolt felületekkel, csarnokokkal. Ezen többletterhelésekkel az igazgatóság egy-egy „befogadói" nyilatkozat kapcsán szembesült, amikor nyilatkozni kellett arról, hogy azon területről az a vízmennyiség bevezethető-e a befogadó csatornába?

A fentiek alapján nem körültekintő tervezés esetén a burkolt felületek növekedése paradox módon a belvízhelyzetet súlyosbíthatja, nem a burkolás helyén, de a bevezetés környezetében.

A *területhasználatok megváltozása* témakörhöz tartozik a *települések természetes tározóterének elvesztése* is. Ezek jellemzően a települések fejlődéséhez szükséges területi terjeszkedés kapcsán „meghódított" vízállásos, mélyfekvésű területek, ahol korábban a településről kikerülő vizek kiterültek, átmenetileg tározódtak. Ezek mintegy közbenső, kiegyenlítő tározó funkcióval bíró területek voltak, ahol ipari parkok, lakóparkok épültek. Ezen változásról nem lelhető fel adatbázis, értékelés sem a szakirodalomban, sem az adatszolgáltatásokban. A változás rendkívül kedvezőtlenül hat a belvízhelyzetre, a belterületi belvíz-veszélyeztetettséget növeli.

Összefoglalóan a településeken az antropogén hatások közül a víziközmű vonatkozású és területhasználattal kapcsolatos változásokat tekintettem át, amelyek hatással vannak a település belvízhelyzetére. Megállapítható, hogy az utóbbi évtizedben az ivóvíz-felhasználás kapcsán nem történ markáns változás, azonban a szennyvíz-hálózatok és szennyvíztisztítás fejlődésével egyrészt a szennyvízdombok eltűnésével jelentős javulás várható, a szennyvíztiszító

telepek bevezetései viszont a külterületi vízrendszerek belvíz-elvezetési kapacitására kedvezőtlen hatást gyakorolnak, ahogyan a burkolt felületek növekedése és a természetes tározóterületek eltűnése is.

KÖVETKEZTETÉSEK

A fentiek alapján a települések belvíz-veszélyeztetettsége a vízgyűjtő általános jellemzésével nem írható le. Az is megállapítható, hogy a belvízveszéllyel a várható globális klímaváltozás hatásainak elemzése alapján továbbra is számolnunk kell, de a várható vízhiányos időszakok miatt a települési vízgazdálkodásra, a komplex szemléletű megközelítésre kell helyezni a hangsúlyt! [15]

Konkrét beavatkozásokat egyrészt a település természeti adottságai alapján (mélyártéri, vagy fennsíki elhelyezkedés, kötött, vagy áteresztő burkolatú talajadottságok, a talajvíz szintje), másrészt az antropogén vízgazdálkodási környezetének együttes elemzése alapján kell meghatározni.

A belvízhelyzet javítása érdekében a terhelések csökkentése szükséges, így pl. az ivóvízhálózatok sürgető rekonstrukciójával a hálózati veszteségek jelentősen lecsökkenhetnének. Az áteresztő burkolatok és a lefolyást késleltető megoldások, a közbenső tározóterületek alkalmazásával jelentősen csökkenthető a belvízi kockázat.

A megállapítások előre vetítik annak szükségességét, hogy a vízgazdálkodás elemeit komplexen kell kezelnünk a külterület és belterületi vízrendszerek vonatkozásában is. Szélsőséges, vízbő és vízhiányos időszakokra kell felkészülnünk. Ez azt jelenti, hogy a vízelvezetési kapacitások fenntartása mellett fel kell készülnünk a vizek helyben tartására és hasznosítására. (Amikor sok víz van a területen, őrizzük meg a vízhiányos időszakokra). A települési szinten is alapvető fontossággal bír a csapadékvíz-gazdálkodás megvalósítása.

FELHASZNÁLT IRODALOM

[1] PÁLFAI I.: *Belvizek és aszályok Magyarországon.* Budapest: Közlekedési Dokumentációs Kft., 2004.

[2] BÁRDOS Z., MUHORAY Á.: A belvíz kialakulása és az ellene való védekezési lehetőségének vizsgálata. *Hadmérnök,* 7 1 (2012), 78–90. http://hadmernok.hu/2012_1_bardos_muhoray.pdf

[3] KOZÁK P.: *A belvízjárás összefüggéseinek vizsgálata az Alföld délkeleti részén, a vízgazdálkodás európai elvárásainak tükrében*. Szeged: Szegedi Tudományegyetem Természettudományi Kar, 2006. (Doktori értekezés) http://doktori.bibl.u-szeged.hu/1679/1/T%C3%A9zisek_HUN.pdf (A letöltés időpontja: 2017. október 22.)

[4] PETRÓ T.: A helyi vízkárelhárítás helyzete napjainkban, a védekezés feladatai. *Hadmérnök,* 6 1 (2011), 172–180.

[5] *Megvalósult Magyarország belvízi veszélytérképezése az Árvízi kockázati térképezés és stratégiai kockázatkezelési terv készítése című projekt keretein belül.* Budapest: BM Vízügyi Főigazgatóság, 2015. www.vizugy.hu/index.php?module=content&programelemid=1&id=1187 (A letöltés időpontja: 2017. október 10.)

[6] BÍRÓ T., TAMÁS J., LÉNÁRT Cs., TOMOR T.: A belvíz-veszélyeztetettség térbeli elemzése. *Acta Agrária Kaposváriensis*, 6 (2002), 139–152.

[7] ESA: *Senitel–2.* s.d. www.esa.int/Our_Activities/Observing_the_Earth/Copernicus/Sentinel-2 (A letöltés időpontja: 2017. október 20.)

[8] PÁLFAI I: Földárja, az Alföld sajátos hidrológiai jelensége. *Hidrológiai közlöny,* 85 3 (2005), 15–18.

[9] BÁRDOS Z., MUHORAY Á.: A települések vízkár elleni védekezési feladatinak változása a megváltozott jogszabályi környezetben. *Hadmérnök, 9 3 (2014),* 48–60. http://hadmernok.hu/143_05_bardosz_ma.pdf

[10] PAPP M., DÁVIDNÉ DELI M., BÓDI G., SOLTI D., SOLYMOSI E., HAVAS A.: *Távlati vízigények elemzése Ivóvízfogyasztás/ivóvízigények megállapítása és előrebecslésük Magyarországon.* Magyar Vízközmű Szövetség, (2007) www.kvvm.hu/cimg/documents/3_tanulmany.pdf (A letöltés időpontja: 2017.november 11.)

[11] KATO S.: Szabolcs-Szatmár-Bereg megyei Szennyvíz-elhelyezési Program főbb cselekvési területeinek ismertetése. *Magyar Hidrológiai Társaság XXVI. Országos Vándorgyűlése.* Nyíregyháza, 2005. http://apps.arcanum.hu/app/hidrologia/view/HidrologiaiVandorgyules_2005_23/?pg=39&layout=s (A letöltés időpontja: 2017. október 10.)

[12] MEZŐSI G., BATA T., BLANKA V., LADÁNYI Zs.: A klímaváltozás hatása a környezetei veszélyekre az Alföldön. *Földrajzi Közlemények,* 141 1 (2017), 60–70.

[13] NOVÁKY B.: Az éghajlatváltozás és hatásai. In. SOMLYÓDY L. (szerk): *Magyarország vízgazdálkodása: Helyzetkép és stratégiai feladatok.* MTA: Budapest, 2011. 85–102.

[14] PUSKAS I., GÁL N., FARSANG, A.: Impact of weather extremities (excess water, drought) caused by climate change on soils in Hungarian Great Plain (SE Hungary). In. RAKONCZAI J., LADÁNYI Zs. (Eds.): *Review of climate change research program at the university of Szeged (2010–2012).* Szeged: Institute of Geography and Geology (2012), 73–84.

[15] AKRAM, F., RASUL, G. M., MASUD, M. K., KHAN, K., SHARIF, M., AMIR, I. I.: A Review on Stormwater Harvesting and Reuse. *World Academy of Science, Engineering and Technology*, 8 3 (2014). http://waset.org/publications/9997816/a-review-on-stormwater-harvesting-and-reuse (A letöltés időpontja: 2017. 10. 10.)

[16] PRIVÁCZKINÉ HAJDU Zs.: A belterületi és külterületi vízrendezés összehangoltságának hiánya. *Magyar Hidrológiai Társaság XXVI. Országos Vándorgyűlése 3. szekció: Területi vízgazdálkodás.* Miskolc, 2008. július 2–4. http://apps.arcanum.hu/app/hidrologia/view/HidrologiaiVandorgyules_2008_26/?query=SZO%3D(priv%C3%A1czkin%C3%A9)&pg=525&layout=s (A letöltés ideje: 2017. 10. 22.)

[17] *Az ATIVIZIG adatbázisa.* Hely: Szeged (ATIVIZIG) 2002 – 2016. Az ATIVIZIG adatbázisa, amely a közműszolgáltatók által szolgáltatott adatok alapján készült, s amely a tárgyévekre vonatkozó Statisztikai Adatgyűjtési Program (OSAP) keretében a jogszabály által, azaz a statisztikáról szóló 1993. évi XLVI. törvény végrehajtásáról szóló 170/1993. (XII. 3.) Korm. rendelet, az Országos Statisztikai Adatgyűjtési Program adatgyűjtéseiről és adatátvételeiről szóló 288/2009. (XII. 15.) Korm. rendelet alapján a víziközmű szakterületi adatgyűjtésekkel összefüggő központi feladatok ellátása kapcsán (pl. OSAP 1376, OSAP1378, OSAP2036) az igazgatóság rendelkezésére áll. A cikkben a 2012-2016 évi adatok szerepelnek.

[18] *Az ATIVIZIG által végzett belvízvédekezési tevékenységek zárójelentései.* Hely: Szeged (ATIVIZIG), 1981 – 2005.

[19] SZILÁGYI J. E.*:* Vízjog: a vizek tulajdonának és használatának főbb magyar előírásai a nemzetközi tendenciák tükrében. *Sectio Juridica et Politica, Miskolc, Tomus XXIX/2. (2011), pp. 595–622* http://www.matarka.hu/koz/ISSN_0866-6032/tomus_29_2_2011/ISSN_0866-6032_tomus_29_2_2011_595-622.pdf

[20] PÁSZTOR L., KÖRÖSPARTI J., BOZÁN CS., LABORCZI A., TAKÁCS K.: Spatial risk assessment of hydrological extremities: Inland excess water hazard, Szabolcs-Szatmár-Bereg County, Hungary, *Journal of Maps (2014)*, DOI: 10.1080/17445647.2014.954647, http://dx.doi.org/10.1080/17445647.2014.954647

[21] *KSH adatok* 6.2.2.6. Közműolló, december 31. (2000–) a KSH 1062-es adatgyűjtése alapján - a települések vízellátásával, szennyvízelvezetésével és szennyvíztisztításával kapcsolatos adatok gyűjtése, tájékoztatás. http://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_zrk006.html

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

MARCAL FOLYÓ MIKROBIÁLIS ÁLLAPOTÁNAK VIZSGÁLATA A VÖRÖSISZAP KATASZTRÓFA TÜKRÉBEN

TESTING THE RIVER MARCAL MICROBIOLOGICAL STATUS IN THE MIRROR OF THE RED SLUDGE CATASTROPHE

TAKÁCS Krisztina

(ORCID: 0000-0002-9481-814X)

takacs.krisztina@uni-nke.hu

Absztrakt

Az emberiség és a technológia fejlődésével az ipari katasztrófák száma is megnövekedett a világon. Ezekről általánosságban elmondható, hogy az okozott kár kiemelkedően jelentős mértékű, illetve tömeges emberi sérülés vagy haláleset következik be.
Magyarország eddigi legnagyobb ipari szerencsétlensége a 2010. október 4-én bekövetkezett vörösiszap katasztrófa volt, mely azon kívül, hogy emberéleteket követelt, a környezetet is jelentősen károsította. A cikk elkészítésével célom volt, hogy bemutassam a hazánkban bekövetkezett vörösiszap katasztrófát, és annak környezetre gyakorolt pusztító hatásait. Írásomban, a Marcal folyóra összpontosítva célom volt kideríteni, hogy a vörösiszap súlyosan károsító hatása hogyan hatott az ökoszisztémára, különösen a mikróba-közösségekre. Saját mintavételezésből származó adatokat feldolgozva egy átfogó képet szeretnék kialakítani a folyó jelenlegi állapotáról.
„A cikk az Emberi Erőforrások Minisztériuma ÚNKP-17-3-I-NKE-7 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült”

Kulcsszavak: *ipari balesetek, vörösiszap katasztrófa, Marcal folyó*

Abstract

With the development of humanity and technology, the number of industrial disasters has also increased in the world. Generally speaking, the damage caused is extremely significant, or massive human injury or death occurs.
The biggest industrial disaster in Hungary so far has been the red sludge catastrophe on October 4, 2010, which, in addition to demanding human lives, has also seriously damaged the environment.
With this article, I was aiming to introduce the red sludge catastrophe and its destructive effects on the environment. In my writing, focusing on the river Marcal, I was determined to find out how the severely damaging effects of red mud affected the ecosystem, especially for the microbial communities. By processing data from my own sampling, I would like to build a comprehensive picture of the current state of the river.
"This article was prepared by the Ministry of Human Resources with the support of New National Excellence Program ÚNKP-17-3-I-NKE-7"

Keywords: *industrial accidents, red sludge catastrophe, river Marcal, microbial community*

A kézirat benyújtásának dátuma (Date of the submission): 2018.04.11.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.01.

BEVEZETÉS

Az ipar folyamatos fejlődésének következményeként a civilizációs katasztrófák általi veszélyeztetettség is növekedett, amelybe beletartoznak az ipari, kémiai balesetek is. [1] Hazánk eddigi legsúlyosabb ipari szerencsétlensége 2010. október 4-én következett be Ajka térségében. A vörösiszap katasztrófa emberéleteket követelt, emellett pedig a környezetet is jelentősen károsította. Ezért is kell kiemelt hangsúly fordítani a kémiai biztonság, illetve az iparbiztonság tevékenységének körére, hiszen a 2012. január 1-én hatályba lépett iparbiztonsági jogi szabályozásban már kiemelt hangsúlyt kapnak az iparbiztonsági feladatok, mint például a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezés, valamint a veszélyes áru szállítmányok, a létfontosságú rendszerek és létesítmények védelme is. [2]
Írásomban szót ejtek a kémiai biztonságról, illetve az iparbiztonság jelentőségéről, bemutatom az ehhez kapcsolódó jogszabályokat. Ismertetem a vörösiszap összetételét, a katasztrófa lefolyását, illetve a környezetre gyakorolt súlyos hatásait, mely többek között a Marcal folyót, és annak élővilágát is érintette.

A cikk elkészítésével célom volt, hogy felmérjem a Marcal mikrobiológiai állapotát a bekövetkezett szerencsétlenség után 7 évvel. Ezeket az eredményeket párhuzamba állítottam a Lajta folyóból vett vízminták eredményeivel, melyeket grafikonon szemléltetek. 1 éven keresztül, több mintavételi időpontban vizsgáltam a 2 folyó főbb bakteriológiai jellemzőit. Jelen tanulmány terjedelme nem tette lehetővé, hogy minden egyes paramétert megvizsgáljak, így csak a főbb indikátor mikroorganizmusokat néztem meg, amik a Coliform, E.coli és Pseudomonas aeruginosa. Ezen mikrobáknak a vízminőség ellenőrzésekor nagy szerepük van, jelenlétükből számos további, hasznos információt tudhatunk meg a folyók állapotáról. Ezen kívül megmértem még a folyók vizének pH-értékét is, a mintavétel idején a víz és a levegő hőmérsékletét is. Mindezek mellett feltüntettem még a két folyó vízállását a mintavételi időpontokban, hiszen ez is hatással lehet a mikroorganizmusok összetételére.

Mindezen vizsgálatokat azért is tartom fontosnak, hogy bemutassam milyen következményei voltak a vörösiszapnak, illetve milyen mértékben sikerült rekonstruálni a katasztrófa előtti állapotot a Marcal folyón.

KÉMIAI BIZTONSÁG, IPARBIZTONSÁG JELENTŐSÉGE

A veszélyes anyagok és készítmények káros hatásainak megfelelő módon történő azonosítása, megelőzése, csökkentése, elhárítása céljából megalkották a 2000. évi XXV. törvényt a kémiai biztonságról, mely a következőképpen definiálja a kémiai biztonság szókapcsolatot: „a kemizációból, a vegyi anyagok életciklusából származó, a környezetet és az ember egészségét károsító kockázatok csökkentését, elkerülését célul kitűző, illetőleg megvalósító intézmények, tevékenységek olyan összessége, amely egyidejűleg tekintetbe veszi a fejlődés fenntarthatóságának szükségességét.” [3]

Ez alapján elmondható, hogy a veszélyes anyaggal, illetve a veszélyes készítménnyel kapcsolatos tevékenységet úgy kell megtervezni és végezni, hogy a tevékenység az azt végzők és más személyek egészségét ne veszélyeztesse, a környezet károsodását, illetve szennyezését ne idézze elő, illetőleg annak kockázatát ne növelje meg, ugyanis egy esetlegesen bekövetkező veszélyes anyag baleset következményeinek felszámolása nehéz, összetett és költséges feladat. [4] A kárfelszámolást nehezíti, hogy a környezetbe jutott veszélyes anyag által szennyezett eszközöket, tereptárgyakat mentesíteni kell. [5]

A vörösiszap katasztrófa világított rá Magyarországon az iparbiztonsági jogszabályok felülvizsgálatának szükségességére, ugyanis a MAL Magyar Alumínium Termelő és Kereskedelmi Zrt. nem tartozott a vörösiszap katasztrófa bekövetkezésekor érvényes Seveso II. irányelv előírásait magába foglaló 18/2006. (I. 26.) Korm. rendelet hatálya alá, mivel a vörösiszap a jogszabály 1. mellékletében foglaltak szerint nem minősült veszélyes anyagnak,

ugyanis nehézfém tartalma a határérték alatt van. Azonban a vörösiszap veszélyességét és potenciális szennyező hatását elsősorban az erősen lúgos kémhatása képzi. A Magyar Alumínium Termelő és Kereskedelmi Zrt. ajkai telephelyén bekövetkezett katasztrófa a jogszabály szigorítását indokolta, melynek eredményeként született meg a jelenleg érvényes a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. Törvény, valamint végrehajtási rendelete a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 219/2011. (X. 20.) Korm. rendelet. [3] A veszélyes anyagokkal foglalkozó üzem definícióját a 2011. évi CXXVIII. törvény tartalmazza, miszerint: ”egy adott üzemeltető irányítása alatt álló azon terület egésze, ahol egy vagy több veszélyes anyagokkal foglalkozó létesítményben - ideértve a közös vagy kapcsolódó infrastruktúrát is - veszélyes anyagok vannak jelen a törvény végrehajtására kiadott jog-szabályban meghatározott küszöbértéket elérő mennyiségben, és ennek alapján alsó vagy felső küszöbértékűnek minősül.” [6] A 2011. évi CXXVIII. törvény, valamint a 219/2011. (X. 20.) Korm. rendelet a korábbi iparbiztonság szabályozását gyökereiben változtatja meg. Az új jogszabály újraértékeli a veszélyes ipari üzemek felügyeleti rendszerét, mely szerint a hatósági jogkört a hivatásos katasztrófavédelmi szerv gyakorolja. A katasztrófavédelem szervezetén belül megalakult az iparbiztonsági szakterület. [3]

Az iparbiztonsági feladatok ellátására létrehozott országos iparbiztonsági főfelügyelőség tevékenysége négy fő szakterületre terjed ki. Ezek a veszélyes üzemek felügyelete, a veszélyes áruk szállításának ellenőrzése, a kritikus infrastruktúrák védelme, valamint a nukleárisbalesetelhárítás szakterülete. [7]

VÖRÖSISZAP TULAJDONSÁGAI

A vörösiszap az alumíniumgyártás során, a bauxit magas hőmérsékleten és nyomáson történő lúgos – általában nátrium-hidroxidos – feltárása után visszamaradó melléktermék. Összetételét a kibányászott bauxit tulajdonságai és a kezelés során keletkező, illetve hozzáadott és visszamaradó anyagok határozzák meg. [8] [9] Nehézfém tartalma jelentős, ezt láthatjuk az 1. táblázatban is. Veszélyes hulladék, a bőrt az égési sérülésekhez hasonlóan kimarja. A lúgos hulladék a természetbe kerülve pusztítóan hat az élővilágra, de ennek a pusztításnak a következményei elsősorban rövid távon jelentkeznek. Az átlagos hazai talajokhoz képest 7-szeres a vörösiszap nehézfémtartalma, a radioaktív elemek aránya pedig a talajokénak 10-20-szorosa. Azonban a nehézfémek a vörösiszapban szerencsére nehezen mobilizálható formában vannak jelen, így azokat az élő szervezetek csak nehezen tudják felvenni. A nevét az iszapszerű állagáról és a színéről kapta, amit a bauxitban jelenlevő vas-oxid okoz. Egy tonna timföld előállításakor 1,5-2 tonna vörösiszap keletkezik. Jellemzően 5-8 % nátronlúgot tartalmaz, pH-ja 12-13 körüli, azaz erősen maró tulajdonságú. [10]

A vörösiszap fő alkotóinak mennyiségét az 1. táblázatban láthatjuk. [8] [9]

Fő komponensek	Tömeg %)	Fő komponensek	Tömeg (%)
Vas(III)-oxid (Fe_2O_3)	33-40	Alumínium-oxid (Al_2O_3)	15-19
Szilícium-oxid(SiO_2)	10-15	Nátrium-oxid (Na_2O)	7-11
Titán-dioxid (TiO_2)	4-6	Kálcium-oxid (CaO)	3-9
Vanádium(V)-oxid (V_2O_5)	0,2-0,4	Foszfor-pentoxid (P_2O_5)	0,5-1,0
Szén-dioxid (CO_2)	2-3	Kén-trioxid (SO_3)	0,8-1,5
Magnézium-oxid (MgO)	0,3-1,0	Fluor (F)	0,1-0,15
Szén (C)	0,15-0,20	Egyéb (ritkaföld) fémek	1>

1. táblázat A vörösiszap kémiai összetétele, Forrás:[10]

A vörösiszap toxikus fémeket és radioaktív elemeket is tartalmaz, amelyek a technológiai műveletek során ebben a melléktermékben dúsúlnak fel. A radioaktív elemek koncentrációja a tipikus hazai talajokra jellemző értékekhez képest 10-20-szoros dúsulást mutat. [10]

KATASZTRÓFA BEMUTATÁSA, HATÁSA A MARCAL FOLYÓRA

A vörösiszapot tároló zagyterek leírása

Az ajkai timföldgyár zagytározó kazettáiban 50 millió köbméter szürke és 30 millió köbméter vörösiszapot tároltak a környezeti katasztrófa előtt. Az I-V. jelű kazettákban erőművi salakot, illetve pernyét tárolnak. A feltöltés vastagsága több mint 10 méter. Fúrásokkal a talajvizet közvetlenül a feltöltés alatt érték el. A VI-IX.-jelű kazetták alatt 1–2 m vastag a néhol meglehetősen laza ártéri üledék kőtörmelékes homok, kavicsos-kőtörmelékes agyag, alatta 5–7 m vastag, durvaszemű homok, kavicsos homok települ. A durvább szemcséjű anyagok egykori mederüledékek. Az egyes üledékek vízzáró képessége erősen változó. A homokrétegek vízáteresztő képessége kisebb, mint a kavicsé. Az allúvium feküjének (ez a kazetták alatti, kőzetlisztes agyag) vízzárósága a homok-, illetve mészerek miatt változó, de szivárgási tényezője általában kisebb, mint 10^{-6} m/s. Ez alatt több 10 m vastag, gyakorlatilag vízzárónak tekinthető agyag települ. A talajvíz a vizsgált területen 1–4 m mélyen található, és a Torna patak völgye felé áramlik, fő áramlási iránya a Ny-i, valamint a dombokról déli irányú.

Magyarország eddigi legnagyobb következményekkel járó, 10 ember életét követelő, több, mint 800 ha területet érintett ipari katasztrófája 2010. október 04-én történt, amikor a MAL Zrt. tulajdonában lévő Ajkai Timföldgyár Kolontár és Ajka között létesített, 400×600 m-es vörösiszap tároló X. kazetta észak-nyugati sarkánál, nem pillanatszerű, hanem kb. 10-15 percig tartó folyamatos gátszakadás következett be. [11]

A vörösiszap katasztrófa bemutatása

A gátszakadás következtében a több mint egymillió köbméternyi zagy a Torna patak medrén keresztül elöntötte Kolontár, Devecser és Somlóvásárhely települések mélyebben fekvő részeit és mintegy 800 hektár területet árasztott el. Rövid idő alatt elmosta a környező falvakat, a hömpölygő iszap lakóházakat károsított, elöntötte az épületeket, autókat sodort el. Az erősen lúgos, maró hatású ipari hulladék körülbelül 40 négyzetkilométeren terült szét, felbecsülhetetlen gazdasági és ökológiai károkat okozva a Devecseri kistérségben. Az esemény következtében tíz ember meghalt, a sérültek száma több mint 150 fő. [12] Az áradat súlyos sérüléseket okozott a lakosság és a mentő erők körében egyaránt. A beömlési ponttól lefelé az erősen lúgossá váló víz a Tornán és a Marcalon gyakorlatilag letarolta az egész élővilágot, egyetlen baktérium, sőt, a vízinövények sem maradtak életben. [13]

A Marcal folyó vízminőségének védelme érdekében a vízügyi szakemberek irányításával a katasztrófát követő nap megkezdődött a kálcium-nitrát és magnézium-nitrát bejuttatása a folyóba. A Marcal védelmén túl a munkálatok a Duna szennyeződésének megakadályozása érdekében is kiemelkedően fontosak voltak. A védekezés fő célja az volt, hogy a Marcalba jutott nehézfém szennyezés a folyó medrében maradjon, és onnan a későbbiekben eltávolítható legyen. Ennek érdekében a Marcalon, több helyen fenékküszöb épült, hogy a duzzasztott térben a lelassult vízből a veszélyes iszap kiülepedjen. A pH további csökkentése érdekében bioecetsavas semlegesítést is alkalmaztak, az ecetsav adagolása két ponton történt, a duzzasztónál és a Koroncói hídnál. Továbbá a beavatkozási pontokon tovább folytatták a gipsszel való kármentesítést, amit a duzzasztással párhuzamosan kezdtek el. A gipsz bejuttatásának másik előnye az volt, hogy segítette a kiülepedést, a veszélyes anyag továbbjutásának akadályozását.

Ezt követően a víz tovább hígult a Rába, majd a Mosoni-Duna vizével és csak ezt követően került a Dunába 9.1-es pH-val. A szennyezés hullám levonulása után a pH érték fokozatosan visszaállt a természetes 8,5 körüli értékre, mivel a szennyezés utánpótlása megszűnt. [14]

A gyors és szakszerű beavatkozási munkálatoknak köszönhetően sikerült megakadályozni a Rába és a Duna súlyos lúgos kémhatású és nehézfém szennyeződését. [8]

Az Országos Katasztrófavédelmi Főigazgatóság (továbbiakban: OKF) a vörösiszap katasztrófa másnapján a Magyar Tudományos Akadémia (továbbiakban: MTA) segítségét kérte az iszaptól elárasztott terület vizsgálatára, a károk meghatározására. Az MTA által felkért vegyészekből, ökológusokból, biológusokból és környezetvédelmi szakemberekből álló szakértői csoport 2010. október 5.-én utazott le először a katasztrófa helyszínére. A helyszínen majd laboratóriumi mérések útján megvizsgálták a katasztrófa által okozott károkat majd elkészítették gyorsjelentésüket és javaslataikat a legszükségesebb teendőkről.

Az MTA Kémiai Kutatóközpont Anyag- és Környezetkémiai Intézet (továbbiakban: MTA KK AKI), a Magyar Állami Földtani Intézet (továbbiakban: MÁFI) és egy független szervezet – a Bálint Analitika Kft.- munkatársai 2010.10.12-ig összesen 16 db., Kolontár és Devecser térségében összegyűjtött vörösiszap minta elemzését végezték el. A különböző helyekről vett minták elemzése alapján a tározóból kifolyt zagy pH-ja 11-14 között változott, ezért a vörösiszap a környezetre veszélyes anyagnak tekintendő.

A vörösiszap kiömlése óta eltelt időszakban nagyszámú mintavétel és elemzés történt. A szakértők a vörösiszap okozta környezeti károk részletes felméréséhez, a szennyezés terjedésének megállapításához további mintákat vettek, vizsgálatokat végeztek el. A vörösiszap lúgos tulajdonsága már ismert volt, de a nehézfém tartalma is komoly riadalmat keltett a nehézfémek bizonyított humán egészségügyi/toxikológiai és környezeti/ökológiai hatásai miatt. A minták nehézfém tartalma a 3. számú táblázatban látható. Elemanalitikai módszerekkel elvégzett laboratóriumi vizsgálatok során megállapították, hogy a vörösiszap a szennyvíziszapokra megengedett határértékeknél kisebb, esetenként jóval kisebb koncentrációban tartalmaznak kadmiumot, krómot, higanyt, nikkelt, ólmot és cinket. Az arzéntartalom az MTA KK AKI Kolontár külterületén vett mintájánál és a Bálint Analitika Kft. által vizsgált mintáknál ugyancsak kisebb a szennyvíziszap határértékénél, az MTA KK AKI a gátszakadás közelében vett mintánál és a MÁFI által gyűjtött mintáknál az adott elemre vonatkozó határértéknél magasabb arzéntartalmakat mért.

Minták	Vörösiszap fémtartalma (mg/kg) szárazanyag						
	As	**Cd**	**Cr**	**Hg**	**Ni**	**Pb**	**Zn**
MTA KK AKI 2010.10.05. (gátszakadástól 100 méterre)	135-144	n.d.	632-677	1,64-8,59	192-219	189-195	47,9-56,7
MTA KK AKI 2010.10.05. (Kolontártól 1km-re nyugatra)	33,4-35,7	n.d.	83,4-85,8	n.d.	64,3-73,1	43,2-53,9	36,8-43,6
Bálint Analitika 2010.10.05. gátszakadástól 30m-re vett iszap	43,6-44,5	2,30-2,42	689-721	0,54-0,67	281-289	80,9-83,2	142-155
Bálint Analitika 2010.10.05. gátszakadástól 50m-re vett iszap	27,9-32,3	0,24-0,34	57,6-74,5	0,18-0,28	26,3-36,4	7,52-11,8	64,2-77,9
MÁFI 2010.10.06. Kolontár/Devecser térségében vett 10 iszapminta adatai (határértékek)	81,6-131	0,82-1,44	360-694	0,61-2,83	143-322	96,2-177	108-172
MH HAVÁRIA 2010.10.05-i kolontári és devecseri minta átlaga	69-176	-	-	-	112-259	51-125	35-96
Határértékek szennyvíziszapra	*75*	*10*	*1000*	*10*	*200*	*750*	*2500*

Megjegyzés: n.d.: nem mérhető; -: nem mért elem

2. táblázat A vörösiszap fémtartalma[10]

Korábbi irodalmi adatok és kutatások alapján ismert, hogy a hulladék (minta) nehézfém tartalma akkor jelent valós környezeti veszélyt, ha a fémek kioldódnak a vörösiszapból és ezáltal lehetővé válik, hogy az élő szervezetek könnyebben fel tudják azokat venni. A fémek kioldódását szabványos módszerek szerint szárított iszap mintákon, desztillált vizes, illetve ammónium-acetátos pufferben (pH=4,5) határozták meg. Vizsgálták a mintákban lévő arzén, kadmium, króm, higany, nikkel ólom és cink mennyiségét, illetve kioldódását. A mérési adatok alapján azonban megállapították, hogy az adott feltételek mellett a vizsgált fémek nem oldódnak ki a vörösiszapból. [11]

A katasztrófát követően, 2010 októbere után még csak feltételezésképpen állították azt a szakemberek, hogy a szennyezés hullám levonulása után a pH érték minden bizonnyal fokozatosan visszaáll a természetes 8,5 körüli értékre az érintett folyókban, és amennyiben a szennyezés utánpótlása megszűnik az élővilág lassan és fokozatosan regenerálódik a felsőbb szakaszról és a mellékvízfolyásokból kiindulva. A mérgezés a közönséges és széles körben elterjedt fajok mellett a ritka és védett fajokat is érintett, így növelte a károsodás mértékét.

A vízi élővilágra a kiömlő vörösiszap nátronlúg (nátrium-hidroxid) tartalma volt közvetlen, igen súlyosan károsító hatással, hiszen ahogy már említettem, a beömlési ponttól lefelé az erősen lúgossá vált patak vizében bizonyosan minden élet elpusztult. A katasztrófa színhelyén mért magas pH érték nagyságrenddel meghaladja a tolerálható szintet, vagyis körülbelül ezerszer lúgosabb volt a víz, mint amit a vízi szervezetek egyáltalán elviselnek.

Különös módon a katasztrófa sokkal szembeötlőbb jele, a vizeket ijesztően vörösre festő iszap károsító hatása kisebb a nátronlúgénál. Az iszap szárazanyagának jelentős részét vízben oldhatatlan fém-oxidok teszik ki, melyek közül is legnagyobb arányban a vörös színért felelős vas(III)-oxid van jelen. Ez nem tekinthető mérgezőnek, bár a tömény iszappal terhelt vizek nyilvánvalóan felborítják a biológiai egyensúlyt, hiszen a sötét vízben leállnak a fotoszintézis

folyamatai. Az igen apró részecskékből álló iszap az állatvilágra is veszélyes, mert életfontosságú szerveket tömhet el. Amikor a szennyezés teljes mértékben levonul a folyókon, és a vörösiszap utánpótlása is megszűnik, a folyók regenerációja lassan megkezdődhet. [8]

MIKRÓBÁK JELENTŐSÉGE AZ ÉLŐVIZEKBEN

A felszíni vizek nem tartalmaznak kórokozó baktériumokat, azonban a háztartási szennyvizekkel kórokozó, patogén baktériumok is kerülhetnek a vizekbe. Ha ezek a kutakba vagy vezetékes vízellátásba kerülnek, közegészségügyi ártalmakhoz, járványokhoz vezetnek. A kórokozó mikrobák meghatározása alkalmasan megválasztott (steril) táptalajon történő tenyésztéssel valósítható meg. Ez azonban nagyon időigényes, illetve a kis baktériumszám esetén a kitenyésztés valószínűsége csak a feldolgozásra kerülő víz mennyiségével (esetleg 5-10 liter) növelhető. [1]

A baktériumok igazi indikátorok: jól jelzik a vízminőség változását. Szerves és szervetlen anyagokból építik fel sejtanyagaikat, vannak aerob fajok és anaerob fajok is. Az élővizekben jelenlevő baktériumok a rendszer tisztulási képességét is jellemzik. A baktériumok és a rendszerben jelen lévő többi mikroorganizmus nagyon szoros kölcsönhatásban vannak egymással. A rendkívül szoros és összetett hatás felelős a vízi környezetben bekövetkező változásokért. [14]

Jelen kutatásban azért is esett a választásom a Coliform, E.coli, illetve Pseudomonas aeruginosa vizsgálatára, hiszen a vízben való előfordulásukból számos további információt megkaphatunk.

A vizek fertőzöttségére a fekális szennyezést jelző és biztonságosan kimutatható kóli baktériumok (pl. Escherichia coli) meghatározása nyújt általános tájékoztatást. Ezek a baktériumok ugyanis megtalálhatók az ember és állatok bélcsatornájában, ahol az aerob, fakultatív anaerob normál baktériumflóra részét képezik, s nélkülözhetetlenek az emésztéshez. A szervezetbe a születéskor és az azt követő napokban, hetekben, szájon át jutnak be, s telepszenek meg elsősorban a vastagbelekben. Az E.coli törzsek nagy része ártalmatlan, de néhány törzs patogén és hasmenéses megbetegedést okoz. Ezeket a törzseket speciális csoportokba sorolják virulencia tulajdonságaik, patogenitásuk mechanizmusa, az okozott klinikai tünetek és O:H szerocsoportjaik alapján. A bélcsatorna megbetegedésein kívül két jellegzetes kórképet okozhatnak még a patogén E.coli törzsek. Újszülöttekben, csecsemőkben súlyos, gyakran halálos agyhártyagyulladás tényezői bizonyos tokos (K-antigént hordozó) törzsek. Felnőttekben viszont az E. coli okozta húgyúti fertőzések száma tízszeresen is nagyobb lehet, mint az enterális megbetegedéseké. [15]

A betegség egyéb, jellemző tünetei a hasi görcsök, hirtelen fellépő vizes hasmenés, amely esetenként véres is lehet, valamint néha felléphet hányinger, hányás és láz is. A legtöbb beteg egy-két héten belül meggyógyul, de a fertőzés okozhat vérzéses vastagbélgyulladást (hemorrágiás kólitisz), vérzékenységgel és vérrögképződéssel járó ún. trombotikus trombocytopéniás purpurát (TTP), vagy vesekárosodást, úgynevezett hemolitikus urémiás szindrómát (HUS) is, mely során a vérerek károsodása következik be. Ez a szövődmény a korábbi járványokban a fertőzöttek kb. 10 %-ában alakult ki, és elsősorban a gyermekeket veszélyeztette. [15]

Bár az Escherichia coli önmagában is lehet kórokozó, azonban általában nem maga a baktérium jelent egészség kockázatot, hanem megjelenése a vízben azt jelenti, hogy a kérdéses víz a közelmúltban valamilyen módon fekáliával szennyeződött. Ilyenkor megkísérlik az egyes betegségeket (hastífusz, kolera, dizentéria) okozó baktériumokat is kitenyészteni. A vizet a kóli-liter vagy a kóliszám alapján minősítik. A kóli- liter az a legkisebb vízmennyiség ml-ben, amelyből a kóli baktérium kitenyészthető. Ha 1 kólibaktérium található 100 ml vízben, akkor a víz tiszta, ha 10 ml-ben, akkor elég tiszta, ha 1 ml-ben, akkor gyanús, ha 0,1 ml-ben, akkor szennyezett, használatra alkalmatlan. A kóliszám a 100 ml vízből kitenyészthető

baktériumtelepek száma. Emellett szokásos még az 1 ml vízmintából 20 és 37°C-on tenyésztett baktériumszám meghatározása is. [15]

A kóliform baktériumoknak nevezzük az Enterobakteriaceae családnak a laktózt 30 °C hőmérsékleten bontó nemzetségeit (Klebsiella, Enterobacter, Citrobacter, Escherichia) melyek az állatok és az ember normál bélflórájának tagjai, ahol lényeges a vitamintermelésük és a kórokozó mikrobák antagonizálása, ezért élelmiszerekben való előfordulásuk esetén bélsár kontamináció lehetősége vetődik fel. [16]

A Coliform baktériumok megtalálhatóak a vizes élőhelyeken, a talajban és a növényzeten; és általában nagy számban vannak jelen a melegvérű állatok székletében. Míg ezek a baktériumok önmagukban általában nem okoznak súlyos betegséget, könnyen kitenyészthetők és a jelenlétük azt jelzi, hogy más, ürülékből származó kórokozók is jelen lehetnek. A coliform baktériumok az emberi szervezetbe kerülve hasmenést, hányást okoznak. Az E.coli ezek mellett okozhat még húgyúti fertőzést, epeúti fertőzést, illetve igen ritkán hashártya-gyulladást, tüdőgyulladást és csecsemőknél meningitiszt is. A Coliform baktérium elsősorban az általános bakteriális szennyezettség fokmérője. [17] [18]

A P. aeruginosa megtalálható a természetes vizekben, szennyvizekben, emberek, állatok bőrén is. Emberben bőrsérülésekhez, égéshez társuló fertőzéseket, kötőhártya-gyulladást (szennyezett úszómedencék, természetes vizek), közép- és belsőfül-gyulladást, csecsemőkben bélgyulladást, vérmérgezést okoz.

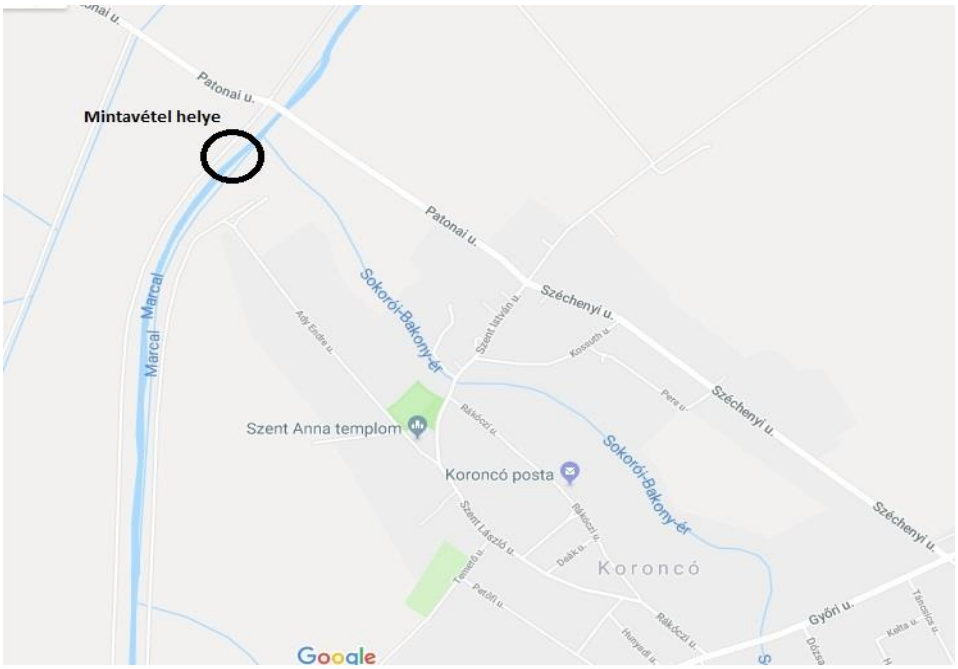
Jóllehet tipikus opportunista kórokozó[1], nagyszámú virulenciafaktora lehetővé teszi, hogy gyakorlatilag bármilyen szervet megfertőzzön kihasználva a védekező rendszerben lévő legkisebb lokális vagy szisztémás zavart is. A fertőzések forrása általában a környezet, tárgyak, de lehet a beteg saját flórája is. A fertőzés behatolási kapuja gyermekekben leginkább a bőr és az emésztőrendszer, idősekben a húgyutak. Sérülésekkel, elsősorban égések során jelentős fertőzés keletkezhet. Ritkábbak, de súlyos lefolyásúak lehetnek a szemfertőzések, fülfertőzések, szívbelhártya-gyulladás, agyhártyagyulladás. Pseudomonas aeruginosa-fertőzésre hajlamosító tényezők közül a következők a fontosabbak: előzetes, illetve ismételt antibiotikum-kezelés; párás, meleg, nedves környezet; csökkent immunitású állapotok. [19]

MINTAVÉTEL, ALKALMAZOTT VIZSGÁLATI MÓDSZEREK

A vörösiszap katasztrófának súlyos környezetkárosító hatásai voltak, melyek többek között a Marcal folyónál is jelentkeztek. Mint ahogy már korábban is említettem, az erősen lúgos vörösiszap szinte a teljes élővilágot kipusztította a folyóból. A magas pH hatására nem csak az állatvilág, hanem a mikroorganizmusok is elpusztultak.

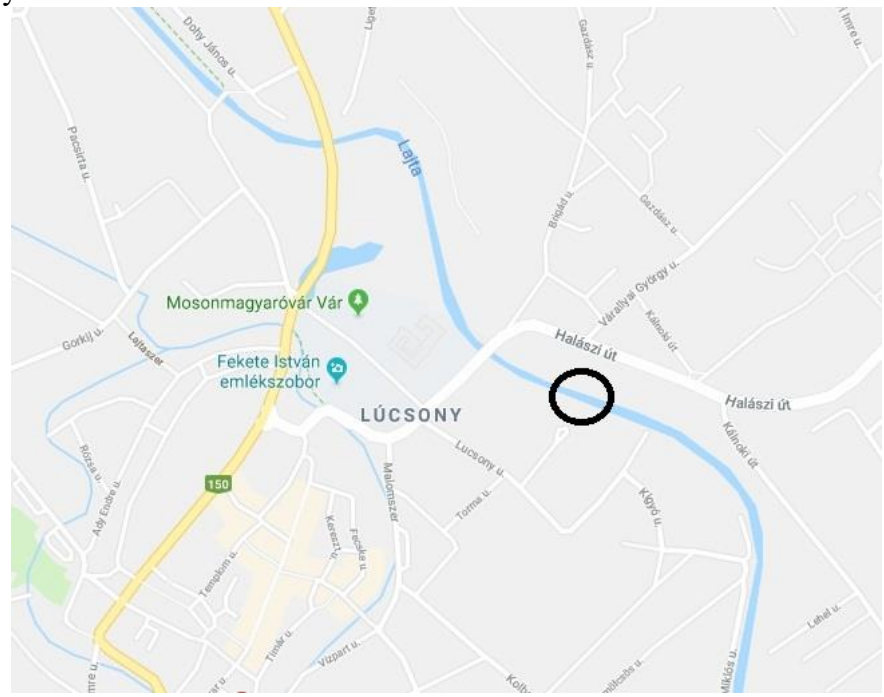
A fent említett feltételezéseket alapul véve, miszerint a folyók öntisztulása a katasztrófát követően megvalósul, mintákat vettem a vörösiszap szennyezéssel érintett Marcal folyóból. A mintavételezéssel az volt a célom, hogy felmérjem a folyó állapotát a katasztrófa után 7 évvel. A 2017-os évben 4 mintavétel történt, februárban, májusban, júliusban és októberben. A mintákat a Győrtől nem messze fekvő Koroncó településnél vettem le, ugyanis ennek határában húzódik a Marcal folyó. A vízmintákat, ahogy az 1. ábrán is látható, még a Marcal és a Sokorói-Bakony-ér torkolata előtt vettem a Marcalból.

[1] Az egészséges immunrendszerrel rendelkező szervezetben gyakran természetesen előfordul, de csak igen ritkán, illetve enyhe lefolyású betegségeket okoz, immunhiányos állapotban súlyos, gyakran végzetes kórfolyamot indíthat el. Ezt nevezzük opportunista fertőzésnek.



1.ábra Mintavétel helye a Marcal folyónál (forrás: Google Maps, a szerző kiegészítésével)

Összehasonlításként a Mosonmagyaróvár térségében található Lajta folyóból is vettem mintákat ugyanazokban az időpontokban, mint a Marcal esetében. A választásom azért a Lajta folyóra esett, mert hasonló vízhozamú és paraméterű folyó, mint a Marcal. A Lajtából való mintavétel helye a 2. ábrán látható.



2.ábra Mintavétel helye a Lajta folyónál (forrás: Google Maps a szerző kiegészítésével)

A mintavétel idején megmértem a víz és a levegő hőmérsékletét is. A vízminták steril üvegbe kerültek, melyeket a lehető leggyorsabban eljuttattam a vizsgáló laboratóriumba. A mikrobiológiai vizsgálatokat a Pannon-Víz Zrt. akkreditált Minőségvizsgáló Laboratóriumában végeztem el a labor munkatársainak közreműködésével. Minden egyes mintavételi időpontban 3 párhuzamossal és 2 ismétléssel dolgoztunk a hiteles eredmények elérése érdekében. Az egyes

mintáknál Coliform, E.coli, illetve Pseudomonas aeruginosa tartalmat vizsgáltunk, ezen kívül megmértük a pH-t is.

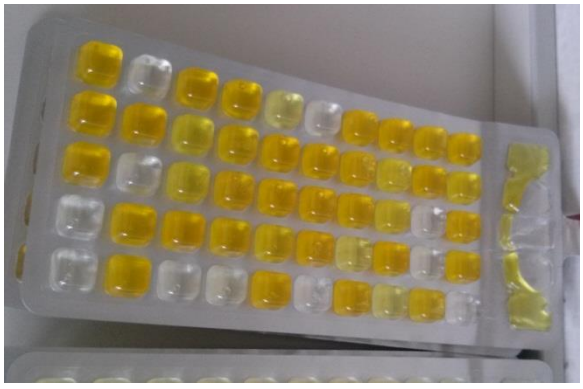
Az alkalmazandó módszerek kiválasztásánál talán az idő játssza a legnagyobb szerepet. Nem mindegy ugyanis, hogy például egy hirtelen bekövetkezett katasztrófahelyzetben, egy esetleges vízszennyezés során milyen hamar tudjuk kimutatni a szennyező anyagokat a vízből. A kémiai szennyezők kimutatásánál valamivel egyszerűbb a helyzet, ugyanis számos gyorstesztet fejlesztettek ki, amivel percek alatt megkaphatjuk az eredményt. Ilyenek például a nitrit, nitrát, foszfát, kálium, klór, vas, réz kimutatására szolgáló tesztek, ahol leggyakrabban egy tesztcsíkot kell a vízbe belemeríteni és a kialakuló színt összehasonlítva a színskála valamelyik színével megkapjuk az eredményt. Ezek persze csak tájékoztató jellegű adatok, később szükséges lehet más laboratóriumi módszerekkel megerősíteni az eredményt. Azonban a gyorstesztek tökéletesen alkalmasak arra, hogy nevükből adódóan is gyorsan, rövid idő alatt eredményt szolgáltassanak, és mihamarabb megkezdődhessen a szennyező anyagok inaktiválása.

A mikrobiológiai módszereknél már nem ilyen egyszerű a helyzet, ugyanis a mikrobák szaporodásához, kifejlődéséhez idő kell. Valamilyen szinten fel lehet gyorsítani a kimutatásukat megfelelő, dúsított tápközeggel, de ezzel sem tudunk elérni azonnali eredményt.

Jelen vizsgálatok elvégzésénél nem a hagyományos tenyésztéses eljárásokat alkalmaztuk, hiszen azok mind a Coliform, E.coli, illetve Pseudomonas esetében minimum 72 órás inkubálási időt igényeltek volna, s csak ezután tudtuk volna telepszámlálásos módszerrel megadni az eredményt.

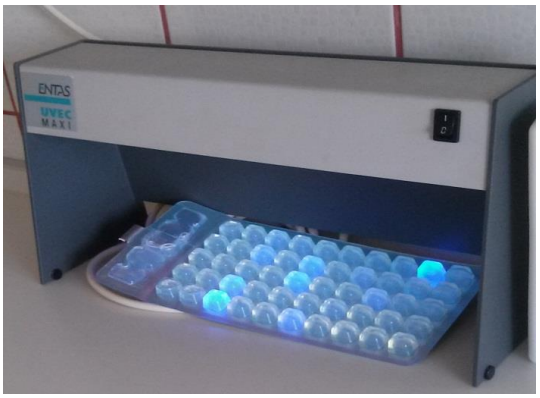
A levett mintáknál egy újabb vizsgálati módszert alkalmaztunk. A Coliform és az E.coli kimutatása Colilert 18 módszerrel történt, amikor is a vízmintából meghatározott mennyiséget pipettáztunk egy üvegbe majd adtunk hozzá steril vizet, illetve Colilert reagenst, mely különböző sókat, vitaminokat, cukrokat tartalmaz. Mindezt beletöltöttük egy tasakba, amit lezárás után 36°C-on 20 órán át inkubáltunk. A Coliform pozitivitást, ahogy az 1. képen is látszik, a sárga cellák jelzik.

A Coliform kimutatásánál a Colilert 18 módszer az orto-nitrofenil-β-D-galaktopiranosid (ONPG) ß-galaktozidázzal történő enzimatikus bontásán alapszik. Az emzimaktivitás eredményeként a minta színtelenről sárgára változik. Az eljárás UV megvilágítást nem igényel. [20]



1.kép Coliform mimutatása Colilert módszerrel (Forrás: saját készítés)

Az E.coli esetében azonban a 4-metil-umbelliferil-β-D-glükuronid (MUG) ß-glükuronidázzal történő enzimatikus bontásán alapszik. Az emzimaktivitás eredményeként a minta coliform pozitív, sárga buborékjai közül az E. coli pozitívok UV megvilágítás alatt kéken fluoreszkálnak. [20] A színes cellák száma alapján MPN módszer segítségével, egy statisztikai táblázatból kiolvasható az eredmény. A vízminta mennyiségétől függően az eredményeket 1,10,50 vagy 100 ml-re adtam meg.



2.kép E.coli mimutatása Colilert módszerrel (Forrás: saját készítés)

A Pseudomonas aeruginosa kimutatása Pseudalert módszerrel történt, mely hasonló elven működik, mint a fent említett Colilert. 38°C-on 24 órán keresztül inkubáltuk a tasakokat, majd utána megszámoltuk az UV fény hatására kék színnel fluoreszkáló pozitív buborékokat. Az eredményt pedig szintén MPN módszerrel adtam meg. [20]

A Colilert és Pseudalert módszerek hazánkban még nem elterjedtek, ugyanis meglehetősen drágák, viszont nagy előnyük a hagyományos tenyésztéses módszerekkel szemben, hogy lényegesen rövidebb idő alatt kapunk eredményt. Ezekkel az eljárásokkal 1 napon belül kiértékelhetjük az eredményeket, míg a széles körben használt tenyésztéses módszereknél az inkubálási idő ennél jóval több időt vesz igénybe.

A pH méréseket a WTW Multi 3430 gyártmányú Sen Tix 940-3 típusú hitelesített mérővel végeztem.

EREDMÉNYEK ÉS ÉRTÉKELÉSÜK

Jelen tanulmányban a 2017-es évben általam levett vízminták vizsgálati eredményeit mutatom be. 8 darab mintavétel történt a Marcal, illetve a Lajta folyóból. Megmértem a minták pH értékeit, illetve az egyes mintavételek idején a levegő és a víz hőmérsékletét is. Az átlagértékeket az 1. táblázatban láthatjuk.

Vizsgálat ideje	**Marcal**			
	pH	levegő hőmérséklete °C	víz hőmérséklete °C	vízállás (cm)
2017.01.09.	8,01	3	2,4	80
2017.02.13.	7,94	5	3,1	86
2017.03.22.	8,05	12	8,2	112
2017.05.16.	8,06	15	11,2	90
2017.07.17.	8,08	31	22,3	91
2017.09.04.	8,12	22	18,1	89
2017.10.31.	8,26	19	15,2	106
2017.12.11.	8,15	4	3,2	134

3. táblázat Marcal folyó vizsgálati értékei
(Összeállítva a saját vizsgálatok eredményei alapján)

Vizsgálat ideje	Lajta			
	pH	levegő hőmérséklete °C	víz hőmérséklete °C	vízállás (cm)
2017.01.09.	7,98	2	2,1	96
2017.02.13.	8,05	5	3,2	105
2017.03.22.	8,01	10	7,6	162
2017.05.16.	8,06	15	10,5	86
2017.07.17.	8,08	31	21,5	61
2017.09.04.	8,16	23	16,3	70
2017.10.31.	8,26	19	14,6	92
2017.12.11.	8,07	3	2,8	108

4. táblázat Lajta folyó vizsgálati értékei
(Összeállítva a saját vizsgálatok eredményei alapján)

Az elemzések alapján kijelenthető, hogy mind a két folyó pH értéke közel azonos a mintavételi időpontokban. A vörösiszap katasztrófa idején 13-nál magasabb értékeket is mértek a Marcalból, azonban ennek nyoma már nem észlelhető a folyónál.

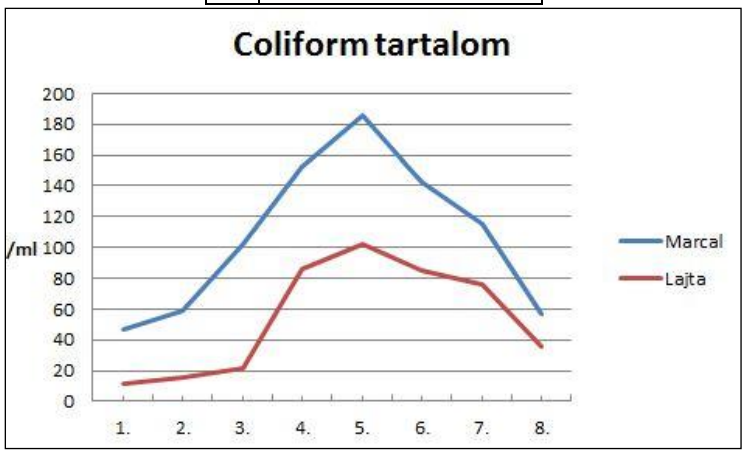
A mintavételi időpontokhoz hozzárendeltem a folyók vízállását is, melyhez a Belügyminisztérium Vízügyi Főigazgatóság, Vízügyi Honlapján megtalálható naprakész adatbázisa nyújtott segítséget. A csapadékosabb hónapokban, illetve hóolvadás idején értelemszerűen a folyók vízszintje is megemelkedik, a Lajta folyó esetében pedig 2017. március 20-22-ig I. fokú árvízvédelmi készültségi fokozatot rendeltek el a magas vízállás miatt. Ilyen esetekben az árvíz- és a belvízvédekezésről szóló 10/1997. (VII.17.) KHVM rendelet 13. § alapján az I. fokú készültség ideje alatt 12 órás nappali őrszolgálatot kell tartani, és a vízállásokat naponta meghatározott időközönként le kell olvasni, illetve jelenteni kell. [8]

A hóolvadás, illetve a hirtelen lezúduló csapadék a mikroorganizmusok számában is változást eredményezhet, hiszen ilyen esetekben a vízfolyás környezetéből, a talajból számos baktérium mosódhat bele a folyó vizébe. Mindezen tényezőkkel normál vízállás idején kell számolni, aszálykor nem.

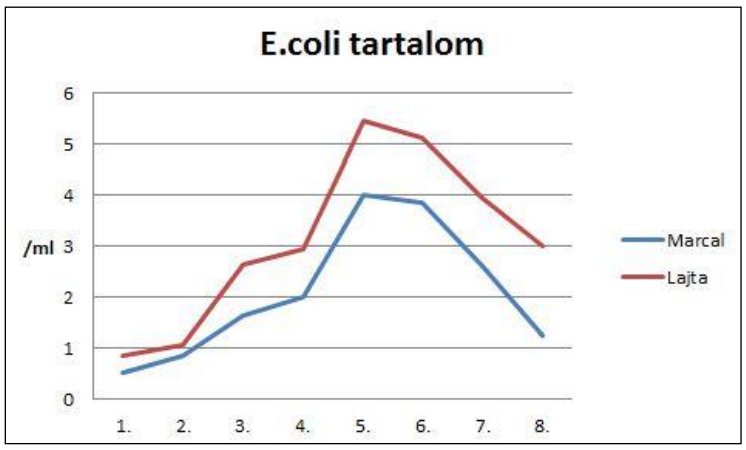
A mintákból mikrobiológiai paraméterek is vizsgáltam, melyek eredményei a következő ábrákon láthatóak.

Mintavételi időpontok:

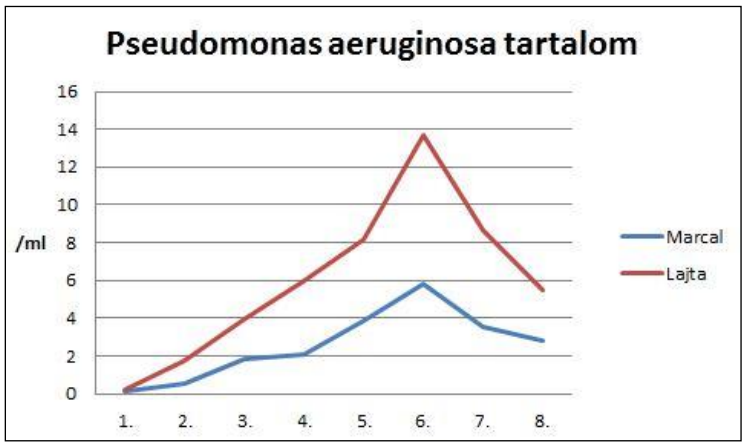
1.	2017. január 9.
2.	2017. február 13.
3.	2017. március 22.
4.	2017. május 16.
5.	2017. július 17.
6.	2017. szeptember 04.
7.	2017. október 31.
8.	2017. december 11.



3. ábra Marcal és Lajta folyó Coliform tartalma
(Összeállítva a saját vizsgálatok eredményei alapján)



4 ábra Marcal és Lajta folyó E.coli tartalma
(Összeállítva a saját vizsgálatok eredményei alapján)



5.ábra Marcal és Lajta folyó Pseudomonas aeruginosa tartalma
(Összeállítva a saját vizsgálatok eredményei alapján)

Összességében elmondható mind a Coliform, E.coli és Pseudomonas vonatkozásában, hogy a két folyó esetén hasonló tendenciát kaptam a mikrobák számát illetően. A melegebb hónapokban, illetve amikor már a folyók vize is felmelegedett, a mikroorganizmusok száma is megnövekedett. A téli, hidegebb időszakban a mikroorganizmusok számának csökkenése volt tapasztalható.

Mindenképp meg kell említeni, hogy ezek a vizsgálatok nem voltak teljes körűek, csak néhány paramétert emeltem ki a sok közül, amit vizsgáltam, viszont ezek megfelelő kiindulási alapot képeztek az összefüggések megállapításához.

A vizsgált paraméterek alapján az mindenképp kijelenthető, hogy a várakozásainknak megfelelően a Marcal folyó már nem mutatja a katasztrófa következtében kialakult negatív tulajdonságokat. A pH értékek és a mikrobiológiai jellemzők alapján egy teljesen „hétköznapi" folyóról beszélhetünk, amelynek sikerült kihevernie a vörösiszap katasztrófa súlyos környezetkárosító hatásait.

KÖVETKEZTETÉSEK

Hazánk eddigi legsúlyosabb ipari katasztrófája rávilágított arra, hogy mennyire sebezhető a környezet. A vörösiszap katasztrófa amellett, hogy emberéleteket is követelt, a környezetet is súlyosan károsította. A Marcal folyó élővilága szinte teljesen kipusztult.

A vizsgált paraméterek alapján azt elmondhatjuk, hogy a Marcal folyó esetében teljesen átlagos adatokat kaptam. Mindehhez persze hozzájárult az is, hogy a katasztrófa óta már eltelt 7 év, így a folyónak volt ideje a regenerálódásra. A vörösiszap katasztrófa jelentős ökológiai károkat okozott, de a gyors és példaértékű összefogás, a hatékony mentesítési beavatkozások a regeneráló folyamatokat felgyorsították, melynek következtében a folyó élővilága is újjáéledt.

ÖSSZEGZÉS

Írásomban bemutattam a kémiai biztonság fogalmát az erre vonatkozó jogszabállyal együtt. Ehhez kapcsolódóan megemlítettem az iparbiztonság jelentőségét is, melynek egyik fő feladata a veszélyes üzemek felügyelete.

Ezen kívül bemutattam a vörösiszap összetételét, röviden ismertettem a katasztrófa súlyos környezetkárosító hatásait, ami többek között a Marcal folyót is érintette. Kíváncsi voltam a Marcal jelenlegi állapotára is, ezért vizsgálatokat végeztem el, melyek eredményeit a Lajta folyó eredményivel vetettem össze. Térképen ábrázolva bemutattam a mintavételi helyeket, a mintavétel gyakoriságát, illetve az elvégzett vizsgálatok módszereit is.

Egy éven keresztül, több mintavételi időpontban vizsgáltam a két folyó egyes bakteriológiai jellemzőit, illetve a pH-t. Mindezek mellett feltüntettem a folyók vízállását, melyek hatással voltak a mikrobiológiai állapotra is.

FELHASZNÁLT IRODALOM

[1] FÖLDI L., HALÁSZ L.: Környezetbiztonság, ISSN 2060-8047. Complex Kiadó Kft. Budapest, 2009

[2] KÁTAI-URBÁN L.: Súlyos Ipari balesetek megelőzését és a felkészülést célzó jogintézmények egységes rendszerbe foglalása. Hadmérnök, IX 4 (2014), 94-105.

[3] 2000. évi XXV. törvény a kémiai biztonságról

[4] KUTI R.: Vegyimentesítőhely kialakításának követelményei, az eljárás személyi és technikai feltételei, Védelem- Katasztrófa- Tűz- És Polgári Védelmi Szemle XVIII.1. (2011) 27-30. p.

[5] KUTI R., NAGY Zs.: Veszélyes anyag baleseteket követő vegyimentesítés eszközeinek optimalizálása, Műszaki Katonai Közlöny XXVII. 4. (2017) 80-89. p. http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2017_4sz/2017_4sz.pdf (Letöltés ideje: 2017. 11. 20.)

[6] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

[7] KÁTAI-URBÁN L. (szerk.): Iparbiztonságtan I.: Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához. Nemzeti Közszolgálati és Tankönyvkiadó, 2013.

[8] BELÜGYMINISZTÉRIUM ORSZÁGOS KATASZTRÓFAVÉDELMI FŐIGAZGATÓSÁG honlapja: http://www.katasztrofavedelem.hu/index2.php?pageid=lakossag_kolontar_vorosiszap (Letöltés ideje: 2016.10.08.)

[9] ÁLLAMI NÉPEGÉSZSÉGÜGYI ÉS TISZTIORVOSI SZOLGÁLAT Országos Tisztiorvosi Hivatal Kommunikációs Főosztály Közlemény, 2010. http://www.katasztrofavedelem.hu/letoltes/lakossag/antsz_vorosiszap_info.pdf (Letöltés ideje: 2016.09.15.)

[10] SCHWITZER F.: Katasztrófák tanulságai, stratégiai jellegű természetföldrajzi kutatások. Magyar Tudományos Akadémia, 2011.

[11] VÁGFÖLDI Z.: A vörösiszap katasztrófa környezeti hatásai, kárelhárítási folyamata, alkalmazott módszerei. Hadmérnök VI. 1. (2011) 261-275.

[12] Ajkai Vörösiszap-katasztrófa: https://hu.wikipedia.org/wiki/Ajkai_v%C3%B6r%C3%B6siszap-katasztr%C3%B3fa (Letöltés ideje: 2017.09.27.)

[13] BÍRÓ R. és mtsi.: A Torna-patak bevonatalkotó kovaalgáinak kolonizációja a vörösiszap katasztrófa után. Magyar Hidrológiai Társaság XXX. Országos Vándorgyűlése. (2011) 1-9.o. http://apps.arcanum.hu/app/hidrologia/view/HidrologiaiVandorgyules_2012_30/?pg=1117&layout=s (Letöltés ideje: 2017.11.05.)

[14] BALLAGÓ Gy.: Katasztrófák- életünk részei, Vörösiszap katasztrófa. Védelem Tudomány. (2014) 0-40.o. http://www.vedelem.hu/letoltes/anyagok/485-katasztrofak-eletunk-reszei-vorosiszap-katasztrofa.pdf (Letöltés ideje: 2017.02.15.)

[15] DEÁK T.: Élelmiszer- Mikrobiológia. Mezőgazda Kiadó. 2006. 382.o.

[16] BÍRÓ G.: Élelmiszer-higiénia. Agroinform Kiadó. 2014. 668.o.

[17] ÁLLAMI ÉS NÉPEGÉSZSÉGÜGYI ÉS TISZTIORVOSI SZOLGÁLAT: Magyarország ivóvízminőségi rendszere, 2011. http://oki.antsz.hu/files/dokumentumtar/ivoviz-minoseg-2011.pdf (letöltve: 2017.04.12.)

[18] ORSZÁGOS KÖZEGÉSZSÉGÜGYI KÖZPONT: Ivóvíz kiskáté, lakossági tájékoztató a gyakran ismételt kérdésekről, 2016. http://oki.antsz.hu/files/dokumentumtar/kiskate-2016-03.pdf (letöltés ideje: 2017.04.05.)

[19] PÁL T.: Orvosi mikrobiológia tankönyve. Medicinia Könyvkiadó Zrt. 2012. 544. o.

[20] RESKÓNÉ DR. NAGY M., DÖMÖTÖR Sz.: Gyors vizsgálati módszerek a víz mikrobiológiai ellenőrzésében. Hungalimentaria- Budapest, 2015. http://www.hungalimentaria.hu/Portals/0/doksik/2015%20El%C5%91ad%C3%A1sok/mikrobi/mikrob_Gyors_vizsgalati_modszerek_a_viz_mikrobiologiai_ellenorzeseben_Reskone_Dr._Nagy_Maria_WESSLING.pdf (Letöltés ideje: 2016.02.16.)

[21] BELÜGYMINISZTÉRIUM VÍZÜGYI FŐIGAZGATÓSÁG, Vízügyi Honlap: http://edukovizig.hu/map/layout.html (Letöltés ideje: 2017.12.28.)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

THE COMPLEXITY AND METHODS OF CITIZEN EMERGENCY PREPAREDNESS

A LAKOSSÁG VESZÉLYHELYZETI FELKÉSZÍTÉSÉNEK KOMPLEXITÁSA, MÓDSZEREI

TEKNŐS László

(ORCID ID: 0000-0003-0759-5871)

teknos.laszlo@uni-nke.hu

Abstract

Every citizen has the right to know the dangers in his/her surroundings, to master the applicable rules of protection and behavioral norms. He/she has the right and the duty to contribute to disaster relief also. This involves as well as requires public hazard education and real-time public hazard communication. Education and communication can save lives. Before, during and after the damage event, the population must be provided with information, guidance, moreover, its interpretation and effective implementation has to be educated.

In this publication, the author attempts to present the current inquiries and information gathering methods. Taking into account the legal background, he analyzes the basic requirements and rules of domestic hazard education in prevention, preparation, defense (intervention), restitution and reconstruction periods. He gives suggestions to enhance current content of methods for improving the population's self-rescue skills and for improving public hazard education.

„The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in István Egyed Postdoctoral Program."

Keywords: *disaster management, public hazard education, disaster management cycle, social media*

Absztrakt

Minden állampolgárnak joga van arra, hogy megismerje a környezetében lévő veszélyeket, elsajátítsa az irányadó védekezési szabályokat, magatartási normákat. Joga és kötelessége, hogy közreműködjön a katasztrófák elleni védekezésben. Ez magában foglalja, illetve megköveteli az állampolgárok felkészítését és a valós idejű tájékoztatását. A felkészítés, tájékoztatás életet menthet. Egy káresemény bekövetkezte előtt, alatt, után, a lakosságot információkkal, útmutatásokkal kell ellátni, azok értelmezésére és eredményes végrehajtására fel kell őket készíteni.

Szerző jelen publikációban kísérletet tesz arra, hogy bemutassa a jelenkori tájékozódási igényeket és információszerzési módszereket. Elemezze a jogszabályi háttér figyelembe vételével a hazai lakosságfelkészítés alapkövetelményeit, szabályait a megelőzési, felkészülési, védekezési (beavatkozási), helyreállítási-újjáépítési időszakokban. Javaslatot tegyen a társadalom önmentési képességeit növelő, lakosságfelkészítői módszerek aktuális tartalmainak bővítésére.

Kulcsszavak: *katasztrófavédelem, lakosságfelkészítés, tájékoztatás, katasztrófa-menedzsment ciklus, közösségi média.*

A kézirat benyújtásának dátuma (Date of the submission): 2018.07.02.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.24.

INTRODUCTION

Every citizen has the right to know the dangers in his/her surroundings, to master the applicable rules of protection and behavioral norms. He/she has the right and the duty to contribute to disaster relief also. This involves as well as requires public hazard education and real-time public hazard communication. Education and communication can save lives. Before, during and after the damage event, the population must be provided with information, guidance, moreover, its interpretation and effective implementation has to be educated.

In this publication, the author attempts to present the current inquiries and information gathering methods. Taking into account the legal background, he analyzes the basic requirements and rules of domestic hazard education in prevention, preparation, defense (intervention), restitution and reconstruction periods. He gives suggestions to enhance current content of methods for improving the population's self-rescue skills and for improving public hazard education.

LOCATION OF PUBLIC HAZARD EDUCATION IN DISASTER MANAGEMENT CYCLE

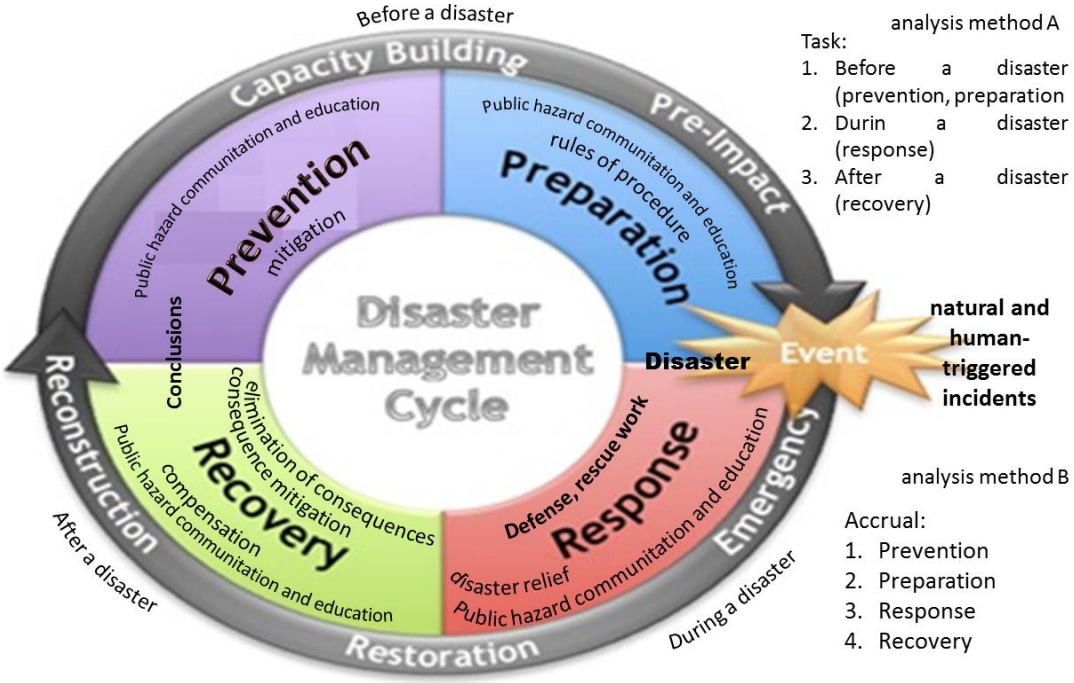


Figure 1 Time cycle of disaster management
(Created by László Teknős, 2018)

On figure 1, time cycle of disaster management can be seen. The circle process can be divided into four phases. The first one is the prevention, which means reducing the likelihood of causes of disasters; this is the main period for hazard education and hazard communication. Furthermore, the conditions of other phases are prepared here. Since impacts, emergencies and injuries cannot be prevented, public hazard education appears as a preventive principle, but in a separate phase. This will be the connection between prevention and response (reaction).

Public hazard education is a complex activity, which is, on the one hand, an activity system that includes the public education for emergencies, which includes the rules of action and

conducts to be followed, the suitability for self-rescue to save people and material goods, and through well-directed exercise, improving the knowledge to its skill level. On the other hand, it is to be aware that population can cause emergencies if it is careless or it is lacking of knowledge. The purpose of this activity is to establish a safety culture and to create self-defense attitude. The main objective of public hazard education is to present the most dangerous threats of local areas and to make the most commonly known behavioral norms to be followed in case of emergency.[1] [1]

The national disaster management task system can be divided into three parts, such as prevention, protection and reconstruction. According to the author, public hazard education and communication should be an integral part of each period, but due to its complex system of activities, legal regulation, interdisciplinary professional nature and significance, it is considered as a separate period. This is the fundamental societal self-protection mechanism of all cycles.

In most of the cases, the events reach only the lowest, the so-called daily activity threshold of the bodies involved in disaster management, therefore for the elimination process, the least-level response of organizations created for this purpose are sufficient. Continuous and strictly coordinated co-operation between local governments and public bodies is generally not necessary. For large-scale events (e. g. catastrophes), defense management actors are widely applied, with activation of higher management levels. This cycle already belongs to the defense-intervention period. Although there are home specialists who divide the national defense periods into three parts (normal period, disaster risk, special legal order), but according to the author, two additional elements can be added to disaster alarm levels based on the following.

During national defense, five periods are separated. These are (see Figure 2):

- regular operation - basic function, basic activity
- event occurred
- protracted event
- disaster risk–transition between regular period and special legal order
- emergency–special legal order

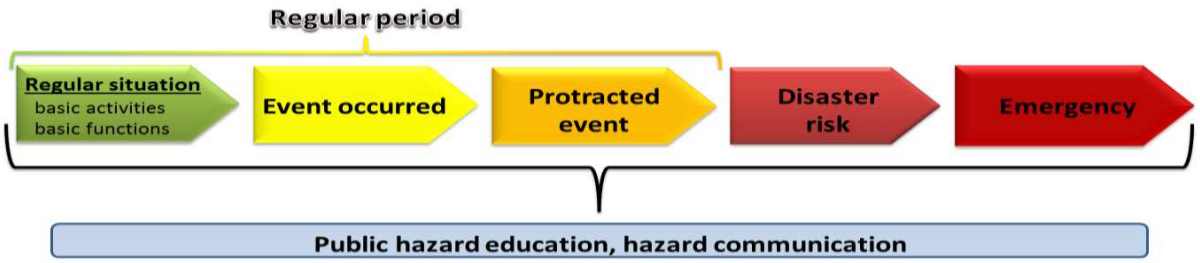


Figure 2: Determination of national defense periods in the aspects of disaster management (Created by László Teknős, 2018)

The fourth period involves the tasks of restoration and reconstruction, which means restoring the original conditions. There is a damage, a post-disaster situation where, after the

[1] Under the provisions of Act No. 62/2011 on certain rules for the protection from disasters, (XII.29.) Ministry of Interior Decree VI. chapter describes the requirements of disaster preparedness, the purpose of disaster preparedness and the preparation of civil protection organizations. The VII. Chapter describes disaster management education of administrative managers and participants in disaster response and national defence.

experiences have been deducted, new elements, methods and tasks are integrated into the prevention phase. This can be described as a circular process.

Overall, it can be stated that, as regards the time cycles of disaster management, the period of public hazard education is manifested as a separate element, mainly with regard to prevention-centric aspects and criteria, but it is also observed that public communication must appear in each period (see Figure 1) and in each defense method, (see Figure 2).

PUBLIC HAZARD EDUCATION IN THE DISASTER MANAGEMENT TASK SYSTEM

Professional disaster management was established on January 1, 2000 and was then reorganized in 2012 into an integrated national disaster management organization. This transformation was promoted by several new legislations. New legal regulations and government policies have imposed the need to strengthen preventive and administrative work, enhance responsiveness, and protect the lives, physical integrity and material benefits of the population. New legal regulations and government policies have demanded the need to strengthen preventive and administrative work, enhance responsiveness, and protect the lives, physical integrity and material benefits of the population. Civil protection is one of the most important tools and task systems for protecting the population.2

From the tasks of civil protection related to disaster management published in the act CXXVIII of 2011 on disaster management and amendments of related acts, according to the topic of present paper, the following should be highlighted:

- Public education about the normative behavioral rules during defense – section 52. a)
- Establishment and preparation of civil protection organizations – section 52. b)
- Communication, warning, alert – section 52. c)

Public education about normative behavioral rules during defense

According to section 1 (2) of the CXXVIII of 2011 on disaster management and amendments of related acts, every citizen and person has the right to know the disaster in his or her environment, to acquire the relevant protection rules, furthermore to have the right and duty to contribute to disaster relief. To be able to maintain these rights and duties, citizen should be prepared. Public hazard education should cover not only the population that is likely or in fact is at risk, but also those who get in contact with emergencies during their occupation (emergency preparedness). [2] It is important not only to know the rules of normative behavior during emergencies, but also to raise awareness of citizens in order to avoid by themselves the mechanisms of action that can cause further damage or even an emergency. The preparation can shape the population's view and way of thinking during preparing and the defense. People need to be taught and motivated by delivering the necessary knowledge, developing skills and providing resources in order to be able to defend themselves against disaster risk, furthermore to perform self-rescue during events as far as possible. [2]

[2] Civil protection: a system of overall social task and action systems designed to protect the lives of the population and to preserve living conditions in the event of disasters or armed conflicts, and prepare the population to overcome its effects and to create conditions for survival.

Figure 3 Residential information demonstrating normative behavioral rules
(Created by László Teknős, 2015)

Establishment and preparation of civil protection organizations

Detailed rules on preparation of civil protection organizations in the field of disaster prevention are set out in Interior Minister Decree no. 62/2011. (XII.29.). According to the legislation, the preparation takes place in theoretical and practical form. Theoretical training consists of basic training, 8 hours of professional training, vocational training and executive training.

<table>
<tr><th>Type</th><th>basic training</th><th>professional training</th><th>executive training</th></tr>
<tr><td rowspan="9">Content</td><td>basic elements of disaster management and civil protection system</td><td>the task of certain civil protection unit and organization</td><td>basic knowledge training</td></tr>
<tr><td>civil protection obligation, civil protection organization</td><td rowspan="2">the tasks to be carried out in their position, implementation and procedural order</td><td rowspan="2">knowledge required to carry out according to their position</td></tr>
<tr><td>rights and obligations related to civil protection</td></tr>
<tr><td>risk mitigation, risk assessment and risk management plans</td><td rowspan="3">the dependence of unit and organization, the order of management, report, command in units and in the organization</td><td>leadership theories</td></tr>
<tr><td>alert and communication, as well as bodies and organizations involved in the management and command</td><td rowspan="2">rules of application of civil protection organizations</td></tr>
<tr><td>civil protection tasks</td></tr>
<tr><td>bodies and organizations participating in defense,</td><td rowspan="2">specialized bodies and organizations, and</td></tr>
<tr><td>protective capital equipment, personal protective equipment</td></tr>
<tr><td colspan="2">labor and work safety</td></tr>
</table>

Table 1 Professional contents of basic training, professional training, leadership training
(Created by László Teknős, 2018)

Practical training of civil protection organizations involves the practical application of the skills acquired during the preparation process, the practice of operations of the rescue co-operation and the implementation and control of their temporal mobilization.

Communication, warning and alert

The Government Decree no. 234/2011 (XI. 10.) on the implementation of Act 2011 CXXVIII details the rules of communication, warning and alert.
Methods for public alert and public communication:

- first of all with notice of public interest, in accordance with the provisions of the act on media services and mass media,
- with the tools of the residential alarm system, [3]
- if technical conditions are available, using electronic communications services,
- in the usual way in place (voice announcer, messenger, wall stickers),
- other locally available fools which are applicable for alert and emergency communication, such as loudspeaker facilities for broadcasting of law enforcement agencies or individuals,
- simultaneously if it is required or possible.

Application order of alarm devices:

The public may be alerted by the alert system of disaster management, by engine syndicates, local alarm system, by electronic devices, by local authorities using local facilities, also by other alarm devices, as well as public service broadcasting, including radio and television stations.

At the case of emergency, radio is the most flexible, most-reachable medium; especially in a well-localized emergency, local radio plays an important role. At an early stage of emergency, the information service of the concerned population needs to be solved in close cooperation with official bodies, it has an important role in the later rehabilitation and in the re-launch of community's life.

Respondents in the area of public alert and emergency reporting work together to provide credible, accurate and prompt information, in which they coordinate the main areas of information, the streamlined flow of information, the population directly and indirectly affected, and international impacts.

At the case of emergency, it is necessary to indicate the occurrence of the event and its disappearance and to inform the population immediately about behavioral rules, the measures envisaged, their implementation and the emergency incident in order to prevent and mitigate threatening effects. [4] Depending on the available alert or information system, text messages or specific siren signals must be used to indicate the likely occurrence of the event or its outbreak, and to inform the public about the behavioral rules to be followed, after the assessment of the notifications, in the event of a disaster risk during the preparations and in the event of an emergency, in order to save the material goods necessary for human life and subsistence. [5]

For alarming the population, the current legislation defines two cases, such as disaster alarm [6] and air warning. [7] Ordering and unlocking the disaster response through broadcast transmitters – with 5 seconds interruption – is repeated three times.

The air warnings an alarming activity which is applied in the event of an unexpected air raid or its immediate danger to the country, the Hungarian Defense Forces, law enforcement agencies and other organizations involved in organized defense are applied, targeted

preventive defense of citizens and personal injury, damage prevention and reduction of damages.[3]

GENERAL PRESENTATION AND COMMON RULES OF PUBLIC HAZARD EDUCATION AND COMMUNICATION

Public hazard education is operated in three different periods (see Figure 1)

- prevention
- response
- recovery

In terms of temporality, the largest part of public hazard education can be related to the prevention period (since normally there are normal temporal events). Here, not only it is necessary to prepare the population for action mechanisms to be followed during an emergency event, but also to assist them in developing their self-defense skills and to be aware of how they can avoid the emergencies.

Suggested content of preventive preparation without the need for completeness:

- Awareness of types and characteristics of the threats (reasonable danger mapping), local dangers and prevention tasks, special phenomena (e. g. extreme weather).
- Consciousness, psychic preparation.
- Legal background, system and significance of disaster protection, responsibility of the citizen during the period of prevention, emergency management, and restoration, the civil protection obligation, establishment of civil protection organizations.
- Knowledge of alarm signs, the ways of informing, the possible ways and tasks of complex protection, the tasks of emergency management in a local context.
- The tasks of restoration, specifics, actualities, helping organizations, normative behavioral norms, etc.

Public hazard education is feasible with:

- Educational presentations, reports and evaluations
- Informative presentation of disaster protection devices
- Visiting Professional Firefighters' Commands, Disaster Management Guards
- Providing leaflets and brochures
- Publishing written and electronic media
- Announcing drawing contest
- Organizing disaster relief camps
- Disaster management youth competitions
- Disaster relief exhibitions
- Organizing competitions in educational institutions
- Disaster Response Population Preparatory Event with Joint Organizations
- own nationwide disaster relief preparatory event
- Educational exhibition
- Disaster relief demonstrations

[3] According to the section 6. B of Ministry of Interior Decree 16/2013. (V. 9.), professional disaster management organizations participate in the preparation and implementation of air warning during the performance of their defense tasks.

Public hazard education directly before the event

Provide targeted and specific knowledge of the perception of threats, the possibilities of defense, the use of methods, means of alerting and information, special organizations and their tasks, cooperation and enhancement of capacity.

In an emergency situation, information plays an important role. Delayed official information will worsen the chances of survival of the population and increase the likelihood of damage and human losses. Emergency communication can save people's lives and help reduce future damage. Emergency communication includes information which supports life and security of property. Interpreting the information with an interactive map is more easily "embedded" in the mind of the citizen, making it easier to memorize the information. In addition, visualization makes the raw text easier to understand. By providing an interactive map of the information leaflets, it is possible to support the people's willingness to rescue themselves. If you know where to go or to ensure your own and your family's safety, you will follow the requirements yourself and increase your chances of survival.

Article 34, section 1 of the Disaster Relief Act lists the methods of warning and alerting the public, among which the first is published in accordance with the provisions of the Public Communications Act, the Media Services Act and the Mass Media Act.

The article 32, section 6 of the Act CLXXXV of 2011 on Media Services and Mass Media and on the Law of the Media (Media Act) provides that public service broadcasters (including: m1, m2, Duna, Petőfi Rádió), the community and the highly influential media service provider (RTL Klub, TV2) body are obliged to share the announcements of the Disaster Management if it informs about the likely occurrence of events endangering or damaging to human life or property security, the mitigation of the consequences of such events already occurring, and the tasks to be performed. (...) The publishing obligation is also borne by the media service provider of a local media service operating in the broadcasting area of these events.

The rules for emergency information are set out in Government Decree no. 234/2011. (XI.10.) "On Disaster Management and the Amendment of Certain Legislation Related to CXXVIII. (1) of the Act on the Implementation of the Law on the Protection of the Rights of the Child, according to which the methods of alerting and warning the general public are as follows:

- Firstly, by publishing a public announcement, in accordance with the provisions of the Act 2010 CLXXXV. (6) on Media Services and Mass Media, if it is justified by the decision of the disaster management body and has been communicated in due time by the media service provider, the public service broadcaster shall publish its public broadcasting program. The obligation in this paragraph is also borne by the media service provider of the social media service. [8]
- With the tools of the residential alarm system.4
- In the case of technical conditions, application of electronic communications services.
- In usual way (voice announcer, messenger, wall stickers).

[4] Residential alarm system: residential alarm system, alarm notification, storm warning systems and the tools and equipment that are closely related to the operation of territorial organs of the professional disaster management body and is operated by it. These can be: residential alarm endpoint, residential alarm alert endpoint, storm endpoint, special endpoint. [9]

- With devices available for localization of alarms and emergency communication via other means, such as law enforcement agencies, loudspeaker devices for the broadcasting of individuals, and handheld hands-free devices
- If required and appropriate, simultaneous application of the previous points.

Personal requirements for hazard communication:

- Using more personal, more interactive methods of public communication.
- The communicators and announcers need to acquire appropriate behavior-psychological and sociological knowledge.
- It is necessary to assess and understand the behavioral-psychological, social-psychological and cultural-psychological characteristics typical of the locals.
- The organizers and executives possess the right knowledge and empathic behavior to effectively inform the vulnerable population.
- The operator must be an experienced, suggestive, confident, intelligible, relaxed person.
- Teaching methods for preparing communicators: training, vocational training.

In an emergency situation, hazard communicator officers cooperate to provide credible, accurate and prompt information, in which the main areas of information, the streamlined flow of information, the population directly and indirectly affected, and international impacts are coordinated. [6]

The Interior Minister Decree no. 62/2011. (XII.29.) "on certain rules of protection against disasters" IX. chapter describes that public hazard education for domestic population can be divided into two groups:

- Active hazard education
- Passive hazard education

	Active	**Passive**
period	• once a year in settlements qualified as I. disaster class • three times a year in settlements qualified as II. disaster class	The branch office shall hold an open public day at least once a year.
modes of implementation	• Issuance of brochures • Publication of information leaflets in local press, local government newspaper, county newspapers, local and regional television, cable television, local radio, and publication of internet information surfaces • By organizing residential forums • Other public events held in a settlement (town and village cap)	• A Providing accessible information for printers and electronically accessible information to those who are interested • Providing open day
content	• Preparing the population for detecting alarm methods and signals • Normative behavioral norms • Forms of assistance • Risks of natural and technological threatening the area • Possible ways of remedying hazards	• Content of communication during

Table 2: Groups of domestic public hazard education[5]

[5] In settlements where the national or ethnic minority reaches 5% of the total population or which is a tourist center, a part of the information leaflet issued or published in the form of active publicity have to contain alerts

Public hazard communication during emergencies

The Interior Minister Decree no. 234/2011. (XI. 10.) "on the disaster management and the related amendments to certain legislations of the act CXXVIII. 2011", article VII. section 34 (1) describes alerting methods and emergency communication.

Essential elements of public hazard communication: [10]

- Depending on available alert or information system, primarily by means of textual communication (in the public interest), in accordance with the provisions of the Act on Media Services and Mass Media, or with certain siren signals, the eventuality of the event must be indicated in order to save human lives and subsistence material (disaster alert), and promptly inform the general public about normative behavioral rules.
- The disaster risk, the emergency situation, event management, defense, normative behavioral rules, civil protection measures, ordered restrictions, and further information providing in the restoration period require further information.
- Other facilities include the use of residential alarm systems (residential alarm, alarm information, storm warning systems and devices and equipment connected to them), electronic communications services (with technical equipment) and traditional customary methods (loudspeakers, wall hangers, law enforcement agencies , the use of hands-free handsets, etc.).

Content of residential information sheet

The content of residential information sheet, which should be included in all information material based on different situations:

- Describe the situation
- Determining the population and area concerned
- Describe the rules to be introduced immediately (behavioral rules)
- Provision of protective equipment
- Relocation, evacuation and reception
- Related to the previous point: determining assembly locations, describing the contents of the evacuation packet
- Presentation of opportunities for getting closed
- Shelter protection (access, address)
- Define the location of personal defense
- Description of health regulations and insurance
- Reading administrative decisions (ordering public work, restricting traffic, etc.)

Further information should be kept in accordance with the order of defense, taking into account the evolution of events.

Public hazard communication after restitution

Restoration is a set of actions and activities to be carried out at the time of or after the elimination of damage, basically during the "restoration" period, which is to be carried out in order to reach or approach the state before the occurrence of a critical event and to determine responsibility, compensation and fact-finding tasks, allowing: [11]

---

and codes of conduct to be followed in minority language or has to be published in the world language. People with disabilities should be provided appropriate guides and aids.

- Eliminating the damage and consequences.
- Normalization of basic provision and public service providing the conditions of life.
- Re-establishing the conditions of practice of citizen's rights, human rights, and obligations laid down in the Hungarian Fundamental Law (to restore the situation in which citizens can exercise their rights).
- Collecting and summarizing experiences.

The "reorganization" of everyday life requires fast and accurate information flow, uniform handling of cases, coordinated activities, and how the population is prepared to do what to do in order to make recovery and reconstruction as soon as possible and with less losses. They have to know the losses, the degree of reversibility and irreversibility of processes. [12]

Elements of communication:

- Provision of damage, insurance data, information
- Sharing area information - road closures, relocation, etc.
- Ensuring the availability of authorities, municipalities, and other important bodies

The preparation activity of this period is only effective if the protective and restorative content framework of emergency preparedness has been developed in the preceding period.

ACTUAL METHODS OF PUBLIC HAZARD COMMUNICATION AND EDUCATION NOWADAYS

In today's world, the Internet is already the cornerstone of communication. The number of internet users is increasing. The snowfall of March 2013 showed that the population wanted to receive timely and reliable information that supports their security. During the flood of Danube June 2013, it was observable that people with social media profiles searched and shared information about the hazard situation on their computers or smartphones. Lack of information or bad, misleading information on the above-mentioned events resulted in people hesitation, wrong decisions, panic-like behaviors.

In order to prove the justification for the programs written on smartphones, it is necessary to examine the frequency of domestic Internet traffic.

Investigating the frequency of domestic internet use

Strategopolis Ltd. made a telephone questionnaire survey conducted by the National Media and Communications Authority (hereinafter: NMHH) on the mobile Internet habits of adult society and its mobile Internet service perception at the beginning of this year. During the survey, 1019 randomly selected adults were asked about their mobile Internet marketing habits and other issues related to the mobile market. [13]

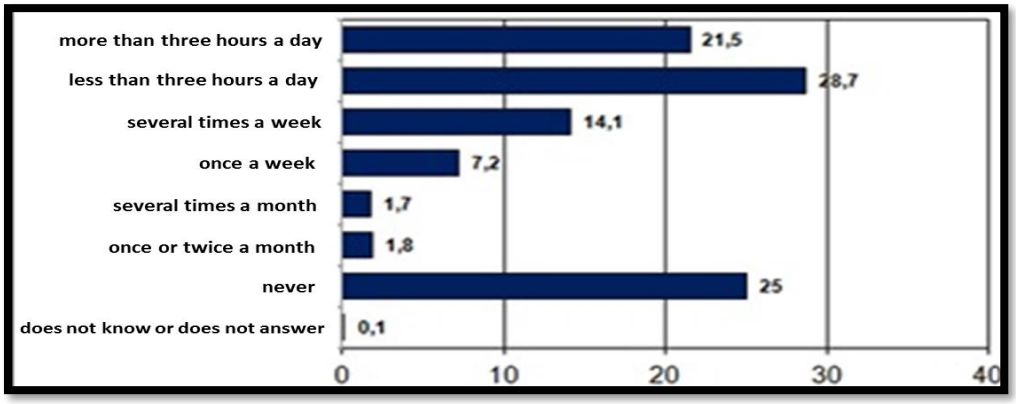


Figure 4 How frequently do you use internet? (%)

Looking at the frequency of Internet usage, half of the population (50.2%) is online every day, with the largest share (28.7%) who use the Internet less than three hours a day and more than one fifth (21.5%) spend more than three hours on the internet each day. 14.1 percent of the respondents are on the Internet more than once a week, and 7.2 percent are those who just surf once a week. Monthly, a total of 3.5 percent of the population browse the Internet, including 1.7 percent several times in a month, 1.8 percent once in a month or less. However, a quarter of the population does not use the Internet at all. The proportion of those who did not respond was insignificant, 0.1 percent.

Presentation of mobile applications

It is important to analyze the habits of domestic population so that the social support of mobile applications can be determined.

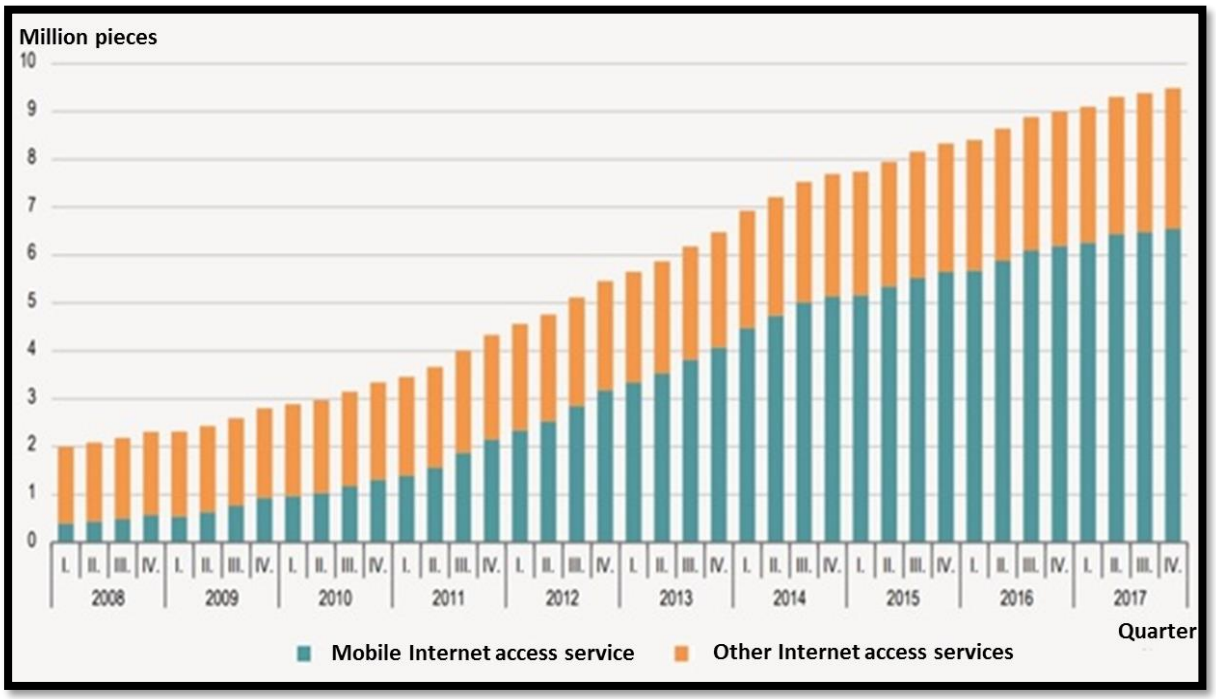


Figure 5 The development of mobile Internet and other Internet access services between 2008 and 2017

At the end of the IV. quarter of 2017, the volume of wire subscription subscriptions (2.8 million) exceeded the base period by 4.7 percent. Within this, the most significant technology for the 50 percent was the cable-based subscription, the number of which was 4.0, the optical networks increased by 19 percent, while the xDSL subscriptions decreased by 3.4 percent. Within the Internet subscriptions, the combined ratio of xDSL, optical and cable subscriptions (29 percent) did not change practically any year. [14]

Strategopolis Ltd. conducted a telephone questionnaire survey between January 25 and February 3, 2013, during which 1019 randomly selected adult adults were interviewed.

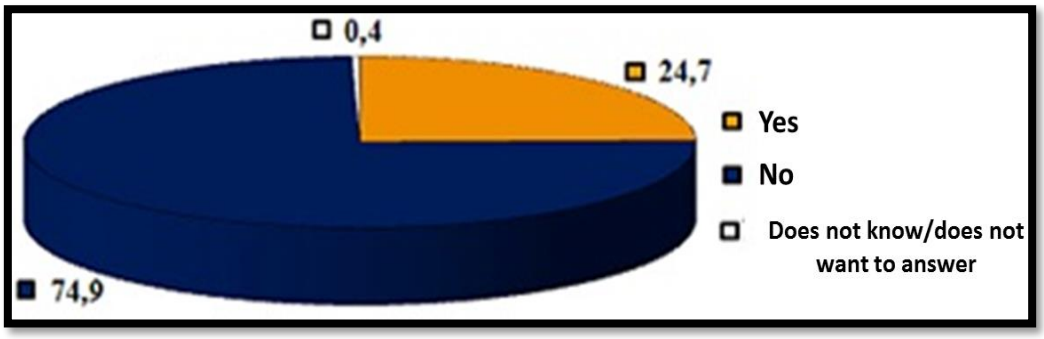


Figure 6 Rate of mobile internet users

Although almost one quarter (24.7%) of the respondents use mobile Internet, most of the Hungarian population (74.9%) does not use such services yet. [15]

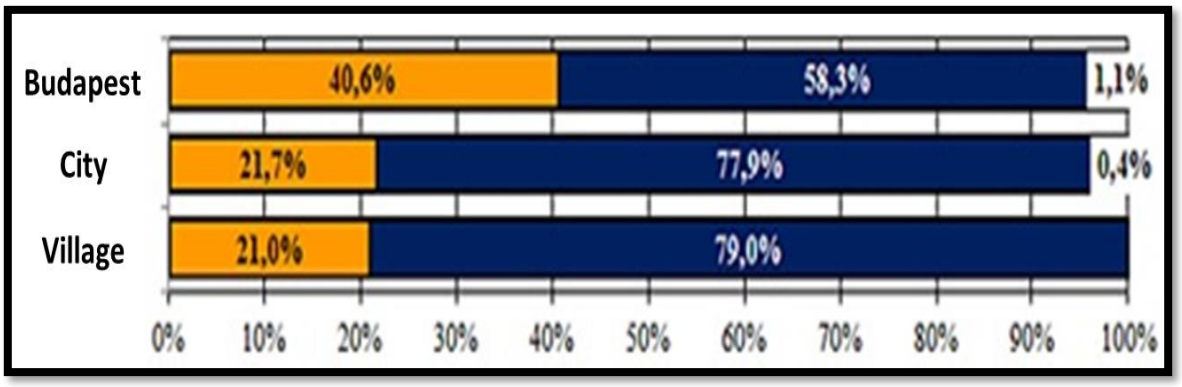


Figure 7 Where do most people use mobile internet? [15]

In Budapest, there are twice as many users (40.6%) as mobile internet users, as in rural towns (21.7%) or in villages (21%). 86 percent of adult Hungarian Internet users, namely nearly 4 and a half million, use smartphones in our country. The survey was conducted by eNET in October 2016 in the framework of eNET-Telecom's "Report on the Internet Economy" survey on the surface of the VeVa online research community, based on 868 fill-in data. The data does not reflect the entire population, but the group of people over the age of 18 who are regularly online. [16]

Taking into account 21st century technologies[6] and social relationships[7] applications for smartphones emerged as a new method of emergency communication. Due to the rapid spread

[6] Laptop, notebook, netbook, smart phone, tablet, wifi system, etc.
[7] Social media: Facebook, Instagram, Twitter, Google+, YouTube, Wikipédia, Reddit, LinkedIn, Tinder etc.

of smartphones and tablet PCs, organizations and other bodies[8] involved in disaster prevention have recognized that applications need to be created in order to inform the public on the basis of their own professional profiles and, as far as possible, to inform the most members of society. They have found that delivering emergency information and short-term weather forecasts to users can significantly increase the security of the population and citizens. Examples of such applications are: Emergency Response Service (VÉSZ) based on the joint development of BM OKF, RSOE and Microsoft Hungary, which serves the immediate, up-to-date, targeted information of the population. [2]

Meteora, [9] a nationwide available and free of charge application developed by the National Meteorological Service, can run on tablet computers, providing critical weather and beforehand authentic weather and hazard warning information for the population and the media.

Another popular weather application is the Időkép website. Its main profile is monitoring the current weather. The difference between Meteora is that it sends alerts to the user based on different weather conditions.

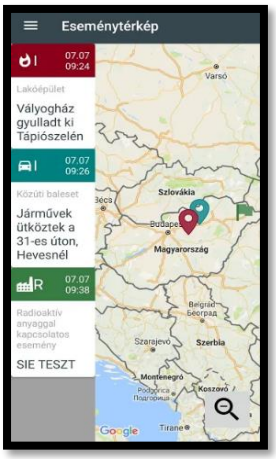
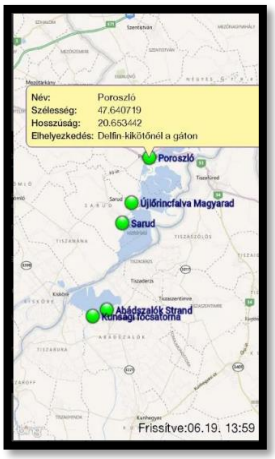
Meteora	**VÉSZ**	**TAVIHAR Widget[10]**	**Hydroinfo**
National Meteorology Service	RSOE	RSOE	National Water Warning Service
			

Table 4. Information-assisted programs installable on mobile tools

Presentation of social media, importance in public hazard education and communication

Social media has become part of everyday life, [17] infiltrating workplaces and homes. A generation that was born into the revolution of infocommunication technologies was formed, through which it became socialized and started to use these new tools skillfully. For them, social media, the use of smartphones is an everyday activity. They spend most of their time on these devices, on content sharing and keep contact on these platforms.

[8] Jointly involved in disaster prevention: Act CXXVIII. (1) of: those involved in disaster relief will provide the citizens with information, life, physical integrity, material goods and the environment.
[9] More information about the application: http://meteora.met.hu/
[10] Tavihar is a program of information on the hikes of Hungary's navigable lakes, which can be run on mobile devices that can be continuously tracked.

GfK Hungária's Digital Connected Consumer survey in 2012 measured Hungary's Internet usage on an average of 207 minutes (nearly 3.5 hours). A year earlier it was 201 minutes. The image of Ipsos's 2013 research, which defines the average social media usage in 2.8 hours, further delights the image. When we break down data for age groups, it turns out that the average daily usage of people under the age of 35 is 4.2 hours, the age between 35-49 is 3.1 hours, and those over the age of 50 spend 2.3 hours on a social network.

The international statistics of SocialTimes (Global Information Center for Social Media) reveal that Hungary has a very high profile in social media use in the global competition: 46.19% of the population, namely 4.6 million, actively use Facebook. For comparison, the penetration rate in the United States is 57.35%. The age distribution is shown in Table 5. According to We're Social's survey in 2018, the use of social networking sites in Hungary amounts to 5.81 million, of which 4.8 million are those who use Facebook also on the phone. [18]

Sex	**13-18**	**19-25**	**26-35**	**36-45**	**46-55**	**56-65**	**65+**
Male	380.000	520.000	560.000	420.000	182.000	186.000	68.000
Female	380.000	500.000	560.000	480.000	260.000	240.000	74.000
All	**760.000**	**1.020.000**	**1.120.000**	**900.000**	**442.000**	**426.000**	**142000**

Table 5 Age and gender distribution for Facebook users. (Created by: László Teknős, 2015)

It can be stated that the above data legitimizes social media research. A large number of users have the potential to be left out, but they cannot be ignored (to name a few: marketers, political organizations, government, national security organs, etc.). From the above data, it is clear that social media is used by the 19-35 age group, the most striking layer that is young, the more capable and for disaster management, can be the largest staffing pillars.

This more than two million user layer should be addressed through social media, and can be involved in disaster management system for Hungary's as a civil protection force. There are also tremendous opportunities in public hazard education, according to the age distribution of the table. The age group of 13 to 35 years old accounts for nearly 3 million users. From this it can be stated that with this well-run long-term social media strategy this huge human being can be an active participant in the successful consolidation of security culture. By winning the current young generation, a large number of human resources can be provided to disaster relief, young people whose approach will shift to sustainable development, self-defense and effective cooperation with authorities. Social media has a tremendous power potential, and many times there is a tremendously high power centered on virtual space.

Social media can assist in the prevention period in preparing for disaster risk and emergency situations. There are preventive solutions that are no longer new to the hazard education so far, but the novelty may be that the collection of today's information society is heavily reliant on the Internet, so the social media created for contacts and news sharing also provides information that supports security to carry it. In the prevention, the media also facilitates the work of the hazard education mentors, with the help of bilateral communication and shared information, in writing dialogues can pass off.

In terms of social needs, social media is an important means of communication. Websites, for example, with a Facebook page, provide greater bilateral communication, such as between population and disaster management. The well-developed web interface provides mainly one-way communication. The information material is provided and recorded by residents, but they can only ask their questions in a separate submenu, and they receive the answer much more later, if they receive at all. The moderator or admin (personally always the leader of the group) can respond to the newsletters and newsletters shared on the Facebook interface, and

may respond by the protocol approved by the Civil Protection Superintendent (or the person responsible for the press release). At one time, more people can ask questions to get answers within a short period of time, commenting on each other's questions, ensuring multidirectional communication. Social media is suitable for raising awareness.

Web sites are slower in this aspect, and even the public information they provide is slower because the authority is not forced to provide information more frequently. Conversely, in community media, ongoing public reactions, questions, comments, and requests for help force the authorities to respond, to inform the general public (this is mostly a case of catastrophic events and massive casualties). Social media is more frequent due to the events, the more frequent postings, than the websites (there is no activity, there are no terms, because the news, sharing is unilateral).

Can social media be used as education and preparation tool?

In 2011, in the United States, the FEMA (Federal Emergency Response Agency) used the community media to inform the public during Hurricane Irene. In the year 2012, at Hurricane Sandy, government agencies and FEMA communicated preventive measures to the general public through communication with the community.

Since many organizations[11] use a Facebook[12] page, therefore, because of the nature of the task, within the tools of social media, Facebook can be the platform through which the population can be widely accessed. In the flood of June 2013, the official Facebook page of professional disaster management was visited by appr. 300,000 person, so it can be found out that, in the event of extraordinary catastrophes, the population is looking for disaster protection information, guidelines, etc. at the time of the event. [13]

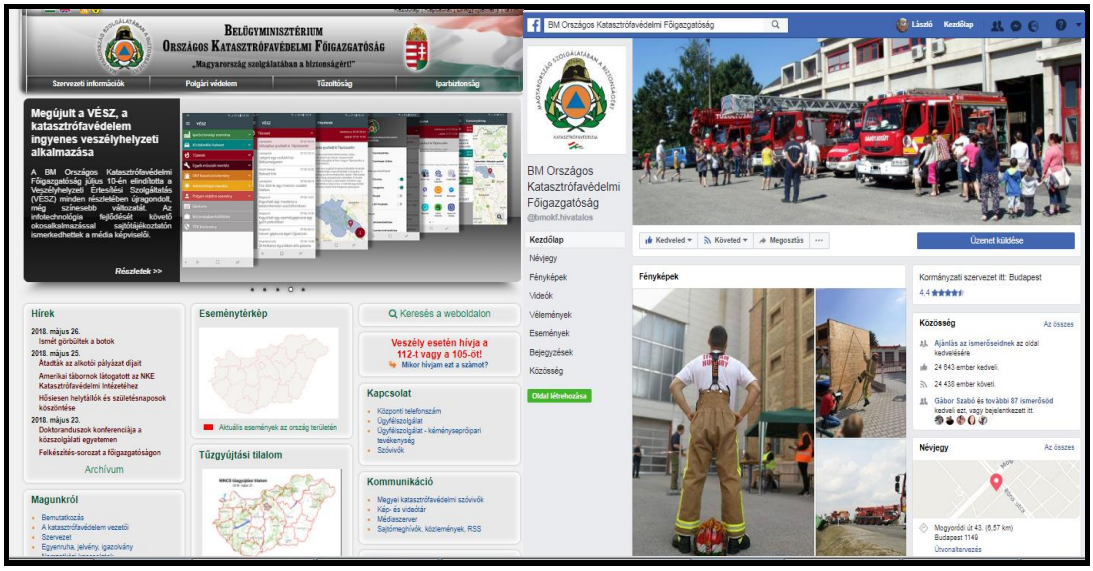


Figure 8 Official website (left) and Facebook page (right) of the National Directorate General for Disaster Management, Ministry of the Interior (Created by László Teknős, 2018)

[11] National Directorate General for Disaster Management, Ministry of the Interior (NDGDM), Hungarian Federation of Red Cross, Hungarian Defence Forces, RSOE, National Meteorology Service, etc.

[12] From the social media scene, only facebook (the most popular means of contact retrieving for home users in the internet) comes to the fore.

[13] On May 20, 2018, 24,438 people followed the NDGDM official facebook page.

Facebook is now available on mobile phones. This is helpful for public hazard communication. It can be expected that accessing Facebook via the phone will allow people to reach the required emergency information from anywhere, at any time, about road closures, about key data related to vulnerable areas, etc., which will help residents to get real-time information. This, in turn, requires that information security on Facebook should be kept in line with the situation. This information is something that affects also personal security, so tracking must be continuous for their own sake. For a citizen, collecting information on a continuous Facebook or website, he or she finds more information about his or her own security and less likely to be in trouble, so it does not affect the involved organization's work very significant. Additionally, if the citizen follows the information and behavioural norms on Facebook, it is more likely that he or she will not be in trouble or the problem will be easily solved. For example, the willingness of the community to engage in contact with the civil protection resources (races, lectures, exhibitions, events, etc.) addressing the traditional population is needed. Willingness to visit Facebook can be achieved through marketing and management. The goal is the continuous measurement and monitoring of the effectiveness of information transfer, preparation and information efficiency on the Facebook page. The possible measurements to be taken into account are: the number of fans, followers and comments, visiting ratios, the proportion of positive and negative ratings.

The current situation and major lessons of domestic emergency communication during public hazard education

With the development of information technology, the possibilities public hazard communication has widened. With the transformation of society, publicity and the need for wider access to public interest data play an increasingly important role. Getting information about communities has become more simple and faster now. While in the old days space and time played an important role in the transfer of information, these factors are no problem today. The Internet, beyond the physical dimension, has dismantled the bounds of constraint. Social Media has become one of the most important elements of this accelerated information flow. Due to the large number of Hungarian users (see previous subsection) it is indispensable that we also examine the domestic adaptation of the possibilities and methods provided by the social media in Hungarian defense mechanism, especially in public hazard communication. As the snowfall of March and the Danube flood of June, 2013 showed, there is a demand on the part of general public for the use of these new infocommunication technologies by the professional organizations. When the official Facebook page of professional disaster management during the flood of June 2013 is visited by approx. 300,000 person, it is assured that in emergency situations, the population is looking for information, guidelines, information from disaster management during the defense.

Providing credible information for the citizens may be life-saving during events caused by extreme weather. Generally, weather anomalies are complex, so negative impacts on population and material assets are expected, emergency communication cannot be prevented or bypassed because information can help to avoid panic-like, irrational "self-defense" actions of the population.

SUMMARY, CONCLUSION

With the development of information technology, the possibilities for informing the public have widened. Getting information about communities has become more simple and faster now. While in the old days space and time played an important role in the transfer of information, these factors are no problem today. The Internet, beyond its physical dimension, dismantled the bounds of constraint.

Due to the large number of Hungarian users, it is indispensable to examine in Hungary the adaptation of the possibilities and methods provided by the social media to the Hungarian defense mechanism, in particular the public hazard communication. As the snowfall in March and flood in July, 2013 showed, there is a demand for the population to use these new info communication technologies by professional organizations.

Social media can help prevent damage, disaster risk or emergencies during the prevention period. Preventive solutions can be made, which are no longer new to the public hazard education. The novelty, however, may be that the collection of information in today's society is heavily reliant on the Internet, so social media created for contacts and news sharing also includes the availability of security-capable information.

The disaster management was created to protect the population and the material goods of Hungary, which has been structurally reorganized in order to respond more effectively to current challenges. Within the three major areas of disaster management, civil protection is one of the most important defense tasks for the protection of the citizens. The snowfall situation in March 2013 and the flood event in 2013 assess the importance of the role of civil protection (primarily in information, training, volunteer management and coordination).

Preparations for Disaster Preparedness are intended to prepare for the implementation of the tasks specified in Section 52 of the Act on Disaster management, as well as, as far as possible, minimizing the adverse consequences of natural, technological and other causes of disasters, their remediation and restoration.

Public hazard education must take place during the pre-disaster (before occurrence) period. It is important that residents are prepared for recovery information and behavioral rules as well. Preparation should not be a periodic population protection program, it must be continuous, because awareness can only be provided through regular, repetitive knowledge transfer.

Younger generations use digital devices at the skill level. It has become part of their lives so much that most of them immediately share everything. The potential of community media (not only Facebook) to support disaster relief needs to be deeper and the author's proposal is to create a strategy which requires a coherent framework for joint application.

Overall, public hazard education and communication are not recent things. The professional disaster management organization took prevention, population information and civil protection training system over the predecessor state-level fire service. By combining and developing the two systems and approaches, the National Directorate General for Disaster Management Ministry of the Interior (hereinafter referred to as "NDGDMMI") developed the new foundations for public hazard education and communication. It has established a network of population training mentors and has established effective cooperation with the Hungarian Civil Protection Association. The HCPA contributes to the implementation of the volunteer population preparation system in the establishment and operation of the Emergency Retail Customer Service Information Centers (VELÜNK center established in Százhalombatta). With publications, organizing exhibitions and open professional days, the professional disaster management body seeks to draw the attention of a wider population to the disaster prevention opportunities, to the recommended forms of behavior in emergencies, and to other important information.

Author is of the opinion that information to the public must be provided, so that in the content keywords must be hidden to reassurance. Regardless of what the situation is, psychological aid can save lives, restore sober thinking, bring people to normal levels of confusion, reduce uncertainty and build trust in the public, etc. Providing quick information save lives.

REFERENCES

[1] *62/2011. (XII. 29.) BM rendelet a katasztrófák elleni védekezés egyes szabályairól IX. FEJEZET 67.§.* https://net.jogtar.hu/jogszabaly?dbnum=1&docid=a1100062.bm&mahu=1 (Download: 17 May 2017)

[2] TEKNŐS L.: *A lakosság és az anyagi javak védelmének újszerű értékelése és feladatai a klímaváltozás okozta veszélyhelyzetben*. Doktori (PhD) értekezés. Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola Budapest. pp.1-263. (2015) http://archiv.uni-nke.hu/feltoltes/uni-nke.hu/konyvtar/digitgy/phd/2015/teknos_laszlo.pdf (Download: 17 May 2017)

[3] HOFFMANN I. - KÁTAI-URBÁN I. - VASS GY.: *Vegyi- és sugárfelderítés katasztrófavédelmi technikai eszközrendszerének vizsgálata I. rész telepített rendszerek*. Hadmérnök, XI. Évfolyam 1. szám - 2016. március. pp. 89-97. ISSN 1788-1919. http://www.hadmernok.hu/161_09_hoffmanni_kui_vgy.pdf (Download: 17 May 2017)

[4] DUDÁS Z. – MUHORAY Á.: *Egyes lakosságvédelmi intézkedések felelősségi rendszere veszélyhelyzet esetén*. Műszaki Katonai Közlöny, XXVI. évfolyam, 2016. 3. szám. pp. 2-22. ISSN 1219-4166. http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2016_3sz/001_Dudas%20Zoltan-Muhoray%20Arpad.pdf (Download: 17 May 2017)

[5] BARTA V. L.: *Katasztrófavédelmi-tűzvédelmi igazgatás.* Rendészeti szakvizsga. pp. 1. 148. http://bmkszf.hu/dokumentum/2143/Katasztrofavedelmi_igazgatas.pdf (Download: 17 May 2017)

[6] *234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról*. https://net.jogtar.hu/jogszabaly?docid=a1100234.kor (Download: 17 May 2017)

[7] *290/2011. (XII. 22.) Korm. rendelet a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény egyes rendelkezéseinek végrehajtásáról*. https://net.jogtar.hu/jogszabaly?docid=a1100290.kor (Download: 19 May 2017)

[8] *2010. évi CLXXXV. törvény „a médiaszolgáltatásokról és a tömegkommunikációról*: https://net.jogtar.hu/jogszabaly?docid=A1000185.TV (Download: 19 May 2017)

[9] *2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról*. https://net.jogtar.hu/jogszabaly?docid=a1100128.tv (Download: 19 May 2017)

[10] TEKNŐS L.: *A rendkívüli időjárás okozta veszélyhelyzetek és a kárterületeken végzendő polgári védelmi feladatok rendszere Magyarországon*. In: Aszódi Júlia; Szabó Ágnes; Hoffer Csaba; Rosta Petronella; Teknős László; Szabó Sándor; Tusori Szabolcs; Murai László Horváth Hermina Horváth Hermina (szerk.) Konferencia kiadvány: "Katasztrófavédelmi Díj" Tudományos Konferencia 2013. c. tudományos rendezvényen elhangzott előadásokhoz. Nemzeti Közszolgálati Egyetem, 2013. pp. 80-100. ISBN:978-615-5305-18-4. https://kvi.uni-nke.hu/document/kvi-uni-nke-hu/teknos-laszlo-a-rendkivuli-idojaras-okozta-veszelyhelyzetek-es-a-karterulet.pdf (Download: 19 May 2017)

[11] HORNYACSEK J.: *A települési védelmi képességek a katasztrófa-kihívások tükrében: A települések katasztrófa-elhárítási feladatai, a végrehajtásához szükséges helyi védelmi képesség alapvető területei, azok kialakításának folyamata*. Budapest: Biztonságunk Érdekében Oktatási- és Tanácsadó Tudományos Egyesület, 2011. 100 p. ISBN:978-963-08-2606-8. http://www.drhornyacsek.hu/sajat%20publikaciok/vedelmi%20kepessegek.pdf (Download: 20 May 2017)

[12] HORNYACSEK J. - CSÉPAINÉ SZÉLL P. - VERES V.: *Önkormányzati vezetők felkészítése a védelmi feladatokra: kézikönyv polgármesterek részére a települési védelmi feladatok ellátásához.* Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2010. 171 p. ISBN:978-963-7060-76-2. http://www.drhornyacsek.hu/sajat%20publikaciok/kezikonyv%20polgarmesterek%20reszere.pdf (Download: 20 May 2017)

[13] *Szinte mindenki tudja mi az a mobilinternet. 2013.* április 24. https://sg.hu/cikkek/96913/szinte-mindenki-tudja-mi-az-a-mobilinternet (Download: 20 May 2017)

[14] *Internetezés Magyarországon: a legfrissebb adatok.* 2018. március 10. http://kamaraonline.hu/cikk/internetezes-magyarorszagon-a-legfrissebb-adatok (Download: 20 May 2017)

[15] CZIPPERER D.: *Kik használnak mobilinternetet hazánkban*? 2013. május 11. http://hirek.prim.hu/cikk/97550/ (Download: 20 May 2017)

[16] HABÓK L.: *Négy és fél millióan használnak okostelefont*. 2017. január 25. https://www.hwsw.hu/hirek/56731/enet-kutatas-felmeres-okostelefon-mobil-hasznalat-olvasas-zene-video.html (Download: 20 May 2017)

[17] BÁNYÁSZ P.: *A közösségi média, mint az információs hadszíntér speciális tartománya.* Hadmérnök, XII. Évfolyam „KÖFOP" szám – 2017. október. pp. 108-121. ISSN 1788-1919. http://hadmernok.hu/170kofop_07_banyasz2.pdf (Download: 20 May 2017)

[18] KEMP, S.: *Digital in Eastern Europe*, In. We are social, 29-01-2018. https://www.slideshare.net/wearesocial/digital-in-2018-in-eastern-europe-part-2-east86865266 (Download: 20 May 2017)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

A TISZTÍTOTT SZENNYVÍZ MEZŐGAZDASÁGI HASZNOSÍTÁSÁRA ALKALMAS TERÜLETEK MEGHATÁROZÁSA MAGYARORSZÁGON

SELECTING AREAS THAT ARE APPROPRIATE TO AGRICULTURAL UTILIZATION OF TREATED WASTEWATER IN HUNGARY

TÓTH Tamás

(ORCID: 0000-0003-2810-0583)

toththamas@live.com

Absztrakt

Az éghajlatváltozás hatására egyre nagyobb nyomás nehezedik a hozzáférhető édesvízkészletekre. A klímaváltozás és a demográfiai változások veszélyeztetik a készletek és az igények közötti érzékeny egyensúlyt. A jövőben megnövekedhet a vízhiányos helyzetek előfordulásának valószínűsége Magyarországon. A különböző gazdasági ágazatok megnövekvő vízigénye miatt egyre kiélezettebb verseny folyik a vízért. Elengedhetetlenné vált, hogy a rendelkezésre álló erőforrásokat hatékonyan használjuk fel. A tisztított szennyvíz felhasználás elősegíthetné a vízhiányos helyzetek kialakulásának megelőzését, ezért a szerző kidolgozott egy módszert a mezőgazdasági hasznosítására alkalmas területek meghatározásához. A tudományos közlemény bemutatja a módszer felépítését és alkalmazását.

Kulcsszavak: *éghajlatváltozás, vízhiány, víz újrahasznosítás, tisztított szennyvíz*

Abstract

Due to climate change the pressure is increasing on the available freshwater resources. Climate change and demographic changes jeopardize the sensitive balance between supplies and demands. In Hungary, the probability of water scarcity may increase in the future. Increasing water demands of the different economic sectors lead to fierce completion. Effective utilization of the resources is necessary. Having regard to the assumption that the treated wastewater reuse may facilitate the prevention of water scarce situations, the author developed a method to define areas appropriate to agricultural utilization. This scientific article presents the structure and the application of the designed method.

Keywords: *climate change, water scarcity, water reuse, treated wastewater*

A kézirat benyújtásának dátuma (Date of the submission): 2018.04.16.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.28.

BEVEZETÉS

Az éghajlati viszonyok szélsőséges változása egyre inkább ráirányítja a figyelmet a fenntartható vízgazdálkodás megvalósításának jelentőségére. A klímaváltozás hatására egyre nagyobb nyomás nehezedik a hozzáférhető édesvízkészletekre. Az éghajlati és a demográfiai változások veszélyeztetik a készletek és az igények közötti érzékeny egyensúlyt. Az egyensúlyfenntartás sérülékenységének egyik legeklatánsabb megnyilvánulása, 2018-ban, a Dél-Afrikai Köztársaságban bekövetkezett vízkrízis. Egyes régiókban, a vízhiány kialakulásának megnövekvő valószínűsége miatt, a vízgazdálkodással foglalkozó szakemberek körében fokozatosan előtérbe kerül, hogy különböző tevékenységre, milyen minőségű vizet használunk.

A jövőben megnövekedhet a vízhiányos helyzetek előfordulásának valószínűsége Magyarországon. A szélsőségeknek való kitettség korlátozza Magyarország versenyképességét. A különböző gazdasági ágazatok megnövekvő vízigénye miatt egyre kiélezettebb verseny folyik a vízért. Elengedhetetlenné vált, hogy a rendelkezésre álló erőforrásokat hatékonyan használjuk fel. A víz újrahasznosítás értékes alternatívát jelent számos igény kielégítésére. A Magyarországon képződő tisztított szennyvizek hasznosításában rejlő potenciál jelenleg még kihasználatlan. Az egyik legnagyobb vízfelhasználó az agrárszektor. Az öntözéses gazdálkodás során a tisztított szennyvíz alkalmas lehet egyes területeken adott növénykultúrák öntözésére. A tisztított szennyvíz újrahasznosításával kapcsolatos szakirodalmat áttanulmányozva megállapítottam, hogy az eddigi kutatások nem foglalkoztak az alkalmas területek kiválasztásának módszertanával.

Felmerül a kérdés, hogy hol találhatók Magyarországon a tisztított szennyvíz mezőgazdasági hasznosítására alkalmas területek?

Feltételezem, hogy a víz újrahasznosítás egyes régiókban biztonságosan és költséghatékonyan megvalósítható.

A közlemény fő célkitűzése, hogy meghatározza a tisztított szennyvíz mezőgazdasági hasznosítására feltételesen alkalmas területeket. Az ideális területek kiválasztásához kidolgoztam egy speciális eljárásrendet.

A tisztított szennyvíz biztonságos és költséghatékony felhasználásával javítható lenne a vízkészletekkel való gazdálkodás hatékonysága. A kutatásom keretében javasolt szempontrendszer alkalmazása elősegíthetné a jövőben megnövekedett előfordulási valószínűséggel kialakuló vízhiányjelenségek megelőzését célzó rentábilis beruházások kivitelezését.

ÉGHAJLATVÁLTOZÁS HATÁSA A VÍZGAZDÁLKODÁSRA

Az *„Éghajlatváltozás hatása a vízgazdálkodásra”* című fejezet a vizek többletének, illetve hiányának kezelésére hívja fel a figyelmet. A vízhiányos helyzetek kialakulásának értelmezése, a területhasználatok és a víztározók miatt, szorosan kapcsolódik az árvizekhez. A vízgazdálkodásban új kihívást jelent, hogy a szélsőséges helyzetek – vizek többlete vagy hiánya – megoldásának igénye egyre rövidebb időintervallumon belül ciklikusan keletkezik, akár azonos területen belül. A szélsőségek előfordulási valószínűségének növekedése következtében változik, hogy milyen helyzet minősülhet rendkívülinek. Az előfordulási valószínűség és a rendkívülivé minősítés között megállapítható, hogy ellentétes korreláció van.

Az üvegházhatású gázok koncentrációjának növekedése hozzájárul a levegő és a víz hőmérsékletének emelkedéséhez, fokozva az aszályos és a vízhiányos helyzetek kialakulásának valószínűségét. A Goddard Institute of Space Studies intézet kutatása szerint az elmúlt 138 év valaha mért 5. legmelegebb januári hónapja 2018-ban volt. [1] A mérésekből megállapítható, hogy a valaha mért legmelegebb január hónap 4 alkalommal az elmúlt 4 évben jelentkezett. A hőmérsékleti viszonyok megváltozásának hatására, a környezeti változásokon túl, gazdasági és társadalmi változások is indukálódnak.

A hőmérséklet növekedése fokozza a tengerszint emelkedését. A globális tengerszint nem egyenletes sebességgel, hanem gyorsulva emelkedik. [2] A tengerszint tartós emelkedése környezeti, gazdasági és társadalmi szempontból egyaránt jelentős és potenciális veszélyt jelent. Az éghajlatváltozás következtében Nyugat- és Közép-Európában az árvízkockázat mértékének emelkedése valószínűsíthető. [3] A magyarországi adatokat értékelve látható az utóbbi években a rekord vagy ahhoz közeli árvizek számának növekedése. A árvízi katasztrófák során szükségessé válhat a vizek tisztítása. [4; 129. o.]

A kárkategóriák tekintetében az árvíz sematizálva vonaltípusú természeti katasztrófa, ezzel szemben megállapítható, hogy az aszály területtípusú környezeti, gazdasági és társadalmi károkat produkál. A szélsőséges helyzetek kialakulásának megelőzésére való törekvés a költséghatékonyság szempontjából elengedhetetlen.

Az éghajlatváltozás a hőmérséklet növekedésén keresztül negatív hatással van a csapadékvíz hasznosíthatóságára. Magyarországon a csapadékmennyiség a téli hónapokban kismértékben növekedhet, viszont a nyári hónapokban nagyobb mértékű csökkenés prognosztizálható. [5] A mezőgazdasági termelés szempontjából az egymást követő hőségnapok számán túl, kiemelt fontosságú a vegetációs időszakban keletkező csapadék mennyisége, eloszlása és intenzitása. Magyarországon, a vegetációs időszakban, éppen a legjelentősebb termőterületeken (Alföld, Kisalföld) valószínűsíthető a legkevesebb csapadék. A vízgazdálkodásban az éghajlatváltozás által generálódó új kihívások kezeléséhez újszerű megoldásokra van szükség. Az éghajlatváltozás által befolyásolt csapadékviszonyok változásából származó termelői kockázat mértékét enyhíthetné a kiszámítható víz újrahasznosítás alkalmazása. A sérülékeny területeken a tisztított szennyvíz újrahasznosítás hozzájárulhatna a termésbiztonság fokozásához. Az igények és a készletek egyensúlyának biztonsága növelhető lenne egy programszerűen kialakított igénymenedzsmenttel és az alternatív vízkészletek kihasználásával.

Összességében megállapítható, hogy az éghajlatváltozás következtében megnövekedett a szélsőséges helyzetek kialakulásának valószínűsége. A döntések minőségét megbízható, jól szelektált hidrometeorológiai és káradatokkal, illetve részletes előrejelzések alkalmazásával lehet biztosítani. [6] Az új kihívások hatékony kezeléséhez az egyes hatások rendszerszintű megértése és számszerűsítése kiemelt jelentőségű.

Az Európai Unió vízpolitikája

Az Európai Unió (EU) vízpolitikáját *„a vízpolitika terén a közösségi fellépés kereteinek meghatározásáról”* elnevezésű 2000/60/EK irányelv tartalmazza. [7] Az 2000/60/EK irányelv, általánosan elfogadott nevén Víz Keretirányelv (VKI) képezi a vízgazdálkodás alapját az EU-ban. A VKI jelentőségét az adja, hogy a vizek védelmét szolgáló, korábban szétaprózódott, nehezen értelmezhetővé vált, irányelvek sokaságának rendszerét összefogja és harmonizálja.

A VKI fő célkitűzése, hogy a felszíni és felszín alatti vizek egyaránt elérjék a *„jó állapotot”*. A tagállamok, a célkitűzés megvalósítása érdekében, intézkedési programokat dolgoznak ki, vízgyűjtő-gazdálkodási tervek (VGT) formájában, amelyeket 6 évente felülvizsgálnak. Az első tagállami VGT-k (VGT1) 2009-ben készültek el, amelyeket 2015-ben felülvizsgáltak, létrehozva a VGT2-ket. [8] Legkésőbb az irányelv hatálybalépését követő 15 éven belül (2015-ig) el kellett volna érni a jó állapotot, amit nem sikerült megvalósítani. A VKI lehetőséget biztosít a megadott határidő meghosszabbítására 2027-ig.

A tagállamok által készített VGT1 és VGT2 állapotértékelések alapján prognosztizálható, hogy a VKI fő célkitűzése nagy valószínűséggel nem teljesíthető teljes mértékben a megadott határidőre. A feltételezésem alapját a VGT1 és a VGT2 állapotértékelési eredményeinek összehasonlításából meghatározható javulás lassú üteme képezi.

Az éghajlatváltozás következtében az állapotjavulás mértéke lelassulhat, illetve fennáll a veszélye az állapotértékelési eredmények romlásának, tovább nehezíthetve a fő célkitűzés teljesítését. A tisztított szennyvíz újrahasznosítás hozzájárulhatna a VKI célkitűzéseinek

eléréséhez. Az Európai Unió vízpolitikájának célkitűzéséhez való hozzájáruláson túlmenően egy esetleges víz újrahasznosítási projekt tervezése során, a megvalósíthatóság szempontjából, kulcsfontosságú, hogy a projekt összhangban legyen a VKI előírásaival.

Aszály és vízhiány

Az éghajlatváltozás ráirányítja a társadalom figyelmét arra, hogy az aszályok és a biztonságot veszélyeztető vízhiányok megelőzése, hatékony kezelése nem halogatható. A várható kihívások megoldása érdekében a jövő vízgazdálkodását ma kell megalapozni.

A globális léptékű kihívások megoldásához nemzetközi összefogás szükséges. A nemzetközi érdekek érvényesítésének érdekében az Egyesült Nemzetek Szövetsége (ENSZ), 1994-ben, elfogadta az elsivatagosodás elleni küzdelemről szóló egyezményt. [9] Az éghajlati viszonyok olyan változásokat indukálhatnak a vízgazdálkodásban, amely indokolttá teszi az egyezmény eredményességének növekedését megcélzó intézkedések bevezetését.

Számos régiót, élelmiszerbiztonsági szempontból kiemelt fontosságú mezőgazdasági területet veszélyeztet szokatlanul nagymértékű aszály, vízhiány. A veszélyeztetettségen túl sok esetben problémát jelent az adathiány vagy az adatok hozzáférhetőségének hiánya.

Az Európai Bizottság (EB) felmérése szerint 1976 és 2006 között az aszállyal sújtott területek száma megközelítőleg 20 %-kal növekedett. Az okozott kárköltség becsült értéke elérte a 100 milliárd eurót. [10] Magyarországon az aszály által leginkább veszélyeztetett területek között olyan jelentős mezőgazdasági területek szerepelnek, mint a Homokhátság vagy a Nagykunság.

A ClimWatAdapt projekt keretében történt kutatások szerint, Európa vízgyűjtőterületeinek akár 50 %-a is vízhiányossá válhat 2030-ra. [11] A VGT2 állapotértékelése szerint az vízigények 40 víztestnél meghaladják a hosszú távon rendelkezésre álló készletet Magyarországon. A vízhiány kialakulásának megelőzése érdekében azonosítani kell azokat az intézkedéstípusokat, amelyek egy-egy adott régióban hatékonyan alkalmazhatók.

Az elérhető készletek és a jelentős vízigények vizsgálatánál megállapítható, hogy az öntözéses mezőgazdaságra jelentős hatást gyakorolnak az aszályok. A hatékony aszálykezelés megvalósítását számos paraméter befolyásolja. Fontos szerepe van a különböző talajtípusok kezelésének, a növénykultúrák és az öntözőrendszerek megválasztásának. A szélsőséges időjárási jelenségek, erős szelek könnyen kiszáríthatják a gyengébb vízháztartási talajokat, amely a tűzveszélyt is fokozhatja. Az éghajlatváltozás során a téli hónapokban megnövekedő potenciális párolgás negatív hatással van a beszivárgásra, csökkentve a hozzáférhető vízkészleteket. [12] Az agrárgazdálkodásban a nyári hónapokban jelentkező alacsony vízhozamok csökkenése a kritikus tényező, mivel ez az időintervallum egybe esik a növények vegetációs időszakával.

A különböző típusú vízigények kielégítését követően a szennyvíztisztító telepeken nagy mennyiségű, eltérő vízminőségű tisztított szennyvíz keletkezik, amelyek hasznosítás nélkül elvezetésre kerülnek. Felmerül a kérdés, hogy az éghajlatváltozás hatására egyre nagyobb valószínűséggel kialakuló aszályok és vízhiányok mérsékelhetők lennének-e valamilyen szinten a vizek újrahasznosításával?

VÍZ ÚJRAHASZNOSÍTÁS

A Víz Keretirányelvben szereplő *„intézkedési programokba felveendő intézkedések listája”* (Annex VI.) tartalmazza a *„hatékonysági és újrahasznosítási intézkedéseket”* és ezzel összhangban Magyarország felülvizsgált Vízgyűjtő-gazdálkodási Tervében is megjelent a víz újrahasznosítás lehetősége. A tisztított szennyvíz újrahasznosítás releváns intézkedés a VKI céljainak megvalósításához és egy forráshatékonyabb gazdaság kialakításához.

Fontos tisztázni, hogy mit értünk a víz újrahasznosítás fogalma alatt. A különböző használatos fogalom-meghatározásokat összevetve megállapítottam, hogy a World Health Organization (WHO) definíciója, a közérthető megfogalmazás mellett, tartalmazza a tevékenység kritikus elemeit. A WHO szerint a víz újrahasznosítás azt a szennyvíztisztítás következtében generálódó víz használatot jelenti, amely az egészségügyi és környezeti kockázatok, illetve a vonatkozó nemzeti és uniós jogszabályok figyelembevételével megfelel a felhasználási cél szerint meghatározott minőségi előírásoknak. [13]

Az EB 2007-ben kiadta a *„Bizottság Közleménye az Európai Parlamentnek és a Tanácsnak az Európai Unióban a vízhiány és az aszály jelentette kihívás kezeléséről”* című dokumentumát, amelyben felhívta a figyelmet, hogy a további vízellátási infrastruktúrák létesítését megelőzően a vízfelhasználás hatékonyságának növelésére ösztönző árpolitikát kell kialakítani és meg kell vizsgálni az alternatív megoldási lehetőségeket. [10] A víz újrahasznosítás alkalmazása valós alternatív megoldást jelenthet az aszályos és a vízhiányos területeken azáltal, hogy eddig kihasználatlan készletként megpróbáljuk hasznosítani a tisztított szennyvizet. Az európai vízkészletek jelentőségéről szóló jelentés újra felhívta a figyelmet a víz újrahasznosítás fontosságára. [14] Az EB 2012-es aszály és vízhiány politika felülvizsgálatából kiderült, hogy egyes EU tagországokban további vízellátási infrastrukturális jellegű beruházások történtek anélkül, hogy kiaknázták volna a javasolt lehetőségeket.

A víz újrahasznosítási projektek sikeres megvalósíthatóságának megalapozása érdekében az EU 2015. évi vízigazgatói ülésen a vízigazgatók egyetértettek abban, hogy a víz újrahasznosítási útmutató véglegesítését kiemelten kell kezelni. A végrehajtás érdekében az EB a Stratégiai Koordinációs Csoport (SDG) irányítása alatt egy munkacsoport létrehozását kezdeményezte. A munkacsoportnak két fő célkitűzése van. Az első célkitűzés a víz újrahasznosítási útmutató véglegesítése volt, amely 2016 sikeresen elkészült. A másik kiemelt feladat a vízminőségi minimum követelmények meghatározása, amely jelenleg a Közös Kutatóközpont (JRC) bevonásával készül. A munkacsoport célkitűzéseinek megvalósításában Magyarország is részt vesz.

Az egyik alapelv a víz újrahasznosítás során, hogy a mennyiségi problémák megoldása nem vezethet vízminőségi problémákhoz. A víz újrahasznosítás - biztonságos és költséghatékony feltételek mellett - értéket jelenthet Magyarország számára. Az aszály és vízhiány által veszélyeztetett területeken javaslom a víz újrahasznosítás lehetőségeinek részletesebb feltárását. A tisztított szennyvíz újrahasznosítás előnyeinek és hátrányainak teljes skáláját fel kell tárni, amelyek általában a helyi adottságoktól függenek, ezért mindig eseti alapon kell meghatározni őket. Az újrahasznosítást úgy kell megvalósítani, hogy az konzisztens legyen az EU környezeti célkitűzésével. A víz újrahasznosítás megvalósításának fontos eleme, hogy a releváns érintettek bevonásra kerüljenek. [15] A víz újrahasznosítási projektek megvalósítása során feltételezhetően hibás lenne azt a megközelítést alkalmazni, hogy kidolgozható egy általános, minden tervezési körülmény között alkalmas megoldás. Nem lehet sablonszerűen előre determinálni a megvalósítást, viszont a jó gyakorlat kialakítása kulcskérdés a társadalmi elfogadottság elősegítésében.

Tisztított szennyvíz újrahasznosítás Magyarországon

A megfelelően tisztított szennyvíz számos célra felhasználható. A közleményben nem határoztam meg a hasznosítási módok között prioritást, mivel ez a terület egyedi igényeitől függ. A potenciális hasznosítási lehetőségek különbözőképpen kategorizálhatók a hasznosítás típusa szerint, úgymint mezőgazdasági, ipari vagy települési használat. A fejezet keretében a tisztított szennyvíz mezőgazdasági célú újrahasznosításának magyarországi tapasztalataival foglalkoztam.

Magyarországon korábban az 1970-es, 1980-as években alkalmazták kísérleti jelleggel a tisztított szennyvíz felhasználását, a gyulai mintaterületen, nyárfás terület öntözésére.

Kezdetben a cél még nem a gazdasági haszonszerzés volt, hanem magának a szennyvíznek az elhelyezése és tisztítása. A gyulai területtel közel egyidejűleg, a kecskeméti modelltelepen, a nyárfás öntözés mellett már más növénykultúrák öntözésére is sor került. [16] Ezek a kezdeti kísérletek a rendszerváltás közeledtével, valószínűsíthetően a tulajdonviszonyok változásával és a támogatottság hiányában fokozatosan megszűntek. Kisebb léptékű nyárfás szennyvíztisztító telepek jelenleg is működnek (pl.: Szakoly, Nagycserkesz), de a létesítmények célja a szennyvíz elszikkasztása, nem a gazdasági haszonszerzés.

A nagykállói szennyvíztisztító telep közelében korábban szintén történt nyárfás hasznosítás. A szennyvíztisztító telepet 2014-ben a *„Nemzeti Települési Szennyvízelvezetési és -tisztítási Megvalósítási Program”*-ban felújították. A tervek szerint, az elfolyó szennyvíz vegetációs időszakban egy energiafűz ültetvényre, vegetációs időszakon kívül pedig a másodlagos befogadó vízfolyásba került volna. A szennyvíztisztító telep közvetlen közelében elhelyezkedő öntözésre alkalmas terület önkormányzati tulajdonban van és egy részét 2015-ben betelepítették energiafűzzel, amely 2016-ban kiszáradt. A terület gyenge termőképességű homokos talaja elméletben alkalmas lenne az energiafűz termesztésére. Az önkormányzat az energiafűz újratelepítését tervezi, amely a megfelelő technológia alkalmazásával alkalmas lehetne a környékbeli közintézmények fűtésére a téli időszakban.

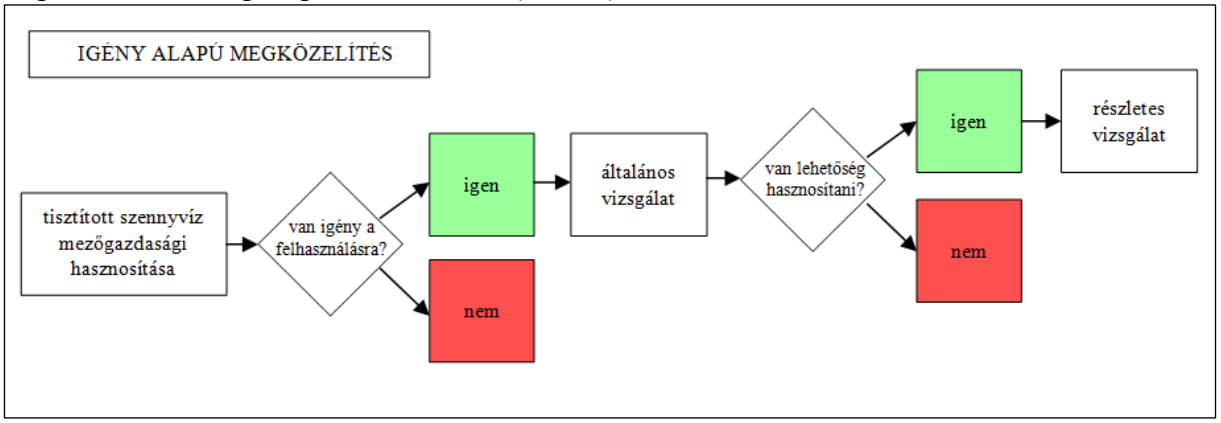
A tisztított szennyvíz mezőgazdasági hasznosításának magyarországi tapasztalatait vizsgálva megállapítottam, hogy az éghajlatváltozás hatásainak mérséklését elősegítő beruházások megvalósításához ismerni kellene, hogy milyen területeken valósítható meg nagy valószínűséggel biztonságosan és költséghatékonyan a víz újrahasznosítás.

A TISZTÍTOTT SZENNYVÍZ MEZŐGAZDASÁGI HASZNOSÍTÁSÁRA ALKALMAS TERÜLETEK MEGHATÁROZÁSA

A tisztított szennyvíz mezőgazdasági hasznosításában rejlő lehetőségek kihasználásához két elengedhetetlen feltételnek kell egyidejűleg teljesülni:

1. *biztonságosság*
2. *költséghatékonyság*

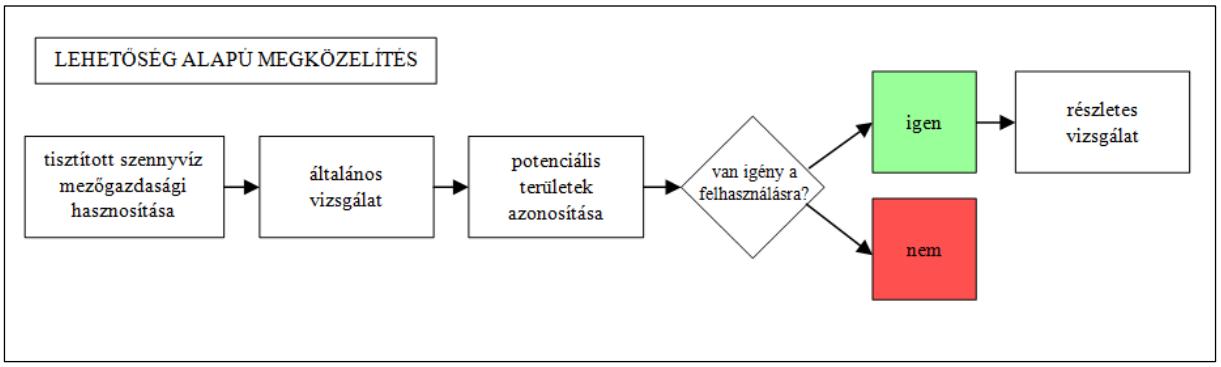
Az általános alapfeltételek kizárólag akkor teljesíthetők, ha mezőgazdasági hasznosításra alkalmas területen valósítjuk meg a beruházást. Felmerül a kérdés, hogy hol lehetnek olyan területek Magyarországon, ahol a tisztított szennyvízhasznosítás biztonságosan és költséghatékonyan megvalósítható. A tisztított szennyvíz felhasználásával történő gazdasági haszonszerzés igényének kielégítéséhez kétfajta megközelítési módszert dolgoztam ki, az igény alapú és a lehetőség alapú módszereket (1. ábra).



1. ábra Igény alapú kiválasztási eljárás metodikája (saját szerkesztés)

Az első változatot igény alapú megközelítésnek neveztem el. A megközelítésnek ebben a formájában az eljárás elején keletkezik egy konkrét igény (pl.: vállalkozó, önkormányzat) a hasznosításra vonatkozóan. Az igény keletkezésének ismerete jellemzően származhat egy igényfelmérés eredményéből. A megközelítés független az igény keletkezésének okától és forrásától. A megközelítés során, az igény keletkezésének helyét kell, különböző szempontok alapján meghatározott paraméterek alapján, általánosan vizsgálni. Ha az általános vizsgálat lefolytatása után igazolttá válik, hogy fennáll a hasznosítás lehetősége, akkor le kell folytatni a részletes vizsgálatot. Ha az általános vizsgálat során kiderül, hogy a terület alkalmatlan, akkor az eljárás lezárul, a részletes vizsgálat nélkül. A vizsgálat általános és részletes típusra való megosztását az eljárási idő és a költséghatékonyság indokolja.

A második változatot lehetőség alapú megközelítésnek neveztem el (2. ábra).



2. ábra Lehetőség alapú kiválasztási eljárás metodikája (saját szerkesztés)

A második változatnál, az igény alapú megközelítéshez képest, fordított logikát alkalmaztam. A lehetőség alapú megközelítés kezdeti szakaszában nem ismertek az igények. Az igények keletkezését megelőzően, a megfelelően kiválasztott paraméterek alapján, általánosan vizsgálok egy nagyobb kiterjedésű területet (pl.: Magyarország). Az előzetes vizsgálat alapján elvégzett szűrés eredménye a mezőgazdasági hasznosításra potenciális területek azonosítása. A nagyobb kiterjedésű összefüggő területektől eljutunk a kisebb részterületek szintjére. A területek szelektálásának az a célja, hogy egy átlátható, könnyen értelmezhető kiindulási alapot biztosítson az esetleges igények kielégítéséhez. A lehetőség alapú megközelítésénél termékként elkészül egy olyan lehatárolás, amely alapján egy esetleges vállalkozó vagy önkormányzat, aki tisztított szennyvíz hasznosításával szeretne beruházni, megnézheti, hogy a saját földterülete alkalmas lehet-e a kiválasztott célra és érdemes-e további forrás felhasználásával részletes vizsgálatot végezni.

A kutatásom keretében a megközelítési módszerek közül, a 2. változatot alkalmaztam, mivel nem rendelkeztem az igények ismeretével, és a fő célkitűzésem az volt, hogy meghatározzam a tisztított szennyvíz mezőgazdasági hasznosítására feltételesen alkalmas területeket.

A területlehatárolás kritikus része a kiválasztási szempontok meghatározása. A tisztított szennyvíz felhasználással kapcsolatos beruházások sikeressége érdekében teljes körűen fel kell tárni azokat a paramétereket, amelyek befolyásolhatják az eredményt. A hatékony tervezéshez nem elegendő egyszerűen a tényezők halmazának összegyűjtése, hanem azokat strukturáltan rendszerezni kell. A tudományos közleményem keretében kiemelt hangsúlyt fektettem a kritériumtényezők meghatározására. A javasolt szempontrendszer kialakítása során összesen 18 döntési paramétert azonosítottam, amit 6-os csoportokban 3 osztályra bontva kategorizáltam (1. ábra).

Az első osztályban *a kizáró tényezőket* gyűjtöttem össze. A kizáró tényezők olyan egyszerű választásos paraméterek, amelyek fennállása esetén a vizsgált célterületen a beruházás nem valósítható meg. Ezek az alosztályok képezik a tiltott területek listáját. Például amennyiben egy

terület védett vízbázisként azonosítható, akkor ott a tisztított szennyvíz felhasználás nem javasolt.

TERÜLETLEHATÁROLÁSI SZEMPONTRENDSZER		
	I. KIZÁRÓ TÉNYEZŐK	I.1. ártéri öblözet
		I.2. belvízveszélyeztetett terület
		I.3. nitrátérzékeny terület
		I.4. Natura2000 terület
		I.5. védett vízbázis terület
		I.6. beépített terület
	II. ÁLTALÁNOS VIZSGÁLAT	II.1. aszály által veszélyeztetett
		II.2. talajtípus
		II.3. szennyvíztisztító telep távolsága
		II.4. szaghatás
		II.5. feldolgozó távolsága
		II.6. FAV mennyiségi állapot
	III. RÉSZLETES VIZSGÁLAT	III.1. talajállapot
		III.2. domborzat
		III.3. költségmegtérülés
		III.4. kockázatelemzés
		III.5. tisztítási technológia
		III.6. növénykultúra

1. táblázat Területlehatárolási szempontrendszer (készítette a szerző)

A második osztályba az általános vizsgálati szempontokat soroltam. A 2. osztály olyan elemeket tartalmaz, amelyek vizsgálata egyszerű választást igényel. Például kiválasztjuk az erősen aszályos területeket az aszálytérképek alapján, amelyek - Magyarország területét különböző osztályokra bontva - szemléltetik a veszélyeztetettséget, és ezt követően már ezen a leszűkített területen folytatunk további lehatárolásokat. A tervezésnél fontos szempont, hogy minél rövidebb úton, gravitációsan eljuttatható legyen a tisztított szennyvíz a célterületre. Egyszerű eljárással eldönthető például az is, hogy olyan területeket határoljunk le, amely a szennyvíztisztító telepektől egy adott távolságra helyezkednek el. Az általános vizsgálatok lefolytatását követően már a rendelkezésünkre áll egy olyan fedvény[1], amely alapján átfogó képet lehet alkotni a tisztított szennyvíz mezőgazdasági hasznosítására alkalmas területekről Magyarországon.

A lehetőség alapú megközelítést alkalmazva, ha ezeken a területeken igény keletkezik a felhasználásra, akkor ott releváns lehet a részletes vizsgálat lefolytatása. A részletes vizsgálat bemutatását terjedelmi okok miatt a tudományos közleményben nem részletezem.

A területlehatárolási szempontrendszer elkészítésekor arra a következtetésre jutottam, hogy javasolt lenne az egyes tényezőket számszerűsíteni és súlyozás alkalmazásával egy optimalizációs eljárássá továbbfejleszteni.

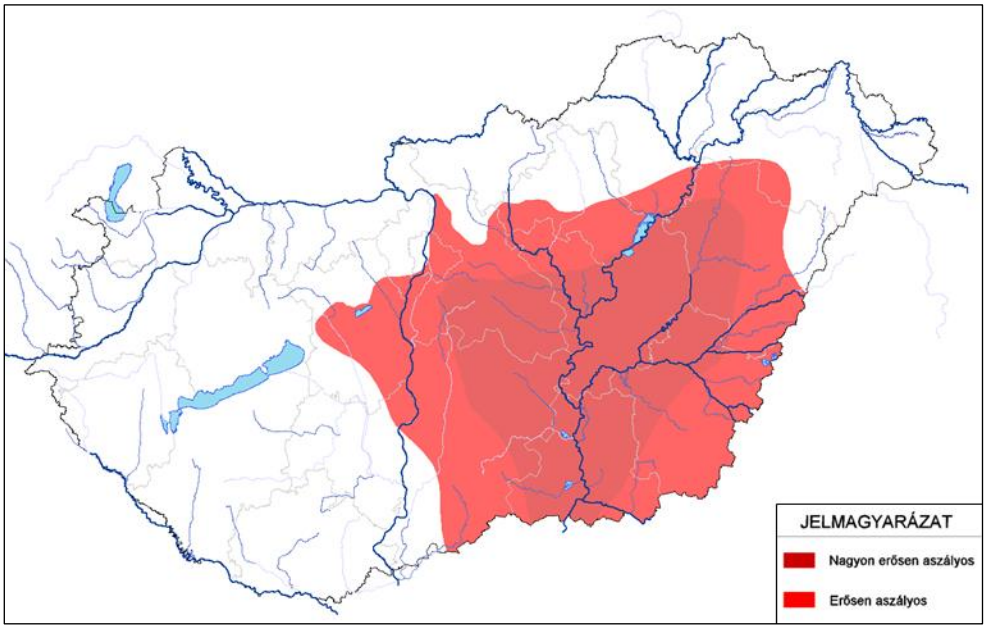
Az amerikai Stanford Egyetem készített egy települési víz újrahasznosításra optimalizált döntéstámogató szoftvert, amit a Colorado állambeli Golden városában teszteltek. [17] A

[1] Megadott szempontrendszer szerint kategorizált, logikailag összefüggő objektumok összességének digitális térképi megjelenítése.

kutatásuk alapján továbbvizsgálható lenne, hogy egy tisztított szennyvíz mezőgazdasági újrahasznosítására vonatkozó eljárás hogyan válhatna programozhatóvá.

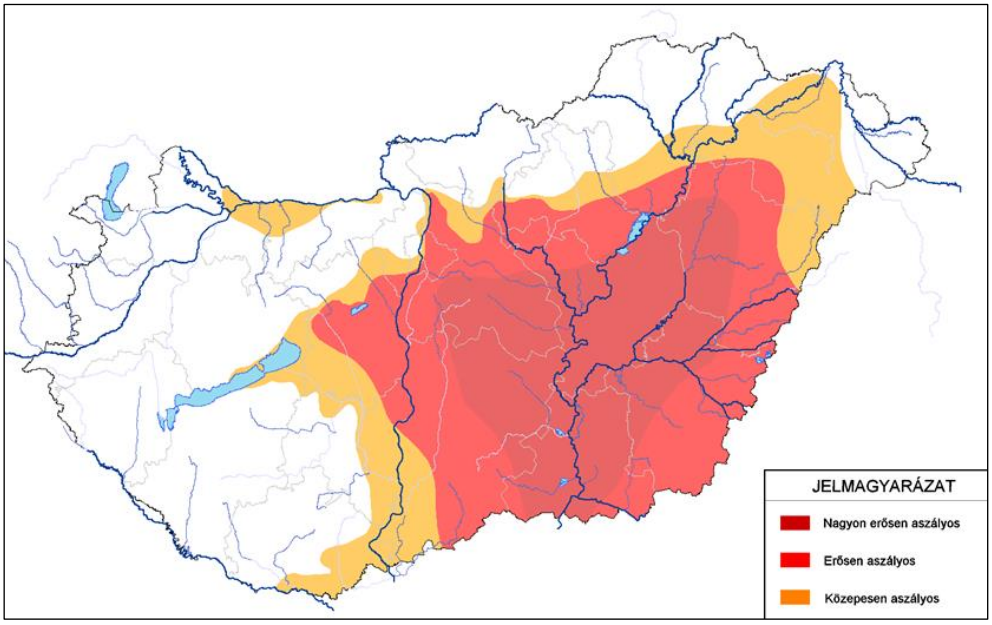
A területlehatárolási szempontrendszerben található elemek szerint különböző fedvények felhasználásával elkezdtem a tisztított szennyvíz mezőgazdasági felhasználására potenciálisan alkalmas területek magyarországi meghatározását. Az eljárás során kiindulási alapként tekintettem az EU víz újrahasznosítási útmutatójának javaslatát, amely szerint a víz újrahasznosítás vizsgálata elsősorban az aszályok és a vízhiányok által veszélyeztetett területeken indokolt. A tisztított szennyvíz öntözési felhasználásának társadalmi és környezeti elfogadottsága tagállamonként nagyon különböző. A tisztított szennyvíz közvetlenül emberi fogyasztásra szánt növények termesztéséhez való felhasználásához jelenleg kevés információ áll rendelkezésre és alacsony a társadalmi elfogadottsága, mivel potenciálisan nagyobb kockázattal jár. Egészségügyi szempontból jelenleg társadalmilag elfogadottabb a kevésbé kockázatosnak ítélt energetikai célú növények termesztéséhez történő felhasználás.

A területlehatárolás során feltételeztem, hogy az eljárás különböző stádiumának eredményei jól szemléltethetők, ha első lépésben Magyarország területéből a Pálfai féle aszálytérképet felhasználva megjelenítem azt a részterületet, amely az aszály által leginkább veszélyeztetett és a további kizárásokat már ebből kiindulva végzem el. [18] A 3. ábra a nagyon erősen aszályos (vörös) és az erősen aszályos (piros) területeket mutatja be.



3. ábra Aszálytérkép – kiemelten aszályos terület (a szerző szerkesztése a [14] alapján)

Az éghajlatváltozás következtében az elmúlt években jelentősen erősödött az aszályveszélyeztetettség olyan területeken is, amelyek korábban mindössze közepesen aszályosnak minősültek. Az éghajlatváltozás miatt indokoltnak tekintettem, hogy a korábban közepesen aszálynak minősített területeket is tartalmazza a lehatárolásom. A 4. ábrán a lehatárolás tartalmazza a közepesen aszályos (narancssárga) területeket.

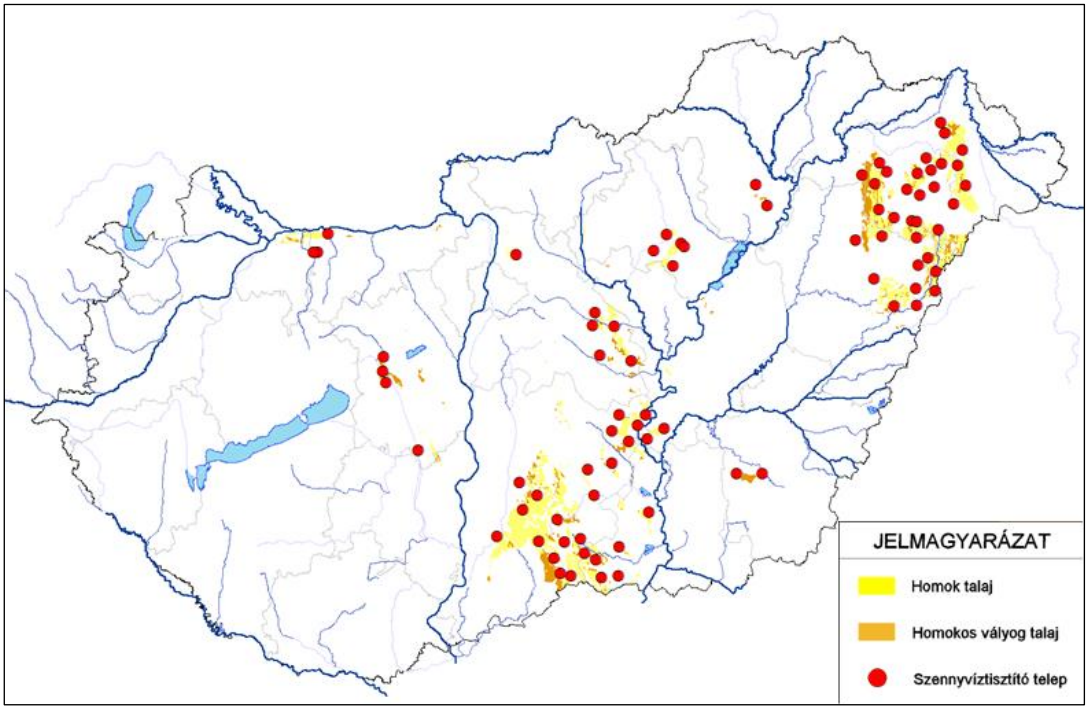


4. ábra Aszálytérkép – kiemelten aszályos és közepesen aszályos terület (a szerző szerkesztése a [14] alapján)

A színtelen részeket az alacsonyabb mértékű aszályveszélyeztetettség miatt nem vizsgáltam tovább az eljárás további részében. A területlehatárolási szempontrendszer alapján a kiindulási lehatárolásom területéből kizártam azokat a területeket, amelyek árvíz vagy belvíz által veszélyeztetettek. Ezt követően a Nitrát Irányelv és 27/2006. (II. 7.) Kormányrendelet alapján kizártam a hasznosításra alkalmas területek közül a nitrátérzékenyeket. A vonatkozó jogszabályok alapján, a biztonságosság elvét érvényesítve, kizártam a Natura2000 és a védett vízbázis területeket, továbbá mezőgazdasági hasznosításra értelemszerűen nem alkalmasak a beépített területek. Kizártam a települési belterületeket is.

A kizárások után fennmaradó területek további vizsgálata során előtérben helyeztem, hogy a víz újrahasznosítás elsősorban olyan gyengébb termőképességű, rossz vízháztartású talajokon lenne indokolt, amelyek kevésbé alkalmas élelmiszernövények termesztésére. Az energiafűz például könnyen kiszáradó, gyengébb minőségű, homoktalajokon is termeszthető. A növény egyik előnye a tág ökológiai tűrőképesség. Ezért az eljárás során, a fennmaradó területet tovább szűkítettem, a talajtípus szerint, homokos (világossárga) és homokos vályog (barna) talajokra (5. ábra).

A szempontrendszer alkalmazása alapján, Magyarországon elsősorban a Duna-Tisza közi Homokhátság és a Nyírség területe azonosítható a tisztított szennyvíz mezőgazdasági felhasználása szempontjából releváns területként.



5. ábra A tisztított szv. mezőgazdasági felhasználására potenciálisan alkalmas területek (saját szerkesztés)

A potenciális területek azonosítása során, arra az eredményre jutottam, hogy Magyarország területének megközelítőleg 3 %-ára becsülhető az a része, amely alkalmas lehet a tisztított szennyvízzel való öntözésére. A Települési Szennyvíz Információs Rendszer (TESZIR) szerint Magyarországon 819 db szennyvíztisztító telep van, amelyből a kutatásaim alapján maximum 85 db telep esetében lehet indokolt a részletes vizsgálatok elvégzése (5. ábra). A becsült terület és ezzel összefüggésben a telepszám a részletes vizsgálatok elvégzését követően várhatóan nagyságrendileg lecsökkene.

Az 6. ábra egy potenciális hasznosítási területet szemléltet, amelyet a fentiekben meghatározott kritériumok alapján választottam ki.

6. ábra Potenciális hasznosítási terület kijelölése (saját szerkesztés)

Összességében megállapítható, hogy a potenciális területek kijelöléséhez első lépésben, a rendelkezésre álló információk alapján, ki kell választani, hogy melyik megközelítési eljárást alkalmazzuk. Az igény alapú megközelítés során az igények ismeretének tükrében kell alkalmazni a javasolt kiválasztási szempontrendszert, kezdve a kizáró tényezőkkel, az általános vizsgálaton keresztül a részletes vizsgálat lefolytatásáig. A lehetőség alapú megközelítés során pedig a szempontrendszer alkalmazása során, az általános vizsgálat lefolytatását követően válik indokolttá a részletes vizsgálat lefolytatása.

KÖVETKEZTETÉSEK

Az éghajlatváltozás következtében a vizek állapotjavulásának mértéke lelassulhat, illetve fennáll a veszélye az állapotértékelési eredmények romlásának, tovább nehezíthetve a Víz Keretirányelv (VKI) fő célkitűzésének teljesítését. A Magyarországon képződő tisztított szennyvizek hasznosításában rejlő potenciál kihasználásával hozzájárulhatnánk a VKI célkitűzéseinek eléréséhez. A tisztított szennyvíz, Magyarország egyes területein, alkalmas lehet különböző növénykultúrák öntözésére.

A tisztított szennyvíz felhasználás biztonságos és költséghatékony megvalósítása érdekében javaslom a területlehatárolási szempontrendszer alkalmazását. A szempontrendszer értékét az adja, hogy strukturáltan tartalmazza a területlehatároláshoz szükséges paramétereket. Az eljárás során elsőként a kizáró tényezők alapján meg kell vizsgálni a területet, majd ezt követően le kell folytatni az általános vizsgálatot. Az általános vizsgálat eredménye alapján célszerű a részletes vizsgálat végrehajtása. A javasolt szempontrendszer alkalmazása elősegítheti a vízhiányjelenségek megelőzését célzó rentábilis beruházások kivitelezését.

FELHASZNÁLT IRODALOM

[1] NASA GODDARD INSTITUTE FOR SPACE STUDIES: *January 2018 was fifth warmest January on record*; NASA 2018. https://climate.nasa.gov/news/2683/january-2018-was-fifth-warmest-january-on-record/ (letöltve: 2018.02.17.)

[2] NEREM, R. S., BECKLEY, B. D., FASULLO, J. T., HAMLINGTON, B. D., MASTERS, D., MITCHUM, G. T.: *Climate-change–driven accelerated sea-level rise detected in the altimeter era*; Proceedings of the National Academy of Sciences, 2018.

[3] ALFIERI, L., DOTTORI, F., BEETS, R., SALAMON, P., FEYEN, L.: *Multi-Model Projections of River Flood Risk in Europe under Global Warming*; Climate 2018 VI. 1. (2018) 1-19. o.

[4] HORNYACSEK J.: *A katasztrófák elleni védekezés műszaki szakfeladatainak rendszere, a végrehajtás követelményei, módszerei és eszközei*; Műszaki Katonai Közlöny, XXVIII. évfolyam, 2018. 1. szám, pp.103-139.

[5] PIECZKA I., BARTHOLY J., PONGRÁCZ R.: *Éghajlatváltozási szcenáriók a Kárpát-medence térségére a precis klímamodell eredményei alapján;* ELTE 2012.

[6] TÓTH T.: *A vízhiányos helyzetek kialakulásának megelőzése és hatékony kezelésének elősegítése* In: FÖLDI L. (Szerk): *Éghajlatváltozás okozta kihívások és lehetséges válaszok*; NKE 2018.

[7] EUROPEAN COMMISSION: *Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for Community action in the field of water policy*; Official Journal of the European Communities. (2000) 1–73. o.

[8] ORSZÁGOS VÍZÜGYI FŐIGAZGATÓSÁG: *Vízgyűjtő-gazdálkodási terv – 2015.* OVF 2015. https://www.vizugy.hu/index.php?module=vizstrat&programelemid=149 (letöltés : 2016.09.09.)

[9] UNITED NATIONS: *United Nations Convention to Combat Desertification.* United Nations, 1994.

[10] EUROPEAN COMMISSION: *Adressing the challange of water scarcity and droughts in the European Union*; EC, 2007. http://eur-lex.europa.eu/LexUriServ/-LexUriServ.do?uri=COM:2012:0673:FIN:EN:PDF (letöltés: 2013.10.21.)

[11] FLÖRKE, M., WIMMER, F., LAASER, C., VIDAURRE, R., TRÖLTZSCH, J., DWORAK, T., STEIN, U., MARINOVA, N., JASPERS, F., LUDWIG, F., SWART, R., GIUPPONI, C., BOSELLO, F., MYSIAK, J.: *Final Report for the Project Climate Adaptation - Modelling Water Scenarios and Sectoral Impacts;* Center for Environmental Systems Research 2011.

[12] NOVÁKY B.: *Az éghajlatváltozás vízgazdálkodási hatásai*; MTA 2012.

[13] WORLD HEALTH ORGANIZATION: *Guidelines for the safe use of wastewater, excreta and greywater*; WHO 2006.

[14] EUROPEAN COMMISSION: *A Blueprint to Safeguard Europe's Water Resources;* EC 2012. http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52012DC-0673&from=EN (letöltve: 2012.11.29.)

[15] EUROPEAN COMMISSION: *Guidelines on Integrating Water Reuse into Water Planning and Management in the context of the WFD*; EC 2016. http://ec.europa.eu/environment/water/pdf/Guidelines_on_water_reuse.pdf (letöltve: 2016.12.20.)

[16] VERMES L.: *Vízgazdálkodás*; Mezőgazdasági Szaktudás Kiadó 1997.

[17] LEE, E. J., CRIDDLE, C. S., GEZA, M., CATH, T. Y., FREYBERG, D. L.: *Decision support toolkit for integrated analysis and design of reclaimed water infrastructure;* Water Research (2018), DOI: 10.1016/j.watres.2018.01.037.

[18] PÁLFAI I.: Aszályos évek az Alföldön 1931 és 2010 között; Szegedi Tudományegyetem, 2010. http://www.geo.u-szeged.hu/regi/system/files/14-Kiadvanyok/egyeb/Kornyezeti_valtozasok_az_Alfoldon/10-p%E1lfai.pdf (letöltve: 2014.02.15.)

HADMÉRNÖK

XII. Évfolyam 3. szám – 2018. szeptember

A VÉDELEMGAZDASÁG BIZTONSÁGPOLITIKAI ÖSSZEFÜGGÉSEI NAPJAINKBAN

DEFENSE MANAGEMENT SYSTEM IN THE ACTUAL SECURITY THREATS

BABOS Tibor; BEREGI Alexandra Lilla

(ORCID: 0000-0001-7459-8349); (ORCID: 0000-0003-0436-4875)

babos@uni-obuda.hu; beregi@uni-obuda.hu

Absztrakt

A tanulmány tézise, hogy a védelemgazdaság, védelmi célú tartalékolás szabályozása ma Magyarországon erősen hiányos és elavult. Ezért mielőbb célszerű megalkotni egy, az aktuális és új biztonsági kihívásokra is választ adó, az EU- és NATO-tagság követelményeit is teljesítő, nemzeti összkormány-zati rendszert, amelyben a központi és a területi közigazgatás, a szakmai szervezetek, a fegyveres erők, a nem kormányzati szervezetek, valamint a piaci szereplők különálló feladatrendszere összekapcsolódik, összességében pedig egységes egészet képez. A dolgozat bemutatja (1) a biztonságot alakító katonai és természeti tényezőket, (2) a védelemi igazgatás legmeghatározóbb történeti, jogalkotási sarokköveit; (3) a védelemgazdaság helyzetét a II. világháborúban és hidegháborúban, a rendszerváltozáskor és napjainkban, (4) a védelemgazdaság aktualitását, ajánlásait Magyarország vonatkozásában.

Kulcsszavak: *biztonság, védelmi igazgatás, védelmi felkészítés, védelmi célú tartalékolás*

Abstract

The thesis of the study is that the regulation of defense economy and defense reserve stock system is heavily deficient and outdated in Hungary today, therefore it is important to create a new complex defense management scheme based on the following guidelines: support of Hungary's political; economic and defense interests; response to the actual security threats; transparency with the EU and NATO requirements, imbedded into the central, regional and territorial public administration as well as into the state authorities; and finally connected to the non-governmental organizations, and to the market economy players. In order to justify the thesis, the study first discusses the main military and natural factors of security. The second part presents the relevant historical and legislative cornerstones of the Hungarian defense administration i.e. features of the defense economy in the II. World War and Cold War, in the change of the political regime in the 1990s and afterwards. The third part describes the present context of the defense economy and defense reserve stock system. Finally the author summarizes the main messages of the topic and offers concrete recommendations for a more efficient national defense management system.

Keywords: *security, defense management, defense preparation, defense reserve.*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.01.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.17.

BEVEZETÉS

A biztonság átalakulása a 21. század kezdetén, a korábbi évtized poszthidegháborús trendjeibe illeszkedve folytatódott. A nyolcvanas évek végén megindult politikai, gazdasági és társadalmi változások, a globalizáció kiteljesedése elsöpörte a bipoláris világrendet, amelynek nyomán megváltozott a világhatalmi egyensúlya, felgyorsult a tudományos-technológiai fejlődés, az államok egymásra utaltsága megnövekedett, miközben – a határok általános elgyengülésével – a fenyegetések egyetemessé, egyben közössé váltak. A „régi", hagyományosnak nevezhető fegyveres konfliktusokat felváltották az „új" biztonsági kihívások: az alacsony intenzitású biztonsági kockázati tényezők, a tömegpusztító fegyverek proliferációja, a nukleáris, vegyi, biológiai technológiák kontroll nélküli fejlesztése, a számítógépek tömeges felhasználásából adódó kiber-fenyegetések. Továbbá az egyenlőtlen társadalmi és gazdasági fejlődésből származó érdekellentétek, vagy a nem állami szereplők, terrorcsoportok által szervezett támadások, mind-mind új, megelőző és védelmi természetű célrendszerek meghatározására késztetik az államokat, túlélésük jegyében.[1] E körülmények között a védelemgazdaság, a védelmi felkészítés és a védelmi célú tartalékolás új értelmezést kap, meghatározó jelentősége ugyan megmarad, azonban átértékelődik.

A védelmi igazgatás közvetlen kapcsolatban áll a biztonsági fenyegetésekkel, kockázatokkal és nemzetközi folyamatokkal. Másként fogalmazva: a mindenkori biztonsági körülmények folyamatosan befolyásolják a védelmi igazgatás szervezését és a védelmi felkészítés célrendszerét. A védelemgazdaság, a nemzetgazdaság és a védelmi képességek koherenciáját jelenti. A védelmi felkészítés egyik legfontosabb alapeleme a védelmi igazgatás. A nemzetgazdaság védelmi – vagyis békeidőszaktól eltérő helyzetekre való – felkészítésének meghatározó és megkerülhetetlen eleme a védelmi célú tartalékolás.

A tanulmány az alábbi kérdésekre keresi a választ:

- Melyek az védelmi felkészítést, -igazgatást és -tartalékolást befolyásoló fontosabb biztonsági összetevők?
- Melytényezők mentén határozható meg a védelemgazdaság és annak elemei?
- Mik a védelemi igazgatás kialakításának mérföldkövei Magyarországon a hidegháború időszakában, a rendszerváltozáskor és napjainkban?
- Melyek a védelemi igazgatás legmeghatározóbb jogalkotási sarokkövei Hazánkban?
- Hogyan jellemezhető a védelemgazdaság és a védelmi tartalékolás kapcsolata ma Magyarországon?

A tanulmány tézise, hogy a védelmi felkészítés, azon belül a védelemgazdaság és védelmi célú tartalékolás szabályozása és gyakorlati megvalósítása ma Magyarországon hiányos, elavult, ezért indokolt megalkotni hazánk biztonsági érdekeinek megfelelő, az új biztonsági kihívásokra is választ adó, valamint az EU- és NATO-tagság követelményeinek is megfelelő nemzeti, összkormányzati rendszert. A rendszerben a központi és a területi közigazgatás, a szakmai szervezetek, a fegyveres erők, a nem kormányzati szervezetek, valamint a piaci szereplők lehatárolható és különálló feladatrendszere funkcionálisan kapcsolódik, összességében pedig egységes egészet, komplex védelmi rendszert képez.

A tanulmány a tézis igazolása érdekében először bemutatja a biztonságot meghatározó alapvető tényezőket, számba veszi a védelmi igazgatás jogszabályi hátterét a 90-es évektől egészen napjainkig. Azt követően az új biztonsági kihívások elemzésén és értékelésén keresztül ismerteti a gazdaságmozgósítás és a gazdaság békeidőszaki, védelmi célú felkészítésének alternatív lehetőségeit. A tanulmány végül összefoglalja a bekövetkezett változások hatásait és ajánlásokat fogalmaz meg a gazdaság védelmi felkészítésének aktuális helyzetére vonatkozóan Magyarországon.

A BIZTONSÁGOT MEGHATÁROZÓ FONTOSABB TÉNYEZŐK

A védelmi igazgatás közvetlen kapcsolatban áll a nemzetközi biztonsági fenyegetésekkel és kockázatokkal. A mindenkori biztonsági körülmények folyamatosan befolyásolják a védelmi igazgatás szervezését és a védelmi felkészítés célrendszerét. A védelmi igazgatás rendszerében jelentős hangsúlyt kap a megelőzés és a felkészítés. A téma megértése szempontjából fontos számba venni a nemzetközi biztonsági folyamatok legfontosabb elemeit, értékelni és elemezni azok tartalmát.[2]

A nyolcvanas évek végén a kelet–nyugati szembenállás megszűnésével gyökeresen új globális stratégiai helyzet alakult ki. A közép- és kelet-európai államok sorban szakítottak a szocializmus gyakorlatával, a központosított államrenddel, s deklarálták, hogy a Nyugat és annak társadalmi rendszere felé fordulnak. E történések széles körű dezintegrációs, ugyanakkor integrációs tendenciákat idéztek elő. A Kelet-Európában végbemenő események radikálisan megváltoztatták a világpolitikai arculatát, s az annak hatására meginduló változások még ma is meghatározók a kontinensen. A jelenlegi újszerű, a korábbinál sokrétűbb és instabilabb helyzetben a biztonságot befolyásoló tényezők, veszélyforrások, kockázatok is más hangsúlyt kaptak, újakkal bővültek. Előtérbe kerültek a biztonság egyéb alkotóelemei: a gazdasági, a pénzügyi, a társadalmi, a kulturális, a vallási, a környezeti, a közbiztonsági, vagy a migrációs problémák mellett dominánsan jelentkeznek a technológiai és informatikai kockázatok.

Földünk biztonságát még mindig az átfogó történelmi korszakváltás következményeiből adódó átmenetiség, illetve a dinamikus restruktúrálódás, a piaci és politikai konkurenciaharc, a regionalizáció, lokalizáció és a nacionalizmus jellemzi, miközben a digitális forradalom és annak kiteljesedése meghatározó történelmi jelenséggé lép elő. Míg a nyolcvanas évek óta a második világháborúban kialakult hidegháborús rend szétporladása egyre inkább dinamikáját veszti, addig az új globális hatalmi centrumok súlyközéppontjai átalakulnak és újradefiniálódnak Ázsiában, Észak-Amerikában és Európában. E folyamatban az amerikai és a nyugat-európai gazdasági potenciál ugyan továbbra is meghatározó, azonban már egyértelműen nem domináns. A hatalmi központok kialakulása és sikere a digitális, informatikai, információs rendszerek minél aktívabb, céltudatosabb és szélesebb felhasználásán múlik.

Ezzel párhuzamosan mind a globális, mind pedig az európai biztonsági kihívások átfogó és nagyléptékű mutációt is produkálnak. Ma egyre makulátlanabbul és erélyesebben juthatnak kifejezésre a nemzetállamokhoz nem minden esetben köthető, viszont transznacionális karakterisztikát öltő fenyegetettségek. Az elmúlt két-három évtizedben új biztonsági kihívások jelentek meg: aszimmetrikus biztonsági kockázati tényezők; tömegpusztító fegyverek proliferációja. Napjaink legnagyobb kihívásai: nukleáris, vegyi, biológiai technológiák; génmanipuláció; tömegpusztító fegyverek hordozóeszközei; számítógépek tömeges felhasználása; veszélyforrások, technológiák, illetéktelen kézbe jutása. A globalizáció következménye a terrorizmus, ami veszélyt jelent minden állam bel- és külbiztonság politikájára. Új kihívásként jelenik meg a demográfia és migráció, amely megmutatkozik kulturális, vallási, politikai, gazdasági, klimatizáció és éghajlatváltozásokban is. Európa migrációs politikája olyan jellegű feszültséget okozhat, melynek következménye fegyveres konfliktusokhoz vezethet (pl.: határok lezárása). A nemzetközi szervezett bűnözés megmutatkozik kábítószer csempészetben és kábítószer kereskedelemben egyaránt.[1] Természetüket tekintve korunk biztonsági kockázati tényezői térben kisebb kiterjedésűek, azonban sokrétűbbek, szerteágazóbbak, s egyben dinamikusabbak is; hatásukat tekintve könnyen akár globális méreteket is ölthetnek; időben pedig szinte behatárolhatatlanok.

A globális stratégiai javakat megcélzó nemzeti gazdasági, politikai és katonai stratégiák esetleges konfrontációja a XXI. században is potenciális biztonsági veszélytényező. Míg a fejlett világban a globális centrumok közötti verseny egyre dinamikusabban fokozódik, addig a bizonytalansággal és átmeneti viszonyokkal küszködő térségekben a biztonsági devianciák folyamatos halmozódása tapasztalható. A túlélésért folytatott harc a gazdasági fejlettség különböző

szintjein elhelyezkedő országok között, a jóléttől tulajdonképpen függetlenül zajlik. A fejlett országok éppúgy rivalizálnak egymással, mint a fejletlenek, vagy a fejletlenek a fejlettekkel, és fordítva. Leegyszerűsítve: éppúgy több kell annak, akinek kevés van, mint aki sokkal rendelkezik. A globális stratégiai javak többsége azonban ma még véges. Az informatika adta platformokat azonban minden állami és nem állami entitás használja, fejleszti, ezért a digitális terek nagyban összeolvadnak ez által képezve globális egységet, egyben sokrétűséget.

A globalizáció, a digitalizáció, az információ, és a médiák által befolyásolt társadalmi és kulturális értékek súlyos identitászavarokat okoznak makro- és mikroközösségi szinten egyaránt. A tradicionális nemzeti jellemvonások, öntudatok, szabályok és egyéb értékek új értelmezést kapnak, s e sokrétű folyamatban a nemzeti stratégiai célok is merőben átalakulóban vannak. Ennek egyik legfőbb oka, hogy a nyitottabb határok, a szabad információáramlás és az információ globálissá válása következtében a nemzetközi kapcsolatok ”nemzeti”, ”(nemzet) állami” és ”nemzetközi” vizsgálati kategóriái, szintjei merőben átértékelődnek.

A globalizáció hatására univerzálódó biztonsági kihívások nagyban összemossák a ”kül-” és ”belbiztonság-politikák” közötti különbséget. E folyamatban az államközpontú intézmények és szabályok feloldódnak és teret engednek a globális kapcsolati rendszerek és szereplők diktálta törvényeknek. A kockázati tényezők egyetemessé válása folytán egyfelől élénkülnek a közös biztonságpolitikai fellépést szorgalmazó viták, másfelől a nemzetállamok magasabb, a nemzetközi biztonsági intézményrendszerek szintjére emelik érdekeik érvényesítését, amely tendencia a nemzetközi intézményrendszer felelősségének növekedésével jár. E folyamatban az állam, mint a ”nemzetközi kapcsolatok egyik tényezője” szerepe és kompetenciája átformálódik. Ma az államok a poszt-internacionális dinamizmus időszakában működnek, amely a határokat sokkal átjárhatóbbá, az intézményeket kevésbé hatékonnyá és a politikai erőt zavarosabbá teszi. Az állami intézmények ugyan továbbra is fontosak maradnak, azok azonban kisebb hatékonysággal, kevesebb forrással és csökkenő legitimációval funkcionálnak. Tekintettel azonban arra, hogy a nemzetközi szervezetek presztízs- és legitimációvesztése rohamosabban megy végbe, mint az államoké, a nemzeti szereplők ereje relatíve gyarapszik.

A globalizáció és modernizáció útjában még mindig számos, elsősorban kulturális, vallási és nacionalista bástya áll. Kérdés, hogy az olyan erősen zárt, tradicionális jelszavak mentén szerveződő közösségek, mint például az iszlámtársadalmak, vagy korunk diktatúrái képesek lesznek-e konfliktusmentesen ellenállni e komplex, és többszintű folyamatnak, vagy konfrontálnak vele. Minthogy maga az iszlám sem homogén, valószínű, hogy a konfliktusok az extrémitások, vagyis egyfelől a túlzottan zárt, fundamentalista diktatúrák, valamint a nyitott, liberalizált társadalmak közötti törésvonalak mentén törnek fel. E két ellentétes irányú erő minden bizonnyal mindaddig konfrontálódik egymással, amíg a kontrasztok ki nem egyenlítik, vagy megfelelőképpen le nem rontják egymást. A digitális hálózatok e konfrontáció nyílt színterei. Miközben az internet óriási kulturális hatást gyakorol a zárt társadalmakra, addig a fundamentális rendszerek mind gyakrabban használják e rendszert támadásaik érdekében.

A legnagyobb veszély ma talán a radikalizmus és a technológia kontrasztjában rejlik. Az egyenlőtlen társadalmi, gazdasági alapok és az aránytalan erőforrások következtében fokozódó konfrontáció-kockázatot a kulturális, civilizációs, vallási, etnikai retorikák és politikai érdekek tovább élezik. E komplex társadalmi polarizáció aztán kölcsönhatásba kerül(het) a hidegháború örökségeként megmaradt katonai potenciállal, amely folyamatban a szinte összemérhetetlen technológiai kontrasztok és a tömegpusztító fegyverekhez való relatíve könnyű hozzáférés meghatározó szerepet játszanak. Ehhez ok-okozati összefüggésként kapcsolódik a további rohamtempójú és széles spektrumú tudományos-technológiai fejlődés, amelynek során a gazdagok még inkább gazdagabbá és fejlettebbé válnak, a szegények pedig relatíve még inkább a perifériára sodródnak. Az, hogy ezek a kontrasztok miképpen és mikor egyenlítik ki egymást, ma még beláthatatlan.

Az aszimmetrikus biztonsági kockázati tényezők, úgymint a tömegpusztító fegyverek alkalmazása, azok célba juttathatósága és/vagy a terrorizmus által okozható csapás napjainkban nagyobb valószínűségű fenyegetettséget jelent a fejlett országokra nézve. A hidegháború utáni évek zavaros biztonsági környezetében a tömegpusztító fegyverek és más pusztító technológiák ellenőrizetlenül hagyása és proliferációja következtében ma a világ stratégiai erőegyensúlya átstrukturálódik. A fejlett világgal opponáló országok, nemzetek és nem állami szereplők a nemzetközi érdekérvényesítés "szabályszerű" eszközei hiányában, vagy azok helyett aszimmetrikus kellékeket ragadnak, amelyek relatíve kis forrásigényűek, ugyanakkor hatásukat tekintve akár egyetemesek is lehetnek. Azok a fejlett hatalmak, ahol kifejlesztették e technológiákat, mára potenciális célponttá váltak. Miután növekszik annak lehetősége, hogy a harmadik világ bizonyos politikai erői az egymás közötti, vagy a fejlett világgal szembeni konfliktusai során a hadviselés "piszkos" eszközeihez nyúljanak, a nukleáris, vegyi és biológiai technológiákban, a génmanipulációban, a tömegpusztító fegyverek hordozóeszközeiben, a számítógépek tömeges felhasználásában rejlő szerteágazó veszélyforrások, a technológiák illetéktelenekhez kerülése jelenti napjaink talán a legkönnyebben bekövetkezhető fenyegetését.

A globalizáció egyfajta reakciós tényezője, vagy inkább selejtterméke a terrorizmus. A terrorizmus soha többé nem tekinthető belpolitikai problémának, tudniillik a terrorizmus direkt fenyegetést jelent a nemzetközi biztonságra. Az egyenlőtlenség, a szegénység, a diktatúrák expanziós becsvágya és az ehhez kapcsolódó kulturális gyökerek táptalajul szolgálnak a terrorizmus burjánzásának. A terrorizmus, mint az egyetemes fenyegetés, a támadások skálája, a globális veszteségek minőségi és mennyiségi mutatói, valamint a transz-nacionális, professzionális, mobil és minden gátlást és határt nélkülöző terrorszervezetek által nyilvánul meg, amelyek minden egyes nemzetállam biztonságára potenciális veszélyt jelentenek.

A kultúrák szempontjából a globalizáció, a digitalizáció és az informatikai fejlődés jövőjét illető kérdés úgy fogalmazódik meg, hogy az egyes nemzetek, országok, föderációk, államközösségek, régiók, szövetségek és szervezetek mindegyike képes lesz-e annak érdekében mozgósítani forrásait, hogy konfliktusmentesen kapcsolódjon be e folyamatba, vagy, hogy átalakuljon, esetleg megszűnjön? És ha nem, mely(ek) lesz(nek) az(ok) amely(ek) nem lesz(nek) képes(ek)? Mikor? És milyen áron?

Napjaink biztonságának egyik legfontosabb eleme a mára kialakult nemzetközi rendet szavatoló katonai erőegyensúly. A katonai erő, a technikai, technológiai fejlesztések és az azokban rejlő pusztító potenciál miatt kiemelt figyelmet kap a biztonság értelmezésében. A hidegháború utáni időszakban megtorpant katonai fejlesztések, sok helyütt leállt, vagy – akár – csökkenő katonai képességek tendenciája megfordult, s ma egyre több országban tapasztalható a katonai kiadások emelkedése, a haditechnikai kutatások és fejlesztések növekedése, az új technikai és technológiai megoldások elterjedése: kíberhadviselés; komplex hálózat-alapú fegyverrendszerek; intelligens fegyverek; lopakodó üzemmód; robottechnika.

A fentiek tükrében megállapítható, hogy a felkészülés melletti fontos alapelem a rugalmasság, ami az új kihívásokhoz való alkalmazkodás képességét rejti magában. A védelmi igazgatás rendszerét ezért nem statikus szervezetként kell tekinteni, hanem egy olyan rendszerként, amely folyamatosan képes megújulni, változni és reagálni a megváltozott kihívásokra. A biztonság korszerű értelmezésének követelményei közé tartozik a biztonság fogalmának újraértelmezése, megteremtése, fenntartása és korszerűsítése. Prioritást élvez a megelőző, valamint az integratív jelleg a nemzeti és nemzetközi fellépések során egyaránt.

A VÉDELMI IGAZGATÁS TÖRTÉNETE MAGYARORSZÁGON AZ 1990-ES ÉVEKTŐL NAPJAINKIG [3]

A védelmi igazgatás az 1990-es években

A védelmi igazgatás jelentős változásokon ment keresztül az elmúlt két évtizedben. Magyarország, mint poszt szocialista ország nehezen tudta kialakítani a rendszerváltást követően védelmi igazgatási rendszerét. A már említett nehézségek jegyei, hazánk védelmi igazgatási rendszerének „lemaradásában" mutatkoznak meg.

A tanulmány a tézis igazolása érdekében bemutatja a védelmi igazgatás történetét különös tekintettel a Védelmi Hivatal szaktevékenységeire, mely tevékenységek később strukturáltan kerültek átvételre a Honvédelmi Minisztérium (HM), Belügyminisztérium (BM) és a Nemzetgazdasági Minisztérium (NGM) feladatmegosztásában. A fejezet elemzi a védelmi igazgatás jogszabályi hátterét a 90-es évektől egészen napjainkig. A fejezet bizonyítja, hogy a védelmi gazdálkodás Magyarországon erősen hiányos, tekintettel a jelentős történeti, jogalkotási, kormányzati változásokra.

1995. július 1. napján megalakult a Védelmi Hivatal, amely HM háttérintézményként folytatta munkáját. Ezzel szervezetileg egységessé vált a védelmi felkészítés kormányzati koordinációja. A Védelmi Hivatal feladatai közé tartozott a minősített időszakokra vonatkozó védelmi igazgatási döntések előkészítése és végrehajtásának koordinálása. A védelmi igazgatás központi és területi szintű rendszerének kialakításával párhuzamosan folytatódott a védelmi felkészítés, melynek alapjául a különböző típusú védelmi felkészítési programok szolgáltak. Az 1990-es évek közepétől a Védelmi Hivatal meghatározónak tekintette a gazdaságmozgósítás piacgazdasági viszonyokra kialakított, a nemzetgazdaság védelmi felkészítése tervezéséről és a védelmi célú tartalékolási tevékenység szabályozásáról szóló 1041/1994. (V.I.) Korm. határozatból következő honvédelmi feladatok összehangolását. [4] -A tervezési tevékenység különösen a minősített időszaki tervek kidolgozására, a rögzített hadiipari kapacitások és állami céltartalékok megalakítási és biztosítási feltételeinek megteremtésére irányult. A gazdaságmozgósítási feladatokat egyaránt végezték az ágazatok területi és helyi szintű védelmi igazgatási szervei. Ekkor hazánk részese volt a Partnership for Peace (PfP) folyamatoknak, amely a későbbi (1999) NATO-hoz való csatlakozás lehetőségét készítette elő.

1998. november 1. napjától a védelmi felkészítési feladatokban változások következtek be. A védelmi igazgatás és felkészítés kormányzati koordinációjára megalakult a Miniszterelnöki Hivatal Biztonság és Védelempolitikai Koordinációs Államtitkársága. Ezen feladatok ellátására létrehozott Titkárság a HM Védelmi Hivatalának, a BM-nek és az akkori Pénzügyminisztériumnak vezetőiből és szakértőiből állt össze. A fő feladatok között szerepelt:

- védelmi stratégia és biztonságpolitikai alapelvek kialakítása;
- az ország védelmi felkészültségének biztosítása;
- a nemzetgazdaság védelmi felkészítése;
- a gazdaság mozgósítása;
- a Gazdaságbiztonsági Tartalékolási Tárcaközi Bizottság vezetése.

A védelmi feladatok közé tartozik a természeti vagy ember által előidézett katasztrófák elhárítása is. 1998. november 5. napján árvízveszély következett be a Felső-Tiszán. A védekezést a kormányzati koordináció a területi-helyi védelmi igazgatási szervek szereplőivel összehangolt munkával kezelték. A Miniszterelnöki Hivatalon belül megalakult új államtitkárságot mégis megszüntették. A feladatok a követezőképp oszlottak el az érintett tárcák között:

Honvédelmi miniszter:

- védelmi felkészítés;
- ország mozgósítás feladatai és koordinálásuk;

Belügyminiszter:
- polgári védelmi tervezés, felkészítés és koordináció;

Gazdasági miniszter:
- gazdaságmozgósítási feladatok.

A védelmi igazgatás a 2000-es években

A 2000-es éveken a Védelmi Hivatal tovább folytatta működését. 1999-2000-ben a Védelmi Hivatal feladatai kiszélesedtek hazánk NATO taggá válásának szabályozási és védelmi felkészítési tevékenységeivel. A honvédelem rendszerében a védelmi felkészítés a polgári és katonai képességek komplex felhasználására irányult.

A védelmi felkészítés 2001. évi folyamatába új feladatok, védelmi intézkedések kerültek a 2001. szeptember 11. napi Amerikai terrortámadások kapcsán. 2003-ban megtörtént a VÉDELEM-2003 rendszergyakorlat előkészítése. Ugyanebben az évben a védelmi felkészítés két fontos területén jogalkotási feladatok folytak. Egyrészt a befogadó nemzeti támogatás feladataival és a NATO szövetségi kötelezettséggel összefüggő feladatokkal foglalkoztak, másrészt a Védelmi Hivatal a területi védelmi igazgatási szervekkel közreműködve részt vállalt a nemzetgazdaság védelmi felkészítésére vonatkozó jogforrás megalkotásában.[5] Így váltotta fel a korábbi a nemzetgazdaság védelmi felkészítése tervezéséről és a védelmi célú tartalékolási tevékenység szabályozásáról szóló 1041/1994. (V.1.) Korm. határozatot a nemzetgazdaság védelmi felkészítése és mozgósítása feladati végrehajtásának szabályozásáról szóló 131/2003. (VIII.22.) Korm. rendelet. [4,6] Az új Korm. rendelet kitér a védelemben közreműködő szervek és a lakosság minősített időszaki ellátásainak igényeire, a rögzített kapacitás szükségletekre és a stratégiai tartalékolás kérdéseire.

A 2004. év védelmi felkészítési feladataihoz kötődik, hogy a Kormány elfogadta a terrorizmus elleni küzdelem aktuális feladatairól szóló 2112/2004. (V. 7.) Korm. határozatot, ezzel elfogadta Terrorizmus Elleni Nemzeti Akciótervet, és elrendelte az intézkedések végrehajtását. [7] Ebben az évben elkezdődött a védelmi feladatok költség igényeinek megalapozása és az országos szintű védelmi tervezési rendszer (Országos Veszélyhelyzeti Tájékoztató Rendszer) elméletének a kidolgozása.

A 2007. évben elkészült a nemzeti válságreagálás rendszerének leírása, amely összhangban állt a NATO válságreagálási rendszerével. A 2007. évi védelmi felkészítési feladatok kidolgozásában a gazdasági tárca mellett delegált szakértők is részt vettek. A nemzetgazdasági felkészítés, a honvédelmi igények és a hadiipari kapacitások kidolgozását a honvédelmi tárca végezte.

A védelmi felkészítési feladatok gyakorlati megvalósítására, valamint az állomány elméleti felkészítésére 2008-ban került sor. Ekkor számos településen oldottak meg védelmi feladatokat a polgármester és a helyi lakosság bevonásával, amely hasznosságának pozitív társadalmi visszhangja volt, csakúgy, mint a területi képviseleti szervek elméleti oktatásának, tananyag kidolgozásának.

A védelmi igazgatás napjainkban

A gazdaságmozgósítási feladatok 2010-től a NGM hatáskörébe kerültek. 2012-ben a közös stratégia tervezésére és szabályozására felállították a Nemzetgazdasági Tervezési Hivatalt, de az intézmény két év működés után megszűnt.

A nemzetközi trendek és a nemzeti biztonsági kutatások a terület egységes kezelését sürgetik (átfogó megközelítés – comprehensive approach). Magyarországon a védelemgazdaságot érintő szakpolitikai kérdésekben a Miniszterelnökség koordinálása mellett három tárca jelenléte az uralkodó: HM, BM, NGM. A haderő szerepe a különleges jogrendben nem változott, de a figyelem a polgári biztonsági kihívások, veszélyek irányába fordult, melyet 2010-et követően a

BM vezényel. A BM a rendészeti, katasztrófavédelmi; terrorizmus elleni; kiber védelmi kihívásokat kezeli.

A nem katonai veszélyek egységes kezelési rendszere a BM Országos Katasztrófavédelmi Főigazgatóság (OKF) 2000. évben történő felállításán túl, a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény elfogadásával vált szabályozottá. [8] Így a 2015-ben kialakult tömeges migráció helyzetét már a BM Katasztrófavédelmi Operatív Törzs irányította.

A gazdaságmozgósítás kérdésköre (GM) 2010-től a NGM (a továbbiakban: NGM) irányítása alá került. A Kormány 2011. november 30. napján fogadta el a gazdaságbiztonsági rendszer létrehozásáról szóló 1410/2011. (XII.1.) Korm. határozatot, amely az NGM részére előírta, hogy 2012. április 30. napjáig készítsen a témában előterjesztést. A feladat végrehajtása nem valósult meg. [9] A védelmi felkészítés egyes kérdéseiről szóló 1221/2016. (V.02.) Korm. határozat 1. melléklet 6/a pontja szerinti feladat teljesítése a Miniszterelnökség részéről megvalósult a nemzetgazdaságra háruló védelmi célú tartalékolással összefüggő feladatokról szóló koncepcióról szóló előterjesztés elkészítésével. [10]

A tézist bizonyítja, hogy a védelmi igazgatás történetében bekövetkezett változások következtében Magyarországnak jelentős változásokhoz volt szükséges igazodnia az, amely az 1990-es évektől egészen máig tart. A védelmi igazgatás egységes arculatának kialakítása napjainkban is zajlik, melyre megoldást nyújthat az egységes kormányzati döntéshozatal.

A VÉDELEMGAZDASÁG JELLEMZŐI A II. VILÁGHÁBORÚTÓL A HIDEGHÁBORÚN ÁT A RENDSZERVÁLTOZÁSON KERESZTÜL NAPJAINKIG

A háborús gazdasági stratégiák fő modelljeinek bemutatása a II. világháborúban

E fejezet két háborús gazdasági stratégiát mutat be: az egyik modell célrendszere a háborúhoz szükséges termelés maximalizálása, a másik modell a gazdasági prioritások átsorolásával próbálja kielégíteni a háborús keresletet.

Magyarországon a hidegháború alatt a Kölcsönös Gazdasági Segítség Tanácsa (KGST) és a Varsói Szerződés (VSZ) központi tervutasításos rendszert képezte. A NATO országokban is hasonló rendszer működött, de az ellátási rendszer nem volt központosított, minden tagország magának biztosította a fegyveres erők ellátását. A Varsói Szerződésben mindent centralizáltak, ez azt jelentette, hogy a fegyvereket és a hadfelszerelést homogenizálták, és a logisztikát, valamint a tagországok védelemgazdasági rendszereit azonos módon építették fel. Ez a modell legfőképp a II. világháborúban kialakult szovjet hadigazdálkodásra vezethető vissza. [11] A II. világháborúban azonban volt olyan gazdaságmozgósítási rendszer is, amely eltért a központosított modelltől.

Alan Milward nyomán Szenes Zoltán kétféle háborús gazdasági stratégiát különít el. [12] Az első modell a gazdaságot totálisan alárendeli a háborúnak, ahol az egyetlen cél a háborúhoz szükséges termelés maximalizálása volt. [13]

W1= p+r+s+e-f

w1= háborús termelési potenciál
p= a nemzeti termék egy évben
r= a gazdaságban rendelkezésre álló tartalék
s= a békeidőszaki tőkepótlásból elvett megtakarítás
e= a gazdaságba bevonható külső források mennyisége
f= közigazgatási fennakadás miatt csökkent hatékonyság

A másik modell a gazdasági prioritásokat átsorolja, így próbálta kielégíteni a háborús keresletet.

W2= w1-c-i-d

w1= háborús termelési potenciál
c= háború ellenére fenntartott polgári fogyasztás
i= új, civil beruházások összege
d= politikai és társadalmi rendszer fennakadásai.

A *W1 modell* az ország túlélését szolgáló modell, ennek érdekében minden erőforrást a háborús gazdasági termelésnek vetett alá. A modell akkor sikeressége a teljes megsemmisülés és a túlélés közti választásban rejlett. A II. világháborúban ezt használta a Szovjetunió, Németország, Észak-Korea és Vietnám. Ebben a modellben a meghatározó tényező a túlélés érdekében tehát a termelés maximalizálása volt.

A *W2 modellt* akkor alkalmazták, amikor a háború feltehetően nem járt teljes megsemmisüléssel. Többek között arra való tekintettel, hogy a hadi termelés maximalizálása képes teljesen nyomorba dönteni egy országot.

Fentiek bizonyítják a tézist, mert a II. világháború alatt a Varsói Szerződésben a szovjet modellt alkalmazták, ennek következtében Magyarországnak, mint tagországnak kötelező volt a centralizációt követni. Negatív hatásai abban mérhetők, hogy a rendszerváltozás után nehezen tudott átállni az ország a saját gazdasági stratégia kialakítására.

A védelemgazdaság a hidegháborúban

E fejezet két történelmi aspektusból elemzi a védelmi tartalékolás rendszerét a hidegháború időszakában és a rendszerváltást követően. Összehasonlítja a hidegháborúban alkalmazott szovjet hadviselés modelljét, valamint bemutatja a háborús szükségletekre alkalmazott stratégiát különös tekintettel a stratégiai tartalékok, állami egészségügyi tartalékok és a nemzetgazdasági mozgósítás tartalékainak tárolására. A fejezet utolsó aspektusaként bemutatásra kerülnek az EU és NATO csatlakozásból adódó transzformációk Magyarország vonatkozásban.

Az előzőek alapján megállapítható, hogy a hidegháború időszaka alatt Magyarország a szovjet hadviselésre volt kényszerítve. Ennek következtében a szovjetek a háborút négy szakaszra osztották fel:

1. hagyományos eszközökkel folytatott harc;
2. atomfegyverek korlátozott alkalmazása;
3. atomfegyveresek korlátozott alkalmazása, és
4. befejező haditevékenység időszaka.

A fenti felosztást a NATO is alkalmazta. (vö.: tömeges megtorlás, rugalmas reagálás). A gazdaság háborús felkészítésének koncepciója a következőképp alakult:

- feszültségi időszak: 3-6 hónap;
- háborús veszélyeztetettségi időszak: 1-2 hét;
- közvetlen háborús veszély: maximum 3 hónap. [14]

A fent ütemezett időszak állt rendelkezésre ahhoz, hogy a gazdaságmozgósítás feladatait végrehajtsák, illetve a háborús termelést felgyorsítsák. Az ország védelmi feladatait az állampárt vezetése irányította. Ez azt jelentette, hogy közvetlen felügyeletet gyakorolt a fegyveres, rendvédelmi szervek, valamint a védelmi igazgatási szervek felett. A Számítási év Terve (SZÉ) tartalmazta a fegyveres erők igényeit, szabályozta a hadiipari termelésben érintett gazdasági szervezetek, és közreműködő partnerek termelési, szolgáltatási és ellátási feladatait, melyet az

Országos Tervhivatal (OT) állított össze hasonlóan a gazdaságmozgósítási tervhez. Ami nem volt biztosított az ország területén belül, azt speciális importból biztosították. A koordinációt a VSZ és KGST végezte. 1986-ban készült el az utolsó SZÉ terv.

A háborús szükségletekre az alábbi képletet alkalmazták: [13]

D= s+c+I

D= anyagi szükségletek a háború első időszakában
s= a fronthadművelet végére előírt készletek
c=a haderő fogyasztása hadműveletben
i=a haditevékenységek során keletkezett anyagi és technikai veszteség.

A fegyveres erők a hadműveletek anyagi és technikai szükségleteit hazai készletből, tartalékokból vagy speciális importból fedezték. A későbbiekben a tervezésnél a kereslet és kínálat egyensúlyra való törekvésénél számoltak csak kizárólag szovjet importtal is. Ez ma a NATO tekintetében is így van, amerikai vonatkozásban. A keresleti és a kínálati oldal azonban nem volt egyensúlyban. Magyarország ebben az időszakban a GDP 4-5%-át költötte katonai kiadásokra. A készletképzés viszont kiegyensúlyozatlan volt. A fegyverzeti tartalékok technikailag elavultak voltak. Magyarország nemzetgazdasági mozgósítási tartalékainak (M) képzése az 50-es években indult meg:

- stratégiai tartalék (ST) - üzem-és kenőanyag, gumiabroncs;
- állami egészségügyi tartalék (ÁEÜT) - katonai szükségkórházi felszerelések, gyógyszerek, kötszerek, vérpótló szerek.

A nemzetgazdasági tartalékokat ebben az időszakban a Tartalékgazdálkodási Igazgatóság (TIG) végezte. A TIG különböző tartalékokat (élelmiszer, ipari alapanyagok) az ország különböző pontjain tartalékolta.

Az 1980-as években az állami stratégiai tartalékok képezték a gazdaság rendkívüli időszaki működéséhez szükséges 6-10 hónapnyi ellátást. Az állami egészségügyi rendszer készenlétben állt a fegyveres erők, a szövetségesek és a lakosság egészségügyi ellátására. Egy évre elegendő hadiipari tartalékkal rendelkeztünk. A TIG által központilag tartalékolt javak a lakosság ellátását és a gazdaság működését is fedezték. A rendszerváltást követően a tartalékok elfogytak, és a TIG-et felszámolták.[15]

A fegyveres erők szükségletei külső forrásra voltak alapozva, amely igen jelentős politikai kockázatot jelentett. Alapvető harci és technikai eszközök Szovjet importból érkeztek, de fegyvergyártásban Csehország, Lengyelország és Bulgária is kooperációs partner volt. Összességében elmondható, hogy a hadfelszerelési anyagok 70%-a szocialista országokból került importálásra.

A rendszerváltozás utáni védelemgazdasági szakpolitika állomásai

A rendszerváltozást követően bemutatásra kerül a védelemgazdálkodási politika hármas felosztásban: (1) a rendszerváltás utáni évek, (2) az euro-atlanti szervezeti tagság (3) a 2010 utáni törvényalkotás.

1992-ben a védelmi felkészítés a rendkívüli állapoton kívül már tárgyalta a szükségállapot és a veszélyhelyzet tényállását. Az 1999-es NATO csatlakozás lényeges változásokat hozott hazánk védelempolitikájában, a honvédelem rendszerében. A rendszerbe beemelték a NATO szövetségesi kötelezettségeket, a NATO infrastrukturális beruházásokat, az EU-s csatlakozáshoz szükséges biztonság-és védelempolitikai alapelveket is. 2003-ban a védelmi felkészítésben már elmozdulások fedezhetőek fel a háborús mozgósítás régi felfogásától. Ekkor a gazdaság felkészítése a békeidőszaki tervezésre irányul, amely az alábbiakat foglalja magába:

- beruházás;

- készletezés;
- kapacitás-fenntartás;
- adatgyűjtés;
- adatszolgáltatás.

Megjelenik a tartalékképzés rendszere, mely következőképpen épül fel:
- gazdaságbiztonsági tartalék (GT);
- állami egészségügyi tartalék (ÁEüT);
- állami céltartalék (ÁC);
- pénztartalék (PT).

A 131/2003-as Korm. rendelet bevezeti a védelemgazdasági alapterv elnevezést.[6] A tervezés időtartama az 1994-es állapotot tükrözte miszerint a veszélyhelyzet és szükségállapot időszaka 1-1 hónapot fed le, a különleges állapot hat hónapos veszélyeztetettségi, míg a háborús időszakra egy hónapot, a helyreállítási időszakra pedig hat hónapot számoltak. A Korm. rendelet tartalmazta a gazdaságmozgósítás fogalmát, de nem a termelés háborús célú tartalékolására koncentrált, hanem a GM tervének elkészítésére. A dokumentum csak a katonai válságkezelésben, béketámogató műveletekben és nemzetközi segélynyújtásban való közreműködésével számol.

A védelemgazdaság harmadik periódusa a legújabb időszakot öleli fel. Magyarország Alaptörvénye újraszabályozta az ország védelmi feladatait, miszerint két sarkalatos törvény a honvédelmi törvény és a katasztrófavédelmi törvény fogalmazta meg a külső és a belső biztonság fogalmát. A védelemgazdaság duális felfogása szerint a gazdaság védelmi felkészítésével kapcsolatos feladatok a HM-hez, még a katasztrófavédelemi és rendvédelmi feladatok a BM-hez tartoznak. A védelemgazdaság külön kezeli tehát a katonai és nem katonai természetű veszélyek és fenyegetések elleni küzdelem kérdéseit. Az NGM elkészítette a védelmi felkészítés 2012-2030-ra vonatkozó koncepcióját, amely a gazdaságbiztonságot, mint komplex rendszert vizsgálta. Az új elképzelés szerint a hadtudományból ismert képességalapú metodikát veszik alapul a gazdasági biztonság tervezésére. Ennek előfutáraként az ágazati stratégia gazdasági-pénzügyi kidolgozását határozták meg. A Kormány 2011-ben elfogadta a koncepciót, annak megvalósítása viszont elmaradt. [16]

Az új kihívások transzformációja

A tanulmány értékeli az új biztonsági kihívások transzformációját tekintettel az energiabiztonság, pénzügyi biztonság, migráció, kiber biztonság, környezeti biztonság globális jelenlétére. A rendszerváltást követően az országunk célként tűzte ki az euro-atlanti integrációt kül- és biztonságpolitikai szempontból. Magyarország az 1999 utáni biztonságpolitikai megmozdulások NATO, majd 2004-től az EU csatlakozásokhoz igazodtak. [17] Az átalakulások 3 szakaszra oszthatók:

A hidegháború után megkezdődött a fegyveres erők csökkentése, átalakítása, az új fenyegetettségekre való készülődés, az újfajta háborúra való felkészülés. A külső és a belső biztonság kérdései elválaszthatatlanokká váltak, megjelentek a hibrid háborúk, amely az átfogó megközelítés (vö.: comprehensive approach) alkalmazását hozták magukkal.

Az időszak jellemzői:
- katonai szükségletek racionális csökkenése;
- védelmi költségvetés visszaesése;
- haditechnika megújításának igénye;
- fegyveres erők alkalmazása nemzeti és szövetségi rendszerben is.

A biztonságpolitika átalakulása. A biztonság fogalmának kiszélesítése, így megjelent a katonai és nem katonai biztonsági veszélyek és kockázatok feldolgozása, a rendvédelmi feladatok kiszélesítése, a terrorizmus elleni harc, és nem utolsósorban a katasztrófavédelem. Az adott időszakban az energiabiztonság, pénzügyi biztonság; migráció; kiber biztonság; környezeti biztonság területei jelentkező új biztonsági kihívások jelennek meg. Mindezen tényezők egy integráltabb és jobban koordinált védelmi igazgatási rendszer kialakítását eredményezték. [1]

Magyarország egyre kevésbé számol a konkrét háború kitörésével, amely a megváltozott biztonságpolitika hozadéka. Ennek eredményeképp a gazdaságmozgósítás transzformálódik a gazdaság békeidőszaki, védelmi célú felkészítésére ez által a gazdaságbiztonság kérdésköréhez kerül.

A fejezet igazolja a tézist, mert a bemutatott időszakok védelemgazdasági jellemzőiből kitűnik, hogy Magyarországnak a rendszerváltozást követően számos új követelménnyel kellett szembe néznie, melyet a nemzetközi szervezetekhez való csatlakozásból adódó biztonságpolitikai szemlélethez való alkalmazkodás is alátámaszt. Ennek következtében megállapítható, hogy (1) szükséges az egységes kormányzati koncepció kialakítása és alkalmazása védelmi igazgatás szempontjából (2) célszerű megalkotni egy, az új biztonsági kihívásokra is választ adó, az EU és NATO tagság követelményeire is támaszkodó összkormányzati koncepciót.

A VÉDELEMGAZDASÁG AKTUÁLIS HELYZETE MAGYARORSZÁGON

Az esszé utolsó fejezete elemzi, a fentiekben bekövetkezett változások hatásait ez által bemutatja a gazdaság védelmi felkészítésének aktuális helyzetét Magyarországon. Megállapítható, hogy hazánkban a már előzőekben bemutatott régi és a még kialakulóban lévő új rendszer ötvözete egyszerre van jelen.

A nemzetközi tendenciákhoz hasonlóan Magyarország biztonsági helyzete, ennek következtében biztonságpolitikája is változásokon megy keresztül. Új kihívásként jelent meg az ukrán válság, vagy a 2015. évi migrációs hullám, amely rámutatott a menekültügyi rendszer hiányosságaira, a bevándorlási, határvédelmi és a polgárvédelmi kapacitások elégtelenségére. A védelemgazdaságban egyre erőteljesebben jelenik meg a civil válsághelyzet kezelés. (vö.: átfogó megközelítés) A védelemgazdaság része a biztonságnak.

A védelemgazdaság szerepe a 2008-as gazdasági és pénzügyi válság óta felerősödött. A globalizáció hatására, a regionális szerveződések, valamint a tudomány és technika következtében kialakult újszerű biztonsági kockázatok okán megváltozott a hadviselés jellege. A klasszikus háborús modellt felváltotta a hibrid hadviselés, amely következtében nőttek a kiadások. 2008-tól kezdve a költségvetési erőforrások a biztonság- és védelempolitika alakító tényezői lettek. (vö.: EU: pooling & sharing; NATO: smart defence) [18]

Alapvető összefüggésként állapítható meg, hogy biztonság nélkül nincs erős gazdaság, stabil gazdaság nélkül pedig nincs erős védelem. A fent említett változások azonban nem azt jelentik, hogy az országnak nincs szüksége korszerű fegyveres és rendvédelmi szervek munkájára, hiszen a haza védelem továbbra is szükséges békében, katasztrófahelyzetben, katonai konfliktusban egyaránt. Továbbra is képviselni kell magunkat a nemzetközi érdekek és kötelezettségek érvényesítésére a nemzetközi válságkezelésben és a külföldi béketámogató műveletekben. Hazánk védelmének rendszerébe tartozik az egyenruhás szervezeteken túl az erős védelmi igazgatás, a gazdaság védelmi felkészítése, a lakosság és az anyagi javak megóvása.

A védelemgazdaság a közgazdaság egy alkalmazott diszciplínája, amely a nemzetgazdaság honvédelmi célú felhasználást tanulmányozza.[13] A globalizáció, és az új biztonsági kihívások terjedése miatt a tudományág kibővítetten is értelmezhető, miszerint a diszciplínának nemcsak a haderők gazdasági kérdésit érdemes kutatnia, hanem be kell vonni a vizsgálatba a szélesebb körbe eső biztonsági tényezők gazdasági vizsgálatait is. Az új típusú biztonságpolitikai értelmezés szerint a terrortámadások, globalizáció, természeti katasztrófák, ipari balesetek gazdasági kérdéseinek megoldása ugyanúgy a nemzetgazdaság erőforrásainak mobilitásában rejlik,

mint korábban a klasszikus háborúk kapcsán. Magyarországon a régi hadigazdasági rendszer megszűnt a 90-es években, valamint átalakult a Varsói Szerződés feloszlásával. A változó biztonsági környezet miatt országunk főleg a soft biztonsági kihívások, kockázatok és fenyegetettségek kezelésével foglalkozik.

KÖVETKEZTETÉSEK

A védelmi célú tartalékolás az államot és a társadalmat fenyegető, előre nem látható veszélyhelyzetek kezelésében, az adott szituációk felszámolásában kulcsszerepet játszó, úgynevezett elsődleges beavatkozó (honvédelmi és rendvédelmi) szervek, illetve speciális feladatkörre létrejött civil szervezetek működését, a lakosság ellátását, valamint a gazdaság válsághelyzeti működőképességének fenntartását biztosítja.

A védelmi igazgatás rendszerében nagyobb hangsúlyt kap a megelőzés és a felkészítés, mint a következményekkel való felszámolás. Ez magába foglalja azt a tényt, hogy kellő hangsúlyt szükséges fektetni a felkészülés feladatainak békeidőszakban történő végrehajtására.

A fentiek tükrében a tanulmány a tézis igazolása érdekében először bemutatta a biztonságot meghatározó tényezőket. A második fejezet elemezte a védelmi igazgatás történetét különös tekintettel az 1990-es; 2000-es évek valamint napjaink vonatkozásában. A dolgozat harmadik fejezete történelmi aspektusból elemzi a védelmi tartalékolás rendszerét a II. világháborúban, a hidegháború időszakában és a rendszerváltozást követően, ahol bemutatásra kerül a védelemgazdálkodási politika hármas felosztásban. Az esszé utolsó fejezete elemzi, a fentiekben bekövetkezett változások hatásait ez által bemutatja a gazdaság védelmi felkészítésének aktuális helyzetét Magyarországon.

FELHASZNÁLT IRODALOM

[1] BABOS Tibor: *Az európai biztonság öt központi pillére;* http://193.224.76.2/downloads/konyvtar/digitgy/phd/2004/babos_tibor.pdf (letöltve: 2017.08.22.)

[2] BABOS Tibor - KOVÁCS Zoltán: *A nemzetgazdaságra háruló védelmi célú tartalékolással összefüggő feladatokról szóló koncepcióról szóló előterjesztés*, Budapest 2016.

[3] HORVÁTH László: *Változások a védelmi igazgatás területén;* http://portal.zmne.hu/download/konyvtar/digitgy/nek/2005_2/07_horvath.pdf (letöltve:2017.05.11.)

[4] 1041/1994. (V.I.) Korm. határozat a nemzetgazdaság védelmi felkészítése tervezéséről és a védelmi célú tartalékolási tevékenység szabályozásáról

[5] 176/2003. (X.28.) Korm. rendelet a befogadó nemzeti támogatás feladatairól

[6] 131/2003. (VIII.22.) Korm. rendelet. a nemzetgazdaság védelmi felkészítése és mozgósítása feladati végrehajtásának szabályozásáról

[7] 2112/2004. (V. 7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól

[8] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

[9] 1410/2011. (XII.1.) Korm. határozat a gazdaságbiztonsági rendszer létrehozásáról

[10] 1221/2016. (V.02.) Korm. határozat a védelmi felkészítés egyes kérdéseiről

[11] HORVÁTH Miklós - KOVÁCS Vilmos: *Magyarország az atomháború árnyékában;* Zrínyi 2016.

[12] MILWARD A.S. *Háború, gazdaság, társadalom 1939- 1945. A II. világháború hátterében meghúzódó gazdasági események;* Aquila 1999.

[13] SZENES Zoltán: *A védelemgazdaság helyzete Magyarországon*; http://epa.oszk.hu/02700/02735/00080/pdf/epa02735_katonai_logisztika_2015_2_005-052.pdf (letöltve: 2017.01.20.)

[14] KISS Dávid: *A Kádár- korszak háborús védelmi igazgatási rendszerének kiépítése (1964-1975);*http://www.honvedelem.hu/container/files/attachments/61193/a_kadar-korszak_haborus_vedelmi_igazgatasi_rendszerenek_kiepitese.pdf (letöltve: 2017. 10.14.)

[15] TÓTH József: *A védelmi célú tartalékolás rendszere, és strukturális változásai napjainkban;* http://tudomany.szolnok__mtesz.hu/kulonszamok/2007/cikkek_pdf/Toth_Jozsef.pdf (letöltve: 2017.10.14.)

[16] MEDVECZKY Mihály: *A nemzetgazdaság biztonságos működésének és védelmi felkészítésének 2012-2030 közötti időszakra vonatkozó átfogó koncepciója;* Hadtudomány 21.4. (2011) 59-68. o.

[17] Külügyminisztérium: *Magyarország a NATO-ban;* http://2010-2014.kormany.hu/download/0/7b/20000/magyarorszag_a_NATO-ban.pdf (letöltve: 2017.10.14.)

[18] BABOS Tibor: *Hibrid hadviselés a NATO-ban*; https://adtplus.arcanum.hu/hu/view/HonvedsegiSzemle_2010/?pg=312&layout=s (letöltve: 2017.10.14.)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

MESTERSÉGES INTELLIGENCIA A KÖZÖSSÉGI MÉDIÁBAN

ARTIFICIAL INTELLIGENCE IN THE SOCIAL MEDIA

AMBRUS Éva

(ORCID: 0000-0002-8354-1296)

ambrus.eva.eszter@gmail.com

Absztrakt

Cikkemben összefoglalom a mesterséges intelligencia felhasználásának lehetőségeit a mélytanulási technika neurális hálózatának tovább fejlesztésének bemutatásával különböző területeken, úgymint a karrierportálon, vevőszolgálaton, marketing és személyügyi területeken.
A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett Ludovika Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: *mesterséges intelligencia, közösségi média*

Abstract

My article summarizes the possibilities of the use of artificial intelligence in social media by the deep neural networks in various fields, such as a career portal, customer service, marketing and human resources areas.
The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in the Ludovika Workshop.

Keywords: *artificial intelligence, social media*

A kézirat benyújtásának dátuma (Date of the submission): 2018.04.06.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.05.02.

BEVEZETÉS

Cikkem célja bemutatni a mesterséges intelligencia szerepét és fejlődését a közösségi médiába. A közösségi média többségünk életét át szövi, akár szórakoztatás, akár kapcsolattartás, akár ügyintézés szintjén, azonban a web 2.01 megjelenése óta a mesterséges intelligencia fejlődésével változott, hogy „mit látunk" a hírfolyamunkban, vagy hogy egy élő ügyfélszolgálatos kollégával kommunikálunk-e vagy sem.

A mesterséges intelligencia (MI) definíciója sokrétű, aszerint, hogy mire alkalmazzák. Cikkemben Stuart Russel megfogalmazását fogom alapul venni, miszerint MI-nek nevezzük egy program vagy gép által megnyilvánuló intelligenciát. Alapvető elvárás, hogy a gép emberi beavatkozás nélkül legyen képes reagálni a környezetére, lehetőleg a célnak megfelelően viselkedjen, és képes legyen a(z) (ön)tanulásra. [7]

A közösségi médiában törekedni lehet az egészséges egyensúly megteremtésére az emberi intelligencia és a mesterséges intelligencia között, hiszen azok kiegészítik egymást a területen. A közösségi média 'élményéért' cserébe a felhasználó hozzájárul, hogy a vállalkozások és szolgáltatások jobban megismerjék gondolatmenetét, ízlését, érdeklődési körüket. Hogy ennek milyen hozadékai vannak, arról az alábbiakban bemutatok néhány példát a mesterséges intelligencia felhasználásáról a közösségi médiában, illetve azon keresztül.

FELHASZNÁLÁSI TERÜLETEK

A mesterséges intelligencia tanulásához, tanításához nagy mennyiségű adat kell, hogy rendelkezésre álljon, hiszen azon keresztül képes tanulni. A vállalatok által gyűjtött és tárolt adatok mennyisége felbecsülhetetlen. A mesterséges intelligenciával párosítva hatékonyabban tudnak lenni az adatok kezelésében, elemzésében és felhasználásában. A következőkben bemutatok néhány felhasználási területet.

LINKEDIN & BRIGHT

2014-ben a LinkedIn megvásárolta a Bright.com nevű álláskereső start-upot. A Bright gépi tanulási algoritmusokat használ, hogy jobb állásajánló-álláskereső párosítást biztosítson a vállalatoknak és a felhasználóknak, pontszámokat adva. A LinkedIn ezt a pontszámot használja az álláskeresőknél, mely figyelembe veszi a jelentkező múltbeli felvételi mintáit, a felhasználó földrajzi helyét, korábbi munkatapasztalatát, valamint a munkaköri leírásokat. [8]

PINTEREST és a KOSEI

A Pinterest a személyre szabott ajánlások modellezésére specializálódott Kosei nevű adatszoftver-céget vásárolta fel, amelynek segítségével a Pinterest képes azonosítani az objektumfelismerést, hogy növelje a felhasználást (ún. "pin"-eket), és termékjavaslatokat tegyen, ezáltal csak az adott felhasználónak releváns tartalmak jelennek meg. [9]

A CHATBOT-ok

Az automatizálás egy fontos módja a kapcsolattartásnak egy vállalat vagy szolgáltató számára, növelve az idő-felhasználás hatékonyságát, kiegészítve az emberi tevékenységet az ügyfélszolgálat területén. A chatbot segít gyorsabb és hatékonyabb ügyfélszolgálatot elérni,

[1] Web 2.0-nak kifejezést elsősorban a közösségre épülő internetes szolgáltatásokra értendő.

valamint biztosítani a megfelelő típusú támogatást az ügyfeleknek a megtanult minták és a viselkedések alapján.

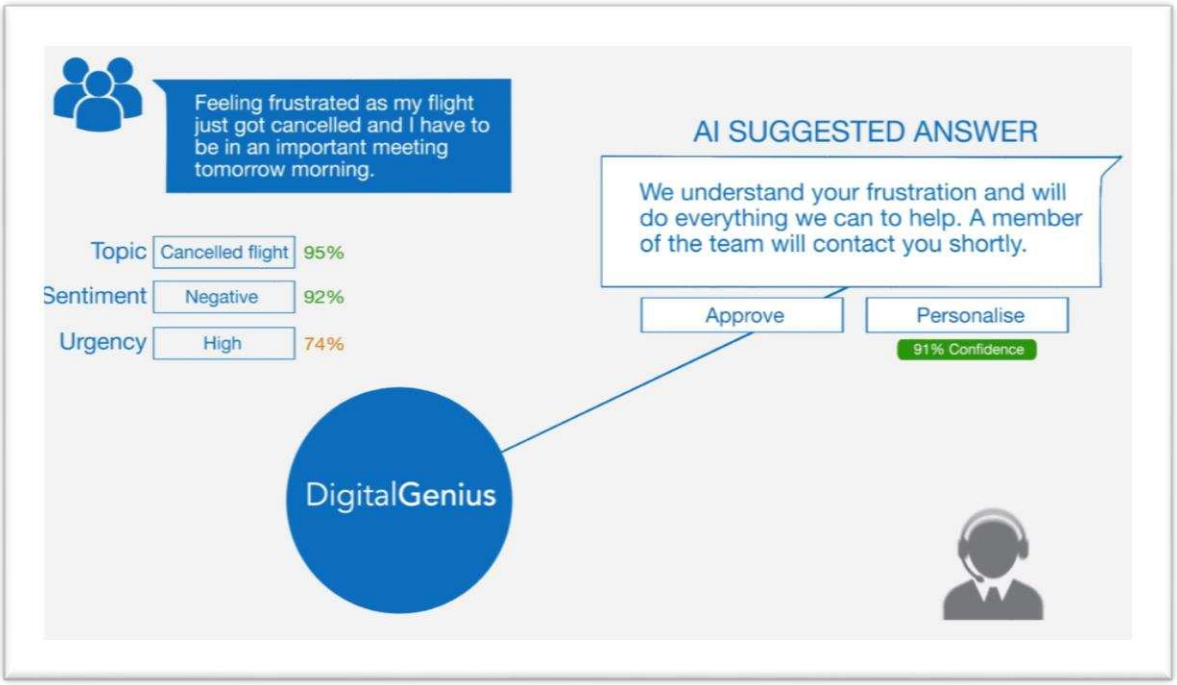
A légitársaságok között elsőként a KLM vezette be, hogy mesterséges intelligenciával válaszolja meg az ügyfelek kérdéseit. A légitársaság a DigitalGenius céggel közösen alkotta meg az automatizált ügyfélszolgálatát, ahol képesek általános, visszatérő ügyfélszolgálati kérdésekre válaszolni emberi beavatkozás nélkül. Ennek köszönhetően az ügyfélszolgálati munkatársaknak több idejük jut a bonyolultabb ügyek kivizsgálására, és az ügyfelekkel való személyesebb kapcsolattartásra. [10]

A DigitalGenius, építette az első ügyfélszolgálati chatbotokat az NVIDIA technológiával olyan vállalatok számára, mint a BMW, a Panasonic és az Unilever. [11]

Az alkalmazás mélytanulási[2] algoritmusokat használ, a tanulási fázisban nagy mennyiségű történelmi ügyfélszolgálati adatot felhasználva.

Amikor új üzenet érkezik egy digitális csatornán, például e-mailen, csevegésben, közösségi médiában vagy szövegben, a DigitalGenius mély tanulási modellje a következő lépéseket teszi:

1. A bejövő üzenethez kapcsolódó metaadatokat (adat az adatról) automatikusan kitölti,
2. A beérkező üzenetre előkészíti a legjobb választ, és elküldi a felügyelő személynek jóváhagyásra vagy személyre szabásra mielőtt kiküldené azt az ügyfélnek.



1. ábra A KLM által használt alkalmazás
https://blogs.nvidia.com/blog/2017/01/27/faster-customer-service-with-ai/

[2] *Mély tanulás (deep learning): gépi tanuló algoritmusok strukturált összesége, melynek rétegei a bemeneti adatok magasabb szintű absztrakcióinak kinyerésével hatékonyan képesek tetszőleges folyamatot modellezni.[12]*

FACEBOOK arcfelismerés

A Facebook nagy hangsúlyt fektet a mesterséges intelligenciára, és olyan arcfelismerő eszközt fejlesztett ki, amely megkönnyíti egy személy Facebookon belüli képének megcímkézését (azaz megjelölését tartalmakon). E mellett a Facebook arra is törekszik, hogy növelje a vállalkozások elérhetőségét (a bejelentkezési adatok alapján), felkínálva a felhasználónak egy valós idejű kedvezményt vagy ajánlatot. Az arcfelismerés technológiája elemzi a már megcímkézett fotók pixeleit, és létrehoz egy sorszámot, egy sablonnak a személyről. Amikor valaki fotókat és videókat tölt fel a facebook rendszerébe, ezeket a képeket a sablonhoz hasonlítják hozzá. [13]

Marketing

A közösségi média marketingjét érintően a következő területeken lehetséges előrelépés a mesterséges intelligencia segítségével:

1. Tartalom létrehozása: a tartalom létrehozása nagy mértékében felgyorsult, 20 évvel ezelőtt az átlagos márka hat hónaponként készített kampányt, manapság egy marketing vállalat akár havonta hat kampányt is végrehajt. Ennek végrehajtására – a marketing tartalmak létrehozásában - nagy segítség lehet a mesterséges intelligencia.
2. Fogyasztói információk: gépi tanulás által betekintés nyerhető a fogyasztókról a közösségi oldalakon megosztott és ügyfélszolgálati adatokból.
3. Vevőszolgálat: több kísérlet folyik a chatbotok integrálásában, növelve hatékonyságát az ügyfélszolgálaton dolgozó embereknek, néhány egyszerűbb esetben akár kiváltva is őket.
4. Influencer marketing:3 ahogyan a márkák a közösségi médiában elkezdtek „influencerekkel” – azaz egy-egy célcsoport véleményvezérével - együtt dolgozni, elengedhetetlenné vált, hogy a márkák jobban felderítsék, hogyan kapcsolódnak hozzájuk a fogyasztók.
5. Tartalom optimalizálás: több online hírfelület alkalmazza a mesterséges intelligenciát a hírek optimalizálására, az alapján, hogy egy-egy hír milyen szinten és minőségben köti le az olvasók figyelmét, ezzel segítve a szerkesztők munkáját. [14] Ilyen a New York Times által használt Blossom is.

Humánerőforrás (HR)

A HR menedzserek mesterséges intelligenciát használhatnak fel a közösségi médiaprofilokkal kapcsolatosan a munkaerő felvételnél az általános háttérellenőrzés kiegészítése céljából. A Frrole DeepSense [16] szolgáltatása lehetővé teszi a szakembereknek, hogy egy teljesebb személyiségprofilt lássanak, olyan személyiség jegyekkel, mint például az introvertáltság vagy extrovertáltság, rendszerezettség vagy preferált médiafogyasztási szokások.

VÉLEMÉNY- ÉS ÉRZELEM BÁNYÁSZAT

Az érzelemelemzés megjelenése egybeesik a közösségi média robbanásszerű népszerűségével. Az érzelemelemzés (más néven érzelmek szerinti osztályozás, véleménybányászat, szubjektivitás-elemzés, polaritásosztályozás, hatáselemzés stb.) egy

[3] Véleményvezér- vagy befolyásoló marketing a marketing egy formája, amelyben a fókuszt a befolyásos emberekre helyezik, a megcélzott piac egésze helyett.

multidiszciplináris tanulmányi terület, amely az emberek különböző érzelmekkel, attitűdökkel és véleményekkel foglalkozik, például a termékekről, szolgáltatásokról, egyénekről, vállalatokról, szervezetekről, eseményekről. Több területet foglal magában, mint például a természetes nyelv feldolgozás (NLP), számítástechnikai nyelvészet, információkeresés, gépi tanulás és mesterséges intelligencia. [18] A kutatási terület interdiszciplináris volta miatt kapcsolódik a gépi tanulási technikákhoz, a természetes nyelv feldolgozásához, és ezekhez az internet hozzáférést biztosít a gépi tanulási technikák számára nagymennyiségű adathalmazokhoz, továbbá folyamatosan jelennek meg alkalmazások és applikációk.

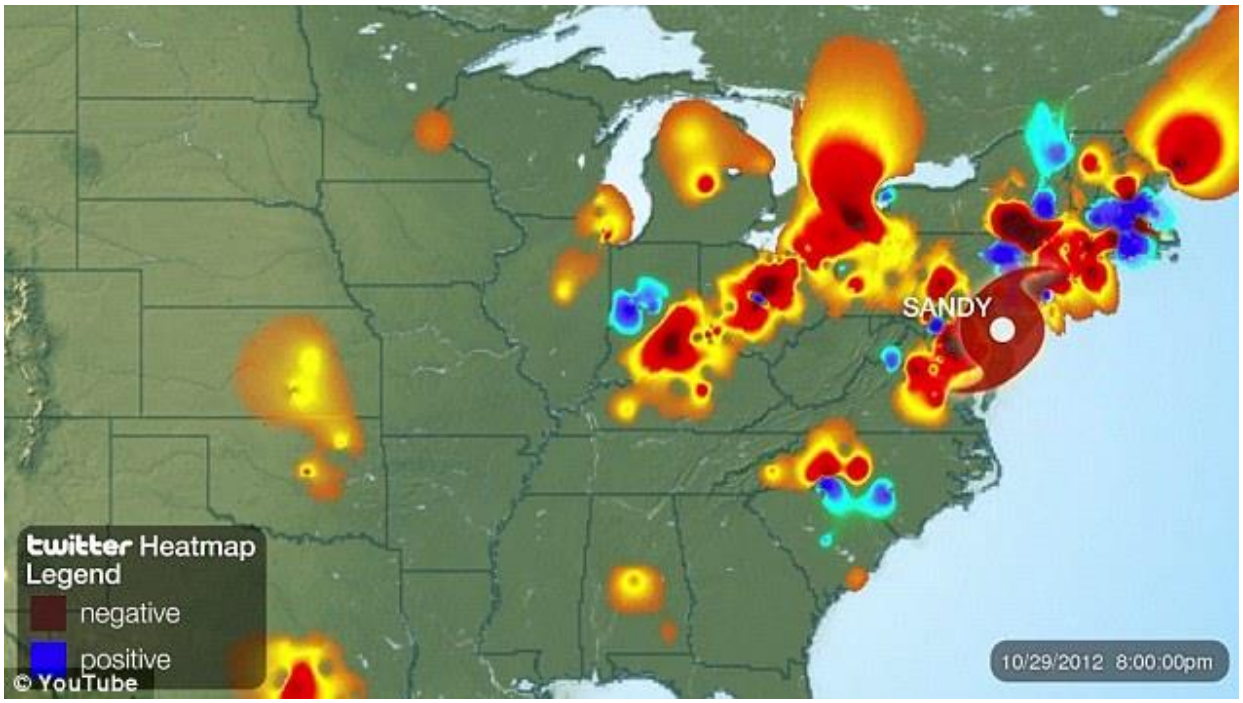
A feldolgozási lehetőségek közül a következőkben a katasztrófavédelemhez kapcsolódó érzelemelemzést mutatom be.

Az elmúlt években több kutatás is született a közösségi média és a katasztrófavédelem kapcsolatáról. A továbbiakban Ghazaleh Beigi, Xia Hu, Ross Maciejewski, Huan Liu: An Overview of Sentiment Analysis in Social Media and its Applications in Disaster Relief című tanulmány megállapításait mutatom be:

„Az elmúlt évtizedben a közösségi média (azon belül a blogok, a mikroblogok, a fórumbeszélgetések és a véleménymegosztások) robbanásszerű növekedésével az internet drasztikusan megváltozott, napjainkban a világon több milliárd ember kommunikálhat egymással. Ez lehetővé teszi számunkra, hogy bármikor földrajzi határok nélkül kapcsolódjanak egymáshoz és kapcsolatba léphessenek egymással. A létrejött, kevéssé strukturált, felhasználók által generált adatok új számítástechnikai technikákat igényelnek a közösségi média adatfeldolgozás számára, miközben lehetőséget adnak a felhasználók tanulmányozására és megértésére példátlan méretű adatskálákon. Az érzelemelemzés egyike az olyan számítástechnikai módszereknek, mely automatikusan kiszűri és összefoglalja ezen óriási adatmennyiségeket.

A közösségi médiában a véleménynyilvánítások nagy mennyisége a felhasználók tevékenységének központi eleme, melyek befolyással bírnak magatartásunkra és hozzájárultak vállalkozások átalakításában. Napjainkban az emberek a termékekkel kapcsolatban nemcsak a barátok és a család véleményének megkérdezésére korlátozódnak és a vállalkozásoknak, a szervezeteknek sem kell feltétlenül felméréseket vagy közvélemény-kutatásokat végezniük a termékekkel kapcsolatosan, hiszen számos felhasználói vélemény, és vita folyik a nyilvános fórumokon. Számos gyors és gyakorlati alkalmazás jött létre a sokoldalú érdeklődés hatására: a vélemények összegyűjtésére és tanulmányozására a fogyasztói termékekről, szolgáltatásokról, egészségügyi ellátásról és pénzügyi szolgáltatásokról, a társadalmi eseményekről, a politikai választásokról és a válságkezelésre. A közösségi média egyre inkább növekvő szerepet kapott a vészhelyzetek és katasztrófák idején a hagyományos médiumok számára fontos alternatív információs csatornájaként.

A katasztrófavédelem közösségi média alkalmazásai nagyjából két csoportba osztható: a helyzetfelmérésre és az információ megosztásra. [19]



2. ábra Sandy hurrikán érzelem-elemzése (2012 október 29.) [20]

Az OECD tanulmánya [21] részletesebben rávilágít a közösségi média információközléshez és figyelemfelkeltéshez kapcsolódó lehetőségekre:

- Korai megfigyelési – felismerési és figyelmeztető rendszerként működni a médiafigyelésen keresztül.
- A közösségi média eszközként szolgálhat információk és utasítások valós idejű riasztások és figyelmeztetések terjesztésében.
- A közösségi média segíthet az önkéntesen mozgosításában mind a válság ideje alatt, mind azután.
- A közösségi média segíthet a túlélők és az áldozatok azonosításában.
- Segíthet a pontos és hiteles információk és hírek terjesztésében.
- A közösségi média segíthet adományok felajánlásában, hogy mely segélyszervezethez fordulhatnak.
- A közösségi média a válságkommunikáció hasznos eszköze a bizalomépítésben, miután használata javíthatja az átláthatóságot és a közigazgatásba vetett bizalmat.
- A válság utáni szakaszban a közösségi média felhasználható a helyreállításra és újjáépítésre vonatkozó információk továbbítására.

SZÁMÍTÓGÉPES LÁTÁS

Egy újabb lépés a mesterséges intelligenciában – amely felhasználható a közösségi médiában is, a számítógépes látás fejlődése. A számítógépes látás az emberi látás azon funkcióit valósítja meg, amelyek a retinai kép elemzését végzik. Ezek elsősorban a képi tartalom értelmezésére irányulnak: a látott képből következtet az objektumok 3D alakjára (felület rekonstrukció), az objektumok térbeli elhelyezkedésére, egymáshoz való viszonyára (mélységi információ kinyerése), illetve több, időben egymást követő képből a mozgás érzékelése és a mozgó objektumok követése. [22] A számítógépes látás és a mesterséges intelligencia elengedhetetlen az olyan úttörő megoldások megvalósulásához, mint az önvezető gépjárművek, vagy az orvosi diagnosztikai szoftverek.

Geoffrey E. Hinton, a Google egyik vezetőmérnöke a Googe Brain Team-nek, amely a neurális hálózatok tanulásának fejlesztésével foglalkozik (amely a számítógépes látás egyik alapja). Hilton egy február eleji tanulmányában [23] kifejtette véleményét, miszerint a számítógépes látáshoz való korábbi megközelítés nem megfelelő. A neurális hálózatok helyett (amely az eddigi gépi tanulási elméletek és gyakorlatok egyik alapja) Hinton bemutatta egy másik "régi" ötletét, amely átalakíthatja a számítógépes látást és a mesterséges intelligenciát.
Hinton új megközelítése az úgynevezett kapszula hálózatok, amely a neurális hálózatok egy változata. Ennek lényege, hogy a gépek jobban meg tudják érteni a világot állóképeken és mozgóképen keresztül. A kapszula hálózatok célja a mai gépi tanulás rendszerek gyengeségének orvoslása, ami korlátozza hatékonyságukat. A ma használatban lévő képfelismerő szoftvereknek nagy számú tanulóképre van szüksége, amelyeken keresztül megtanulják az objektumok megbízható felismerését többféle térbeli helyzetben (ezért is szükséges a nagymennyiségű adat megléte, amelyet a közösségi média szolgáltat is). Ennek az az oka, hogy a szoftver nem túl jó az általánosításban, a tanultakat nem tudja alkalmazni új helyzetekhez (értelmezni, hogy egy objektum ugyanaz egy új nézőpontból).

Példának álltja, hogyha olyan számítógépet szeretnék megtanítani, hogy felismerje a macskát több szögből, több ezer olyan fotót kell feldolgoznia, amelyek számos látószögből bemutatja a macskát. Az emberi gyermekeknek nincs szükségük ilyen explicit és kiterjedt képzésre ahhoz, hogy felismerjen egy macskát. Hinton elképzelése, hogy szűkítse a szakadékot a legjobb mesterséges intelligencia rendszerek és a gyermekek természetes tanulása között, az, hogy egy kicsit több világi tudást építsen a számítógép-látószoftverébe. A kapszulákat - a nyers virtuális neuronok kis csoportjait - úgy tervezték, hogy nyomon kövessék az objektum különböző részeit, például a macska orrát és fülét, valamint az térben viszonylagos helyzeteiket. Egy több kapszulás hálózat használhatja ezt a tudatosságot annak megértéséhez, hogy egy új helyzetben lévő tárgy tulajdonképpen egy korábbi tárgy más szemszögből. Ez azért is fontos, mert nagyban meghatározza a számítógépes látás pontosságát és a tanuló algoritmusok működését.

KÖVETKEZTETÉSEK

Cikkemben kísérletet tettem összefoglalni a mesterséges intelligencia felhasználásának lehetőségeit a jelenleg és a jövőbeni irányait a mélytanulási technika neurális hálózatának tovább fejlesztésének bemutatásával a közösségi médiában. Ahogyan a mesterséges intelligencia egyre inkább mindennapi életünk részévé válik, úgy segít megérteni az emberi észlelés és értelmezés és a gépi észlelés és értelmezés közötti határokat. A közösségi médián keresztül a felhasználókról gyűjthető adathalmazok rendelkezésre állnak a vállalatok adatbányászatai számára, amelyek egyre inkább támaszkodnak a mesterséges intelligenciára, azonban a felhasználók tudatosságának növelésére is érdemes lenne fókuszálni, hiszen többségünk nem tudja pontosan, mi az, amit a közösségi médián keresztül a vállalatok és szolgáltatók tudnak róluk. Azonban ahogyan a felhasználók egyre inkább tudatásra ébrednek, hogy adataik milyen módon kerülnek felhasználásra, illetve, hogy harmadik felek (egyéb szolgáltatók, adatkereskedők) is hozzáférnek az olykor érzékeny adataikhoz, a fogyasztói hozzáállás lassan változni látszik.

FELHASZNÁLT IRODALOM

[1] KEMP, S.: *Digital in 2016.* https://wearesocial.com/uk/special-reports/digital-in-2016 (a letöltés ideje: 2018. Február 24.)

[2] BUGHIN, JACQUES ET AL.: *Artificial intelligence – the next digital frontier.* McKinsey Global Institute, 2017. június. http://www.odbms.org/2017/08/artificial-intelligence-the-next-digital-frontier-mckinsey-global-institute-study/ (a letöltés ideje: 2018. Február 24.)

[3] https://www.britannica.com/technology/artificial-intelligence

[4] LinkedIn Newsroom: *LinkedIn To Acquire Bright* https://news.linkedin.com/2014/02/linkedin-to-acquire-bright (a letöltés ideje: 2018. Február 24.)

[5] HVG / MTI : *Az ügyfélszolgálatot keresi? A mesterséges intelligencia válaszol* http://hvg.hu/tudomany/20180112_ugyfelszolgalatmesterseges_intelligencia_klm (a letöltés ideje: 2018. Február 24.)

[6] https://blogs.nvidia.com/blog/2017/01/27/faster-customer-service-with-ai/ (a letöltés ideje: 2018. Február 24.)

[7] S. RUSSELL, P. NORVIG: *Mesterséges intelligencia, Modern megközelítésben*, Második, átdolgozott, bővített kiadás, Budapest, Panem Kiadó, 2005, ISBN 963-545-411-2
Közvetlen link: http://project.mit.bme.hu/mi_almanach/books/aima/index

[8] *Bright.com* https://ph.linkedin.com/company/bright.com (a letöltés ideje: 2018. Február 24.)

[9] *Pinterest Acquires Machine Learning Commerce Recommendation Engine Kosei*, techcrunch.com. https://techcrunch.com/2015/01/21/facebook-past-google-present-pinterest-future/(a letöltés ideje: 2018. Február 24.)

[10] *KLM's next step using artificial intelligence on social media.* https://news.klm.com/klms-next-step-using-artificial-intelligence-on-social-media/ (a letöltés ideje: 2018. Február 24.)

[11] *KLM Customer Service Reps Avoid Turbulence in Social Media with AI Tool* https://blogs.nvidia.com/blog/2017/01/27/faster-customer-service-with-ai/ (a letöltés ideje: 2018. Február 24.)

[12] *Neurális hálózatok* http://www.eletestudomany.hu/neuralis_halozatok(a letöltés ideje: 2018. Február 24.)

[13] *Facebook newsroom*: https://newsroom.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/(a letöltés ideje: 2018. Február 24.)

[14] *The New York Times built a Slack bot to help decide which stories to post to social* media http://www.niemanlab.org/2015/08/the-new-york-times-built-a-slack-bot-to-help-decide-which-stories-to-post-to-social-media/ (a letöltés ideje: 2018. Február 24.)

[15] https://www.inc.com/wanda-thibodeaux/this-artificial-intelligence-can-use-social-media-to-tell-hiring-managers-about-your-personality.html (a letöltés ideje: 2018. Február 24.)

[16] https://frrole.ai/deepsense (a letöltés ideje: 2018. Február 24.)

[17] BEIGI, G., HU, X.,MACIEJEWSKI, R., LIU, H.: *An Overview of Sentiment Analysis in Social Media and its Applications in Disaster Relief* https://www.researchgate.net/profile/Ghazaleh_Beigi/publication/288516377_An_Overview_of_Sentiment_Analysis_in_Social_Media_and_Its_Applications_in_Disaster_Relief/links/56bd215208ae6cc737c6d3ed.pdf(a letöltés ideje: 2018. Február 24.)

[18] NASUKAWA, T. AND YI, J. *Sentiment analysis: Capturing favorability using natural language processing*. In *Proceedings of the 2nd International Conference on Knowledge Capture*, K-CAP '03, pages 70–77, New York, NY, USA, 2003. ACM.

[19] SAKAKI, T. Et. Al.: *The possibility of social media analysis for disaster management.* In *Humanitarian Technology Conference (R10-HTC), 2013 IEEE Region 10*, pages 238–243. IEEE, 2013.

[20] http://i.dailymail.co.uk/i/pix/2012/11/20/article-2235778-16218178000005DC-582_634x356.jpg (a letöltés ideje: 2018. Február 24.)

[21] WENDLING, C., J. RADISCH AND S. JACOBZONE (2013), *"The Use of Social Media in Risk and Crisis Communication"*, *OECD Working Papers on Public Governance*, No. 24, OECD Publishing, Paris,https://doi.org/10.1787/5k3v01fskp9s-en. (a letöltés ideje: 2018. 09.23)

[22] Kató Zoltán, Czúni László: Számítógépes látás, Typotex Kiadó, 2011. (a letöltés ideje: 2018. Február 24.)

[23] Geoffrey E Hinton, Sara Sabour, Nicholas Fross: Matrix capsules with EM routing https://openreview.net/forum?id=HJWLfGWRb&noteId=HJWLfGWRb (a letöltés ideje: 2018. Február 24.)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

THE EMERGENCE OF CYBER SECURITY IN THE SCIENTIFIC COMMUNITY

A KIBERBIZTONSÁG MEGJELENÉSE A TUDOMÁNYOS KÖZÉLETBEN

Péter BÁNYÁSZ

(ORCID: 0000-0002-7308-9304)

banyasz.peter@uni-nke.hu

Abstract

Providing an appropriate level of cyber security is essential for individuals, organizations and states. The increase of info-communication technologies further enhances our dependence on cyberspace. This study examines the occurrence of cyber security in scientific publications in order to motivate coverage of other researches related to the Hungarian topic in a broader spectrum in the field of doctoral studies.
Supported by the ÚNKP-17-3-IV-NKE-59 New National Excellence Program of the Ministry of Human Capacities.

***Keywords**: cyber security, scientific metrics, research, publications, doctoral training*

Absztrakt

A megfelelő szintű kiberbiztonság megteremtése elengedhetetlen az egyének, szervezetek és államok részére egyaránt. Az infokommunikációs technológiák számának növekedése tovább fokozza a kibertértől való függőségünket. A tanulmány a kiberbiztonság tudományos publikációkban való megjelenését vizsgálja annak céljából, hogy ösztönözze a magyarországi témával kapcsolatos kutatások szélesebb spektrumban történő lefedését a doktori képzések területén.
A tanulmány az Emberi Erőforrások Minisztériuma ÚNKP-17-3-IV-NKE-59 Kódszámú Új Nemzeti Kiválóság Programjának Támogatásával készült.

***Kulcsszavak**: kiberbiztonság, tudománymetria, kutatás, publikációk, doktori képzés*

A kézirat benyújtásának dátuma (Date of the submission): 2018.06.05.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.25.

INTRODUCTION

This study was inspired by researches conducted by Péter Sasvári és Anna Urbanovics, in which they have examined university courses related to cyber security by analyzing scientific metrics [1] [2]. As a lecturer for undergraduate and master's programme students at the Faculty of Science of Public Governance and Administration of the National University of Public Service I hold several courses on cyber security, where I ask them whether they believe that cyber security is a discipline that belongs to technology or humanities. The majority of respondents usually vote for technology. Our students participate in courses of social sciences, which means that those who typically classify cyber security as the scientific domain of technology often present themselves as persons not understand issues regarding cyber security because of its technical nature. Clearly, my small questionnaires cannot be viewed as representative, but they made me think about the scientific distribution of Hungarian researches on cyber security.

The Hungarian National Cyber Security Strategy established in 2012 defines cyber security as follows: *"Cyber security is the continuous and planned taking of political, legal, economic, educational, awareness raising and technical measures to manage risks in cyberspace that transforms the cyberspace in to a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace."* [3] It can be inferred from the definition that Hungarian strategy creators interpret cyber security as a research domain of inter- and multidisciplinary nature. In my research I tried to find answers to how the inter- and multidisciplinary approach of cyber security prevails in the case of scientific statements, and what trends can be observed in researches on cyber security. Within my examinations based on the analysis of global trends, I refer also to the evaluation of publication activities in Hungary, and I've also examined doctoral thesis topic proposals of 2018 announced regarding cyber security.

METHODOLOGY

During the course of my analyses I've conducted a keyword analysis by using the Scopus database. Scopus, founded in 2004, is the largest abstract and citation database of peer-reviewed literature, which enables the analysis of scientific journals, books and conference proceedings. I've built my database based on the keyword "cyber security" using Scopus. However, this database doesn't include the scientific domain and discipline classification of scientific statements, but I've relied on the database of SCImago Journal Rank (hereinafter SJR) in order to define it. SJR uses numerous indicators to rank scientific journals and conference proceedings based on the assessment of scientific metrics. It is important to note that a scientific journal or a conference proceeding can be relevant in several scientific domains.

The search concerned every scientific statement that included the search term "cyber security" in its title, abstract or keywords. The database, similarly to Google search interprets the connection between words based on several keywords only then, if they are in quotation marks, otherwise every result will be displayed that include the terms "cyber" or "security". The search was conducted with this restriction. The results included scientific journals, conference proceedings, books and other forms of publication. I've examined the result list according to scientific domain distribution.

In the international scientific community each scientific domain does not cover the same fields as determined in the scientific domain nomenclature by the Hungarian Academy of Sciences. The SJR distinguishes 27 major thematic areas, while the Hungarian Academy of Sciences distinct only 3 scientific domains. In my study I applied the scientific domain approach used by the SJR.

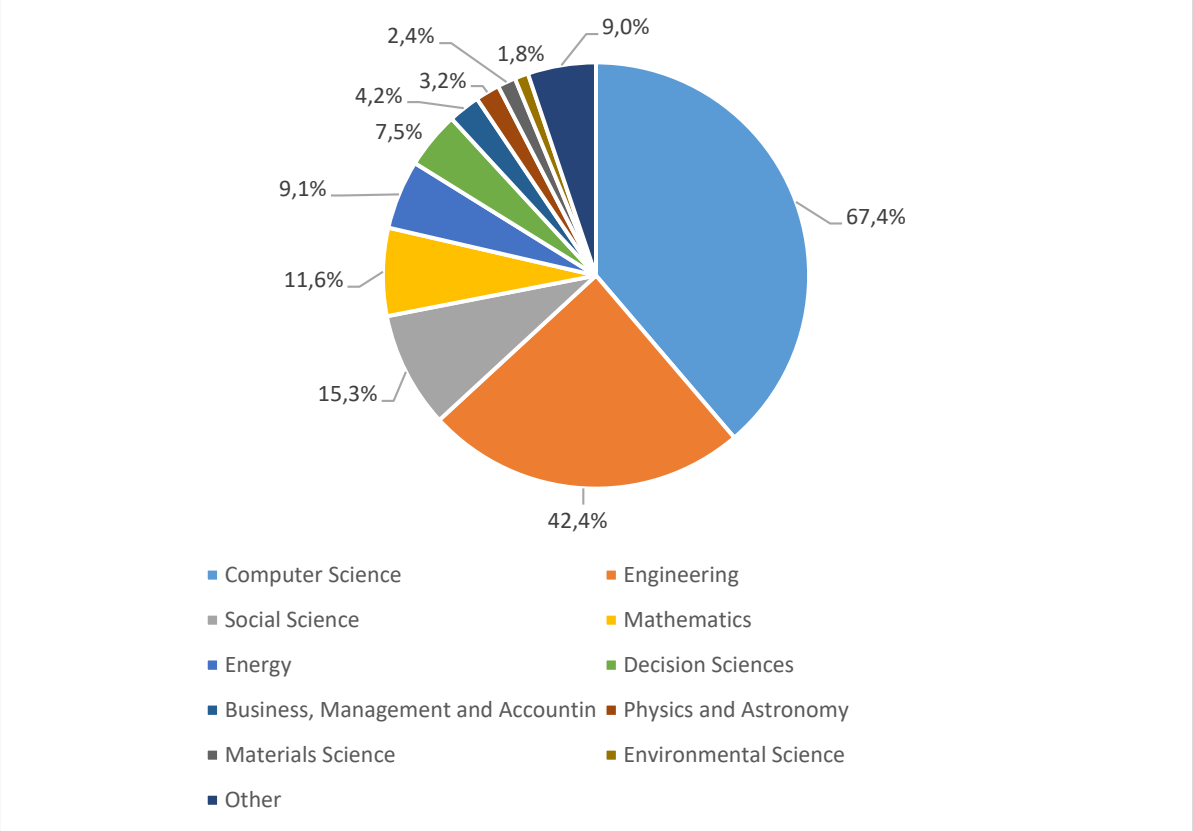
Beside the scientific metrics approach, I've also conducted a keyword analysis. Reason for this is the notion that the more frequently a certain keyword occurs the more relevant it can be

viewed as. I've conducted a trend analysis based on the occurrence of relevant keywords in order to examine whether a pattern could be determined for the proliferation of single keywords.

Further, I've conducted an international examination by limiting the scope to Hungary in order to find out how researches related to Hungarian cyber security are fitting in global trends. The proposed doctoral thesis topics in 2018 were also analyzed in order to be able to examine to what extent are new doctoral researches related to cyber security appearing in international trends. For this purpose, I've examined on one hand the doctoral thesis topic proposals related to cyber security filtered by branch of sciences, and on the other hand I've also conducted a keyword analysis in international scientific statements by using the most frequently provided keywords.

THE EMERGENCE OF CYBER SECURITY IN SCIENTIFIC STATEMENTS

Up until 2018, to May 2018 included, Scopus found 7,100 results on the search term "cyber security". Figure no. 1 shows the scientific domain distribution of statements.



1. Figure Distributions of the search terms cyber security globally per scientific domains according to SJR (own editing, source: Scopus, SJR)

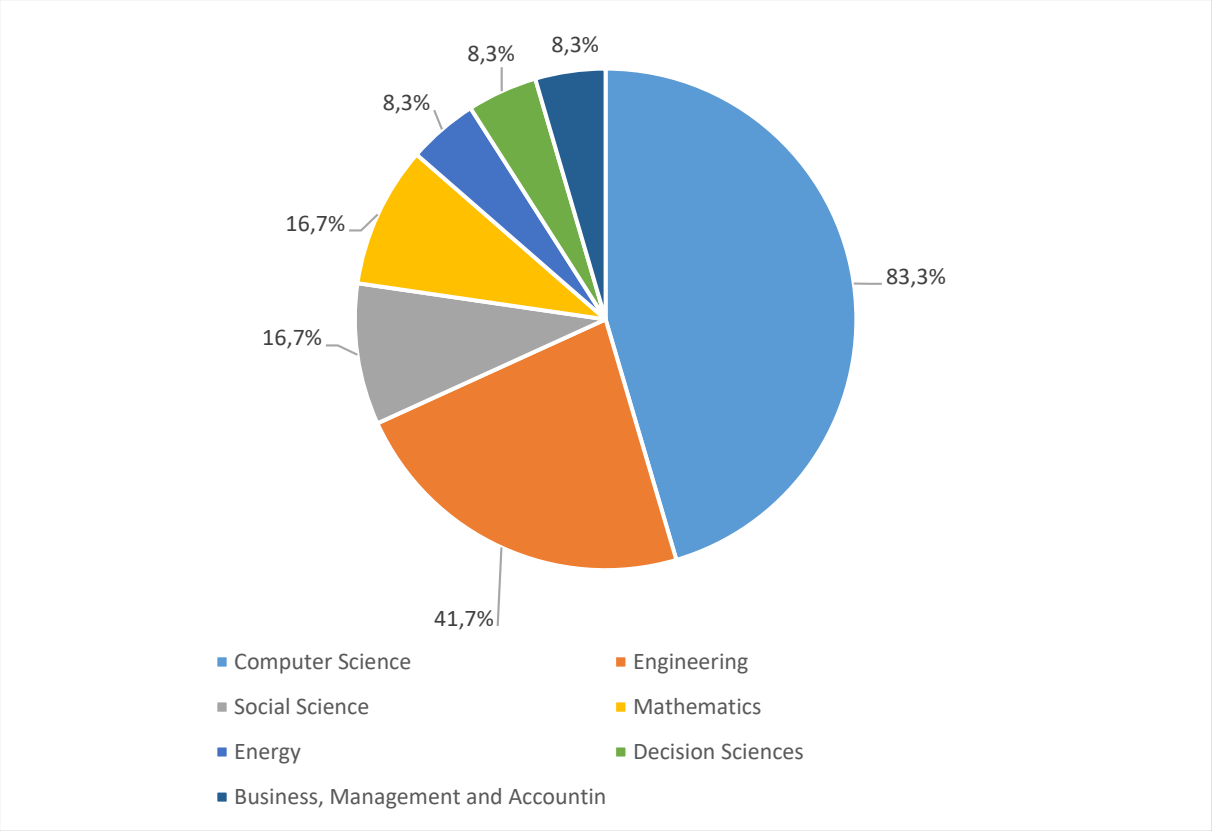
As shown in the figure publications of technical nature are dominating researches related to cyber security, 67.4% of all publications can be subject to Computer Science, and 42.4% to the scientific domain of Engineering. Social sciences only occur 15.3% in publications.

Table no. 1 shows the distribution of each publication according to country based on the top 10 countries.

Country	Documents
United States	3,115
United Kingdom	538
China	365
India	305
Canada	205
Italy	197
Australia	184
Japan	173
South Korea	164
Germany	156

1. Table Top 10 distributions amongst countries on the search term cyber security
(own editing, source: Scopus)

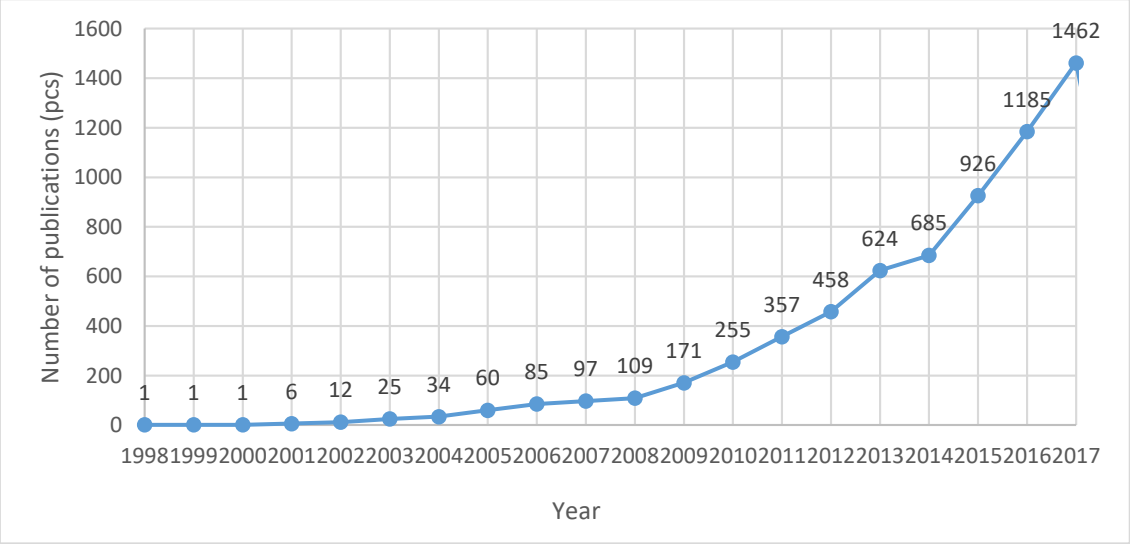
The Scopus database only stores 13 scientific statements after narrowing down the scope to Hungary. This distribution is presented in figure no. 2.



2. Figure Distributions of the search terms cyber security in Hungary per scientific domains according to SJR
(own editing, source: Scopus, SJR)

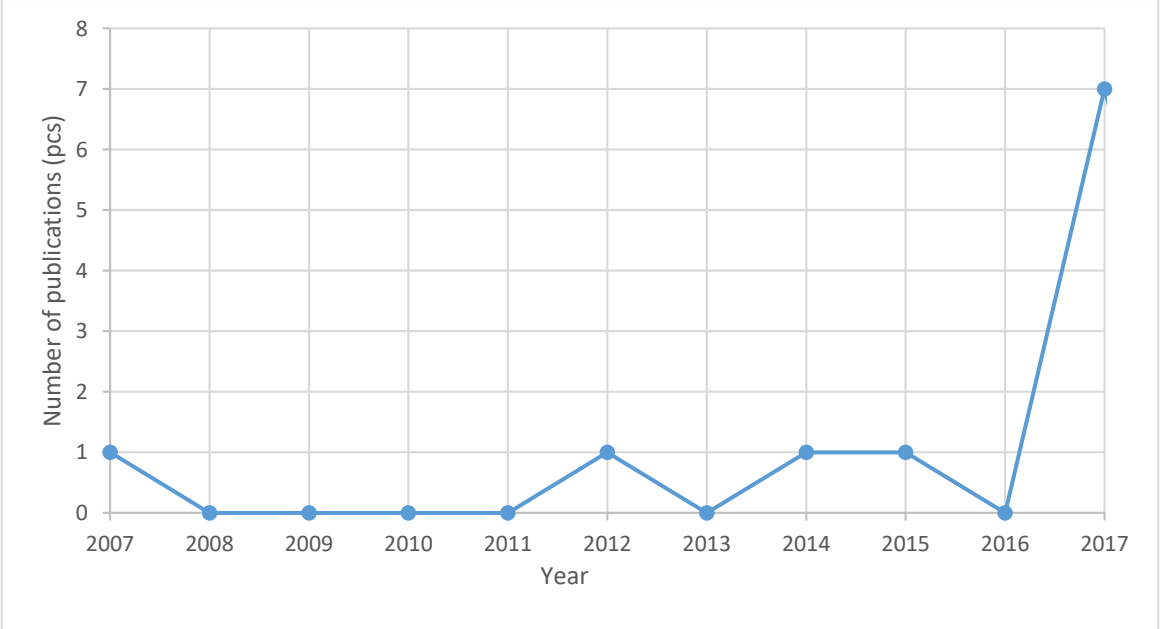
Proportionally, the classification of scientific domains of Hungarian publications is distributed almost identically. Although the dominance of Computer science is more significant, 83.3% of all publications can be included here, but the proportions are almost identical when we look at Engineering (41.7%) and Social science (16.7%).

Figure no. 3 contains the yearly distribution of each publication. Statements dated back to 2018, which means 6,557 publications are not listed in the figure. It is apparent that the first result for the search term cyber security can be dated back to 1998, and that the number of publications related to this topic has considerably grown from the year 2000.



3. Figure Yearly distributions of the number of publications globally based on the search term cyber security (own editing, source: Scopus)

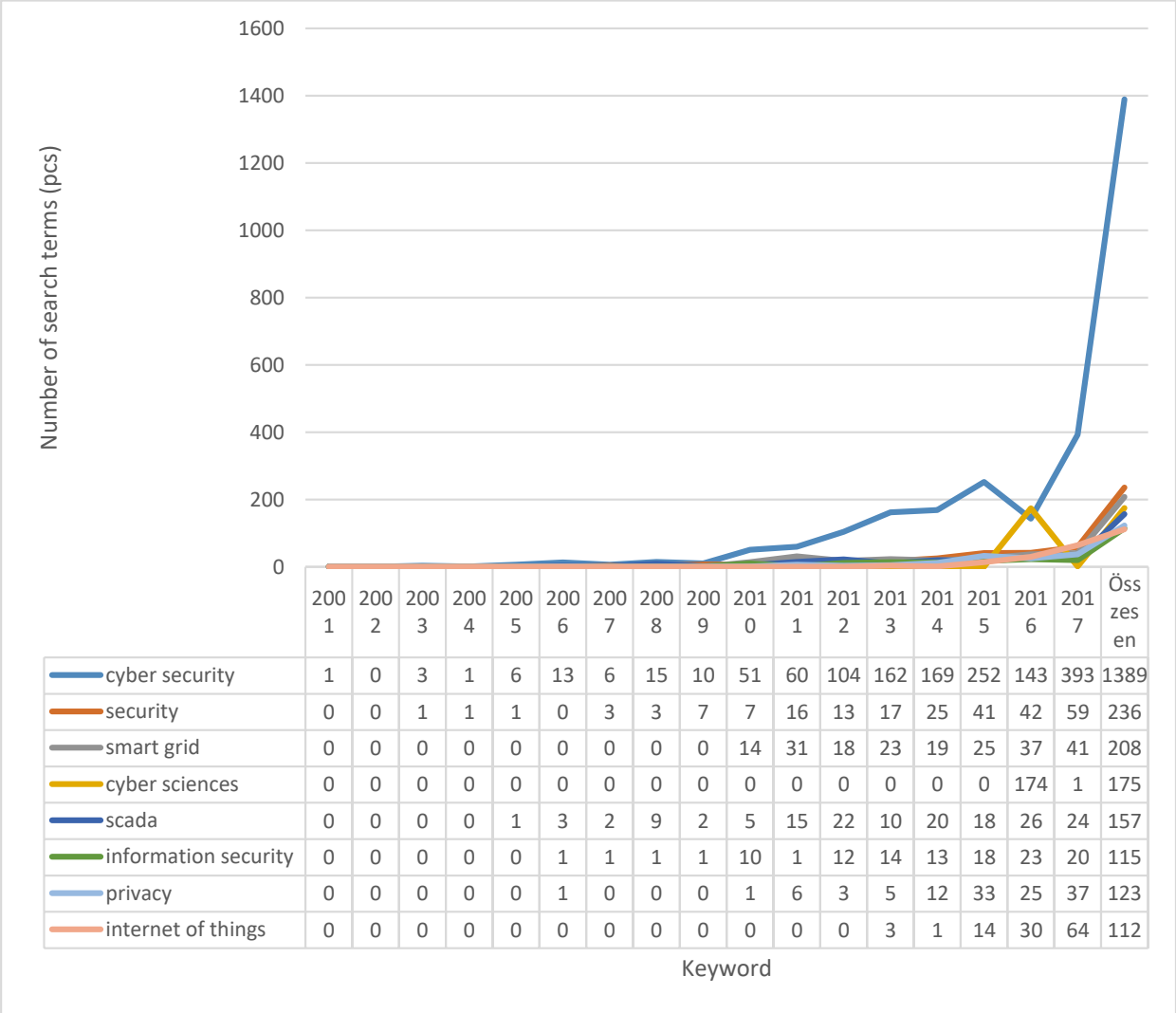
The trend of the number of Hungarian publications is represented in figure no. 4. In this case I've omitted publications from 2018, thus 11 scientific statements can be seen in the figure.



4. Figure Yearly distribution of the number of publications in Hungary based on the search term cyber security (own editing, source: Scopus)

The first publication on the topic in Hungary has been published in 2007, but more than 60% of all statements have been published in 2017.

The publications include overall 14,137 keywords, which needed to be narrowed down in order the manage them in a consistent manner. This was justified by the use of the singular and plural form of each keyword, by their different spelling,[1] and typos. In figure no. 5 I've displayed those search terms where the result rate was over 100.



	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Összesen
cyber security	1	0	3	1	6	13	6	15	10	51	60	104	162	169	252	143	393	1389
security	0	0	1	1	1	0	3	3	7	7	16	13	17	25	41	42	59	236
smart grid	0	0	0	0	0	0	0	0	0	14	31	18	23	19	25	37	41	208
cyber sciences	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	174	1	175
scada	0	0	0	0	1	3	2	9	2	5	15	22	10	20	18	26	24	157
information security	0	0	0	0	0	1	1	1	1	10	1	12	14	13	18	23	20	115
privacy	0	0	0	0	0	1	0	0	0	1	6	3	5	12	33	25	37	123
internet of things	0	0	0	0	0	0	0	0	0	0	0	0	3	1	14	30	64	112

5. Figure Occurrence of keywords globally for results on the search term security between 2001 and 2017 (own editing, source: Scopus)

The trends in the figure are interesting because the occurrence of search terms by years could explain why certain topics have peaked. The keyword privacy illustrates the validity of the finding, which occurred only in a few publications until 2013, but the number of occurrences has increased from 2014. Presumably, this can be due to the surveillance revelation regarding Edward Snowden, which can be dated back to 2013.

[1] For example cyber security, cybersecurity, Cyber security, Cyber Security, Cybersecurity

As is well known, Edward Snowden as the former employee of the National Security Agency has exposed the surveillance process related to the National Security Agency and its partner services, which has fundamentally changed our mindset regarding privacy [4].

The search terms smart grid and scada occur primarily in technical researches, but not only the occurrence of the keywords refers to the dominance of the topic. By examining the citations of all publications, we can conclude that 8 publications of the 10 most cited scientific statements are included (see table no. 2). The keywords indicated in table no. 5 are highlighted by being written in bold and italic style.

Cited by	Document title
458	A questionnaire on ***smart grid*** communication infrastructures: Motivations, requirements and challenges
332	Cyber-physical security of a ***smart grid*** infrastructure
321	Cyber-physical system ***security*** for the electric power grid
305	***Cyber security*** in the ***Smart Grid***: Questionnaire and challenges
288	***Security*** issues in ***SCADA*** networks
205	A questionnaire on ***cyber security*** for ***smart grid*** communications
198	***Cyber security*** and power system communication essential parts of a ***smart grid*** infrastructure
194	A questionnaire of game theory as applied to network security
172	***Cyber security*** analysis of state estimators in electric power systems
170	***Cyber security*** and ***privacy*** issues in smart ***grids***

2. Table The most cited scientific statements globally for results on the search term security (own editing, source: Scopus)

In the case of keywords in Hungarian publications 42 keywords occurred when examining 13 statements. These are included in table no. 3.

Keyword	Occurrence
cyber security	3
networked production	2
behavioral analytics	1
blockchains	1
cloud computing	1
computer supported collaborative work	1
cryptographic protocols	1
cyber-physical systems	1
cyber security	1
cyber security education	1
cybersecurity training	1
data protection	1
decision making under uncertainty	1
eHealth	1
factory of the future	1
fictitious play	1
gdpr	1
human factors	1
ict	1
identity management	1
information flow	1
information security issues related to information retaining principle security of the virtual world's cyber security	1
internet	1
inter-organizational trust	1
intrusion defense	1
medical devices	1
network organization	1
new security culture	1
profiling	1
resilience	1
robot operating system	1
ros 1.x	1
security	1
security operations center	1
small and medium enterprises (smes)	1
smart grid	1
smart meters	1
teamwork	1
vulnerability	1

3. Table Occurrence of keywords in Hungarian scientific statements for results on the search term security (own editing, source: Scopus)

Analyzed globally the top 10 institutions are listed in table no. 4.

Affiliation	Documents
Pacific Northwest National Laboratory	95
Carnegie Mellon University	80
Sandia National Laboratories, New Mexico	56
George Mason University	56
University of Texas at San Antonio	54
U.S. Army Research Laboratory	54
Purdue University	53
Oak Ridge National Laboratory	52
Virginia Polytechnic Institute and State University	52
University of Illinois at Urbana-Champaign	51

4. Table Top 10 distributions amongst institutions globally of publications on the search term cyber security (own editing, source: Scopus)

In Hungary 24 institutions can be determined based on authors, institutions with more than one document are listed in table no. 5.

Affiliation	Documents
Budapest University of Technology and Economics	2
Computer and Automation Research Institute Hungarian Academy of Sciences	2
Hungarian Academy of Sciences	2
Interuniversity Micro-Electronics Center at Leuven	2
KU Leuven	2
National University of Public Services	2
Óbuda University	2

5. Table Distributions of publications amongst institutions in Hungary based on the search term cyber security (own editing, source: Scopus)

The top 10 list of most publishing authors globally are included in table no. 6, the list of authors with more than one publication in Hungary are represented in table no. 7.

Author	Documents
Wang, L.	25
Ekstedt, M.	23
Kozik, R.	22
Sheldon, F.T.	22
Choraś, M.	21
Govindarasu, M.	21
Liu, C.C.	21
Weiss, J.	19
Ishii, H.	18
Zhang, Y.	18

6. Table Top 10 author's list globally for results on the search term security (own editing, source: Scopus)

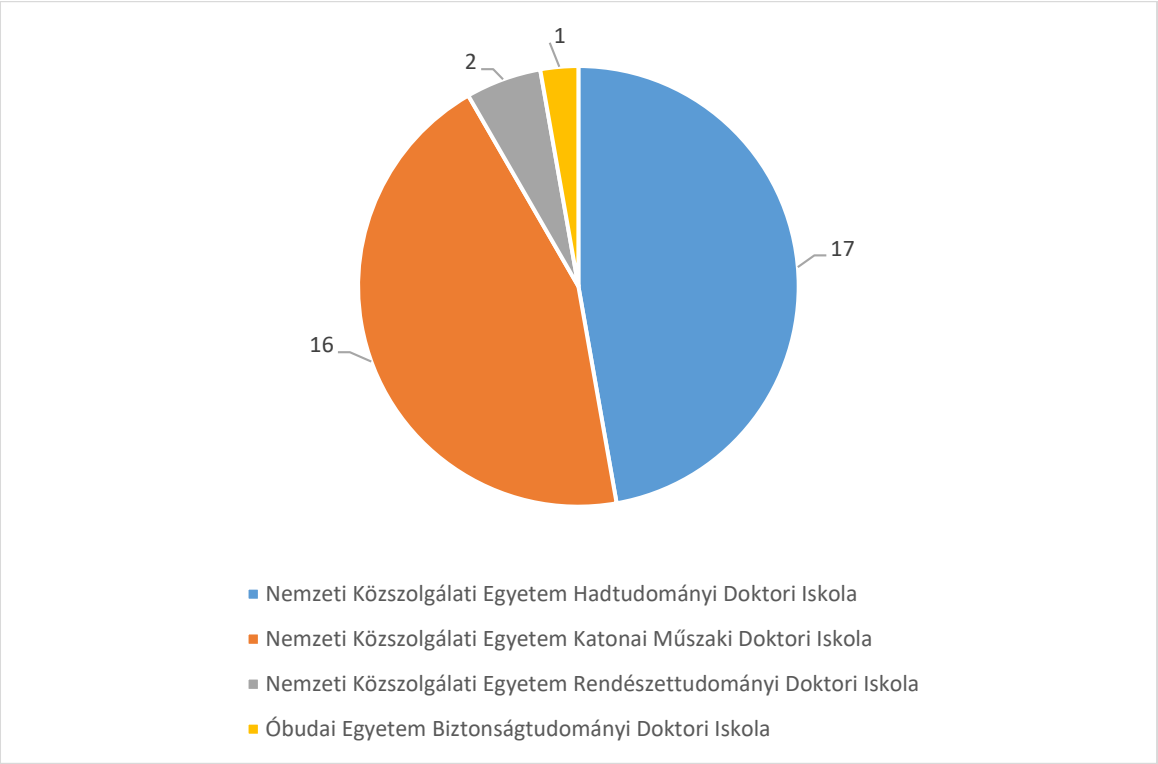
Author	Documents
Joosen, W.	2
Krasznay, Cs	2
Preuveneers, D.	2

7. Table Authors with more than one statement in Hungary based on the search term cyber security (own editing, source: Scopus)

CYBER SECURITY IN DOCTORAL PROGRAMMES IN HUNGARY

Based on Act CCIV of 2011 On National Higher Education the Hungarian Doctoral Council [5] is considered to be a legal person, and is a body comprising the chairs of the doctoral councils of higher education institutions, tasked with formulating positions on questions related to doctoral programmes and the award of doctoral degrees and laying down, in consultation with the Association of Hungarian PhD and DLA Students, the principles governing the organization of the comprehensive examinations. The Hungarian Doctoral Council shall define the principles of a quality and performance-based distribution among higher education institutions of doctoral students admitted for programmes funded through full or partial Hungarian state scholarships. The proceeding is determined by the Hungarian Government Decree no. 387/2012 (XII. 19.) Concerning Doctoral Schools, the Order of Doctoral Procedures and Habilitation [6] and the Decision no. 2013/6/III/1 by the Hungarian Accreditation Committee [7]. According to the latter doctoral advising is a professional and human responsibility and activity in helping the doctoral candidate. Experts may receive/commit such acknowledgement/task based on the decision of the Council of the Doctoral School. Only a person holding a doctoral degree may become a doctoral advisor, further, it is desirable that the assignment/commission doesn't take place right after attaining the degree, and it should be based on independent documented successful research work and publication activity. The announced topics by the doctoral advisor have to be approved by the Council of the Doctoral School. The topics have to be proposed, announced and displayed at the Doctoral School and the following website www.doktori.hu. At www.doktori.hu we can filter our search by doctoral schools, lecturers and proposed topics. In case of the latter there is opportunity to filter by branch of science and research topic. These two filters were used in my research.

I've examined proposed doctoral topics related to cyber security in 2018 that were announced in the following branches of sciences: military engineering within the technical scientific domain, military science, administration science and police studies within social sciences. Based on that we can identify 36 doctoral topics, which are distributed by doctoral schools and are included in the figure.

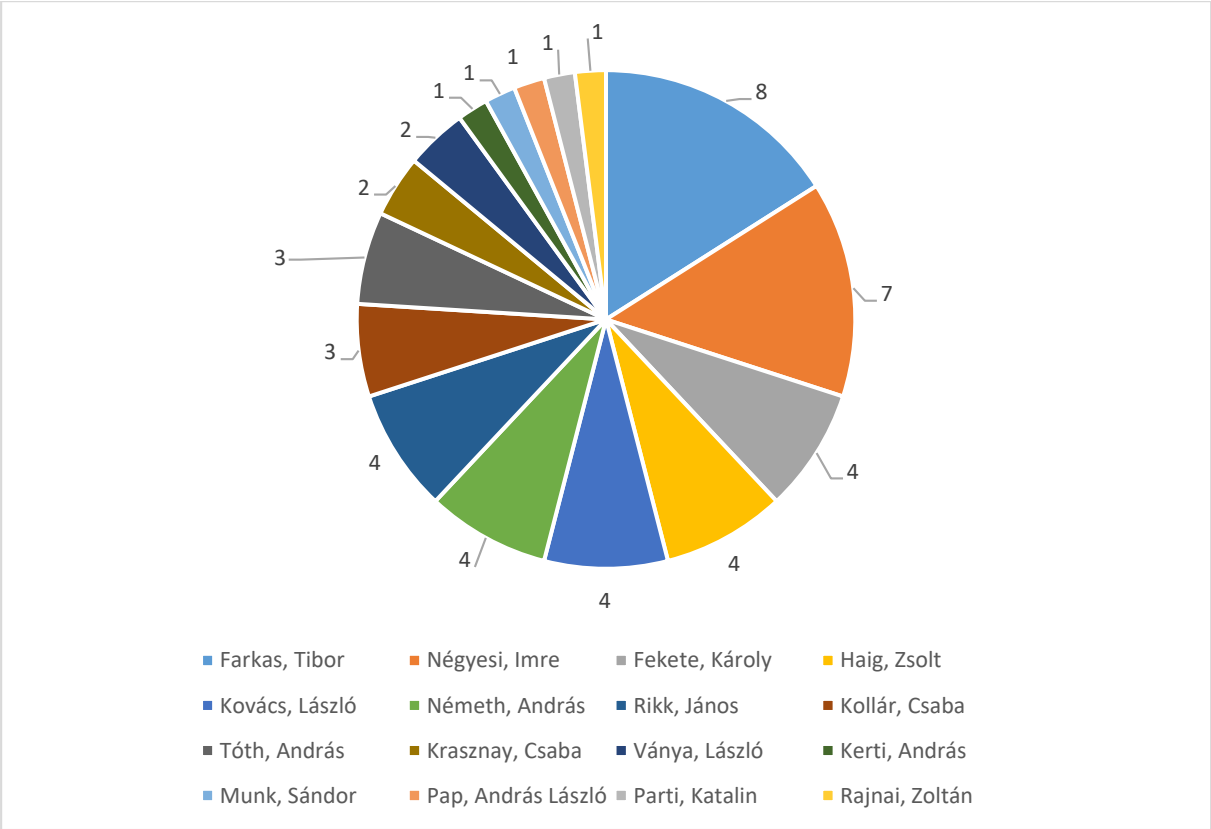


6. Figure Proposed doctoral thesis topics according to branch of sciences in 2018 (own editing, source: Doktori.hu)

The proposed thesis topics of the Doctoral School of Military Science and the Doctoral School of Police Studies at the National University of Public Service are basically related to social sciences, while proposed thesis topics of the Doctoral School of Military Engineering at the National University of Public Service and the Doctoral School of Security Science at the Óbuda University are related to engineering sciences. Based on this we can assume that the distribution between scientific domains within technical and social sciences is almost identical, rate of 17-19, but the doctoral thesis topics by each doctoral advisor and the announcements reflect essentially a technical approach.

This is underpinned by the fact that 36 proposed doctoral thesis topics are distributed between 16 doctoral advisors, of whom six[2] have announced thesis topics also in the Doctoral School of Military Science and the Doctoral School of Military Engineering (see figure 7 for the distribution by the name of the doctoral advisors). Referring to figure no. 1 and no. 2, where the engineering sciences are overrepresented regarding the scientific domain distribution of scientific statements, I believe that the proposed doctoral thesis topics regarding cyber security are following the same pattern.

[2] Farkas, Tibor; Fekete, Károly; Haig, Zsolt; Kollár; Csaba; Négyesi; Imre; Rikk, János



7. Figure Advisors proposing doctoral thesis topics in 2018 on cyber security
(own editing, source: Doktori.hu)

Only Csaba Krasznay can be found amongst the advisors proposing doctoral thesis topics on figure no. 7, who published a statement on the search term cyber security subscribed by the Scopus database (see table no. 7).

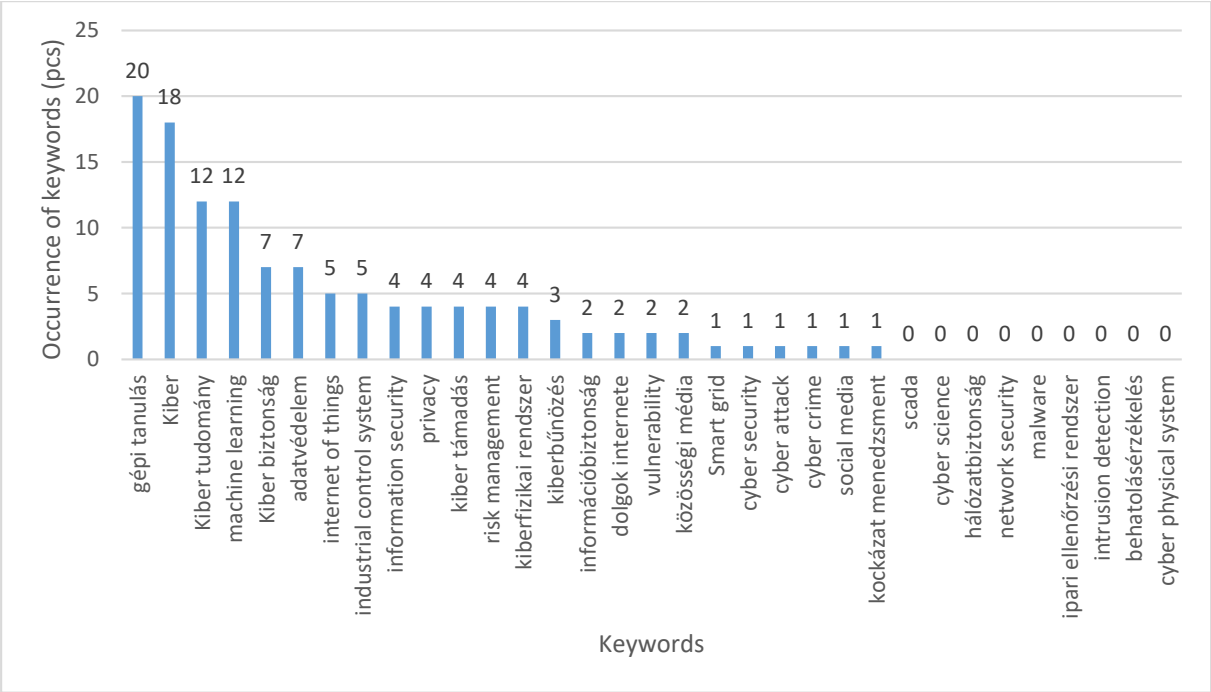
In addition to the Scopus database I've examined the publications of the advisors proposing doctoral thesis topic on figure no. 7 uploaded to the Hungarian National Scientific Bibliography. The Hungarian National Scientific Bibliography is the most important collection and authoritative database of scientific works. Data referring to scientific works and performance of researchers of participating institutions can be uploaded to the database of the National Bibliography of Hungary in a controlled manner. It is the public service obligation of the Hungarian Academy of Sciences to operate the Hungarian National Scientific Bibliography. It is mandatory for the database of the National Bibliography of Hungary containing scientific statements to display data of scientific works and scientific publications created and published within the context of an employment relationship for the budgetary entities (title, place of first publication, name of the author over which scientific statements the author has rights, and publication), for those the author received support from the budget for the creation of the scientific work [8].

Based on my examination we can consider that 16 doctoral advisors published collectively 1,043 scientific statements, 203 thereof in a foreign language. See detailed distribution of statements below.

Teacher	Overall number of scientific statements	Thereof written in a foreign language	Thereof Scopus	Number of scientific journals	Books	Book excerpt	Conference proceeding
Pap, András László	171	34		104	8	53	6
Rajnai, Zoltán	124	40		39	32	22	31
Munk, Sándor	115	24		93	2	8	12
Kollár, Csaba	94	13		32	34	14	14
Kovács, László	79	12		39	7	16	17
Haig, Zsolt	77	6	0	44	7	18	8
Ványa, László	71	5		42	3	2	24
Parti, Katalin	67	16		43	3	18	3
Négyesi, Imre	54	2	0	50	3		1
Farkas, Tibor	34	10	2	17		12	5
Németh, András	33	4		17	1	2	13
Krasznay, Csaba	32	6		11	4	4	13
Kerti, András	30	7		7	9	3	11
Fekete, Károly	28	15	0	13		2	13
Tóth, András	19	5		8		4	7
Rikk, János	15	4		8	4	1	2

8. Table Distribution of publications by advisors proposing doctoral thesis topics in relation to cyber security (own editing, source: Hungarian National Scientific Bibliography)

As formulated above, in addition to the examination by the branch of sciences I've analyzed the proposed doctoral thesis topics also by research topics. Basis for that are the 8 keywords on figure no. 5. In case of the research topics I've searched for the English terms and the Hungarian translations thereof. Based on that I've identified overall 131 proposed doctoral thesis topics, but it has to be noted that this number doesn't cover 131 different topics, because based on some keywords there is an overlapping. Th occurrence of the keywords is presented in figure no. 8. Also, those keywords are included in the figure, for which I didn't get any results, because I think that these are particularly important for the development of the Hungarian doctoral programmes. With regard to the most cited list of statements (see table no. 2), where the terms smart grid and scada were highly overrepresented, figure no. 8 can be interpreted in the following way: the keyword scada gets zero results, the keyword smart grid gets 1 result.

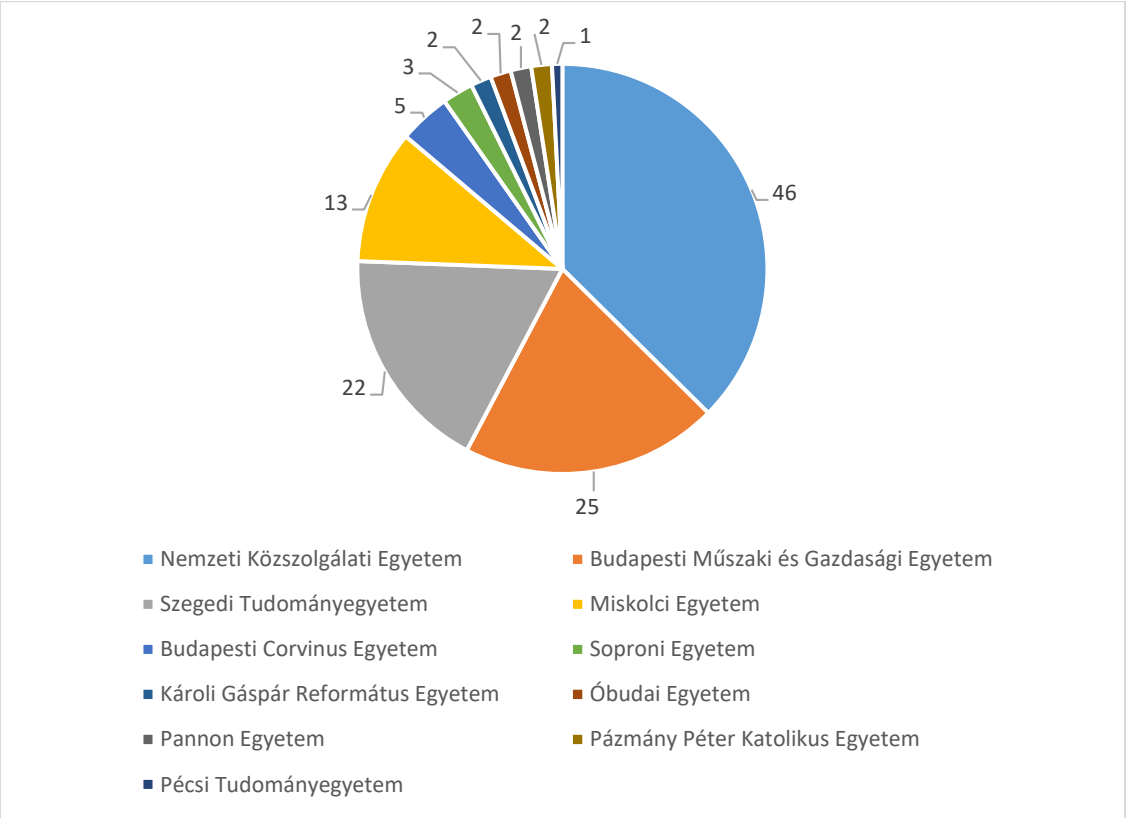


8. Figure Proposed doctoral thesis topics based on keywords in 2018
(own editing, source: Doktori.hu)

In conclusion, the main topics of international scientific publications are represented in the majority of the Hungarian doctoral thesis topic proposals, and according to the trend they are related to engineering sciences in the scientific domain approach. However, researches of technical nature that are related for example to scada systems and smart grid cyber security are underrepresented compared to international researches.

I've also examined the doctoral thesis topic proposals related to keywords included in figure no. 8 based on institutions (see figure no. 9). As indicated above, in case of filtering by keywords some doctoral thesis topic proposals are being displayed several times, which explains for example the occurrence of the National University of Public Service in 46 cases, despite the fact that within the three doctoral schools of the National University of Public Service 25 doctoral thesis topics related to cyber security were announced in 2018. It is important to note that filtering by keywords will not only show the results of doctoral thesis topic proposal related to security, but also thesis topic proposals related to the keyword.

Figure no. 9 shows that based on the keywords the substantial part of the doctoral thesis topic proposals in relation to the National University of Public Service, and nearly one third of all thesis topic proposals can be found at this institution.



9. Figure Proposed doctoral thesis topics based on keywords per institutions in 2018 (own editing, source: Doktori.hu)

SUMMARY

In my study I've examined the occurrence of researches related to cyber security in international and Hungarian scientific publications. It can be concluded based on the scientific metrics analysis of scientific statements related to cyber security stored in the Scopus database that the research domain of cyber security has an inter- and multidisciplinary nature, but engineering sciences are overrepresented.

I've examined the most important research topics with a keyword analysis that are related to researches related to cyber security.

Based on international trends I've analyzed proposed doctoral research topics in 2018 in order to map to what extent the Hungarian doctoral researches cover the most important international trends. According to this I've concluded that the current doctoral thesis topic proposals are in line with international trends and they are dominantly related to engineering sciences, but certain research topics are underrepresented.

REFERENCES

[1] URBANOVICS A.: *Az amerikai és brit kiberbiztonsági képzések elemzése tudománymetriai megközelítésből*, Intézményi TDK dolgozat, Nemzeti Közszolgálati Egyetem Államtudományi és Közigazgatási Kar, Budapest, 2018. április

[2] URBANOVICS A.- SASVÁRI P.: *Az Egyesült Királyságban működő kiberbiztonsági képzések elemzése* (workpaper)

[3] *Government Decision No. 1139/2013 (III. 21.) on the National Cyber Security Strategy of Hungary*, In. Magyar Közlöny, 2013/47.

[4] GREENWALD: GLEN: *A Snowden-ügy*, HVG Kiadó Zrt., Budapest, 2014.

[5] *Act CCIV of 2011 On National Higher Education*

[6] *Hungarian government decree no. 387/2012 (XII.19.), "Concerning Doctoral Schools, the Order of Doctoral Procedures and Habilitation*

[7] *Decision no. 2013/6/III/1* by the Hungarian Accreditation Committee

[8] *Act XL of 1994 on the Hungarian Academy of Sciences*

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

POSSIBILITIES AND SECURITY CHALLENGES OF USING IOT FOR MILITARY PURPOSES

A DOLGOK INTERNETÉNEK KATONAI ALKALMAZÁSI LEHETŐSÉGEI ÉS BIZTONSÁGI KIHÍVÁSAI

BOGNÁR Eszter Katalin

ORCID: 0000-0002-3697-7871

bognarek@uni-nke.hu

Abstract

The most recognizable shift in the age of the modern warfare is that information became the most effective weapon of all. The situational awareness based on the collected information became the core of every military operations. Information operations as a new domain entered the battlefield, the integrated network of sensors, weapon systems and platforms became force multiplier. In the advent of new technologies, new tools and processes appeared based on the concept of network-centric warfare. The aim of this article is to introduce the possibilities of using IoT for military purposes and to discover the IoT related security challenges and their potential countermeasures focusing on the devices and technologies used in the military IoT domain.

Keywords: *internet of things, information security, military sensors*

Absztrakt

A modern hadviselés kapcsán leginkább szembetűnő változás az információ, mint fegyver megjelenése. A katonai műveletek alapját a megszerzett információ révén elérhető helyzetértékelési képesség adja. A harctér kibővült az információs dimenzióval, a szenzorok, különböző fegyverrendszerek és platformok közötti koordináció erősokszorozó képességekkel bír. A technológiai fejlődés hatására új eszközök és eljárások jelentek meg a hálózatközpontú hadviselés koncepciójához kapcsolódva. A cikk célja bemutatni az IoT katonai alkalmazási lehetőségeit, a katonai alkalmazások sajátosságait, valamint feltárni az IoT alkalmazásának biztonsági kihívásait és a lehetséges megoldásokat, különös tekintettel a védelmi szférában alkalmazott IoT eszközökkel szemben támasztott speciális követelményekre.

Kulcsszavak: *dolgok internete, információbiztonság, katonai szenzorok*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.03.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.29.

INTRODUCTION

The function of recently developed technology of Internet of Things (IoT) is based on interaction, communication between different smart devices/equipments/applications using mostly wireless, radiofrequency technology. The devices that may be part of more complex systems act as smart devices taking decisions about specific context using the possibility of sharing and aggregation of information with other objects. The application of IoT has several important advantages in different applications in civil life like precision agriculture, regulation of public traffic, smart home, healthcare etc.

The military and defense sector has been recently recognized the possibilities of IoT. The introduction of paradigm of network-centric warfare directed the traditional military thinking to new directions and created a new basis for military application of extended communication networks. As the military decision cycle focuses on the information obtained from data to plan different military operations, therefore the defense sector is highly interested in the newest technologies to develop further its information processing technology including information collection, processing and transfer. The modern military operations take place in complex, continuously changing multidimensional environment, and the commanders have less and less time to evaluate information, elaboration of operation plan and taking decision based on all relevant information.

One possible solution of these challenges is the introduction of IoT in the military sector. The modern military equipments have larger and larger data processing and communication capabilities that form complex military information network integrated into military information infrastructure. These systems can be used to obtain more precise situational picture, but also in medical and logistical application.

However, several contraindications were expressed against the adaptation of these new technologies, particularly respecting the data security. The defense mechanisms in traditional computer networks are insufficient due to the high complexity of systems, the limited resources of sensors, not reliable communication links and the remote management. More research is required to identify specific security problems of the technology and to elaborate possible solutions. The aim of this article is to present the military application possibilities of IoT, features of military applications, the security challenges of applications and different solutions of IoT particularly the special requirements for IoT devices applied in defense sector.

DEFINITION, TECHNOLOGICAL BACKGROUND AND MILITARY APPLICATION POSSIBILITIES OF INTERNET OF THINGS

Internet of Things, new communication technology from the XXI. century

The recently developed technology of Internet of Things is based on the connection of several, different separated electronic devices that enables the automatic communication and sharing of information between them. However, until now there is not any exact definition for the Internet of Things due to its very fresh profile. The 2015 IEEE initiative provides a good basis for understanding this new concept and its aim is to give an overview about architectural requirements of development and a well-accepted definition for IoT [1]. The most cited definition was provided in 2017 by Gartner informatics research and consulting company: „The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.” [2]

The technological background of IoT

The IoT includes several separated technologies, like embedded systems, computer networks, cellular network, wireless communication technologies, sensor networks, data analysis, cloud-technology and four important elements contributed significantly to their widespread application:

- the development of microelectronics;
- the development of wireless communication;
- the increase of data storage and data elaboration capabilities;
- introduction of software and platforms for data processing.

Table 1 shows the IoT technological stack [4] and the technologies applied at different levels of the stack, respectively. The different endpoint devices are located in the sensing layer at the bottom of the stack. The produced sensors have smaller size and more resources due to the development of the microelectronics. The production of different, even nanometer sized intelligent devices is now possible, therefore there is a large heterogeneity. The architecture, computing capabilities, power resources, data-storage capability of different devices are highly different that makes the interoperability very difficult between them.

The network layer provides smooth communication between the devices using new protocols based on wireless, radiofrequency communication technology. Several different technologies were used by these applications including the Wi-Fi connection, and low bandwidth and shorter-range communication protocols optimized for sensors with lower, constrained resources (e. g. ZigBee, Bluetooth LE, 6LowPan). While for traditional networks several widely accepted de facto standards have been evolved, for the IoT several alternative competing technologies exist. This is highly challenging for the implementation of secure communication between the devices, e.g. the incorrect implementation of ZigBee protocol that is widely used in automation of buildings represents a high security risk [5].

The increase in the number of network devices is automatically accompanied by dramatic increase in the data volume generated by the devices. This large data volume often considered as big data should be stored and processed in real time. The new big data analysis technologies and the cloud technology have contributed significantly to the implementation of these technologies. The widely used cloud technology may solve the problem of efficient management of big data by providing scalable computing capacity and storage volume. There are software and services in the application layer provided by third-party that make the implementation of secure IoT operation even more difficult [3].

IoT layer	Technologies
Sensing layer	Sensor-networks, RFID, cameras, radars etc.
Network layer	ZigBee, Bluetooth, Wi-Fi, 6LoPAN, mobile-networks, GPS etc.
Application layer	smart home, energy/power management, self-driving cars, cloud technology etc.

Table 1 IoT three-layer stack (based on ref. [4])

Present and future military applications of IoT technology

As the military decision cycle focuses on the information obtained from data to plan different military operations, therefore the defense sector is highly interested in the newest technologies to develop further its information processing capabilities including information gathering, processing and transfer to defined person.

The introduction of the network-centric warfare paradigm [20][23] directed the traditional military thinking to new directions and created a new basis for military application of extended communication networks. Although the military application of IoT is still in its early stages, the NATO and US department of defense show large interest in it. The 2015 NATO initiative has started a relevant IST-147 research group under the name „Military applicability of IoT" aiming to identify the possibilities and tentative risks of military application of IoT technology.

In this part several military application areas are described, where the IoT devices have been already introduced or most likely will be introduced. More detailed descriptions are found in the following studies: Zheng and Carter [8], Tortonesi [7] and Fraga-Lamas [9] and Kollár [11].

Logistics

One of the most important applications of sensors in the defense sector is the logistics. The application of this new technology can revolutionize the military capability, the efficiency of the logistic management, precision, reliability, accountability can be improved, and the expenses can be reduced.

One of the most important systems is RF-ITV[1] system of US military [13] that applies RFID labels and satellites to monitor the position and condition of military cargo from sender to the destination. The shipping data are combined and processed with data from the movement detector system (MTS[2]) equipped with localization information that ensures the communication between convoys and web-based maps and report give support for logistic units. The US military labels weekly 16000 shipments with the RF-ITV system based on 2010 data that forms the largest RFID-based shipment monitoring system all around the world.

Fire-control system

The automatic system controlled by sensors is used first for fire-control systems. These systems use sensor data to react even faster and more precise to new events. The integrated marine ballistic missile defense system Aegis applies high performance computer and radar technology to monitor and aim at enemy targets.

It was used first time by US Marine Corps and was followed by deployment by Australian, Japanese, Spanish, Norwegian and Korean Marine Corps. The high preciseness AN/SPY[3] radar system can detect, monitor and direct missiles completely automatically and simultaneously to 100 different targets [8].

Military training

The IoT technology can be applied even during military training. The different combat situations can be modeled by virtual reality. The positions and physiological condition of soldiers are detected by sensors during the military training. The obtained video- and audio-data can be evaluated later anytime.

One of the simulation systems used by several armies including the US army and Hungarian Defense Forces is the MILES[4]. It can simulate real combat situations like the well-known laser tag game. The sensors attached to the uniform of the soldier detect the laser light, count the

[1] RD-ITV – Radio Frequency In-Transit Visibility –
: https://trainer.rfitv.army.mil/login/Login.do
[2] MTS – Movement Detection System –
: http://www.alu.army.mil/alog/issues/julaug05/success_mts.html
[3] AN/SPY radar – http://missiledefenseadvocacy.org/missile-defense-systems-2/missile-defense-systems/u-s-deployed-sensor-systems/anspy-1-radar/
[4] MILES – Multiple Integrated Laser Engagement

detections and provides a sound signal. The newer version of MILES is more complicated and can simulate combat situation with combined arms [8].

Health monitoring

The different sensors play an important role also in the health monitoring of individual soldiers. The soldiers are equipped with special helmets with integrated control-sensors to detect concussion and other brain traumas. Small, intelligent telemetric health monitoring and healthcare devices are more and more frequently used in combat situation, therefore the first aid/healthcare service can be provided without any staff for soldiers. The Tempus Pro [17] deployed by US, British and Norwegian Army is an advanced system that can monitor virtual signals. Figure 1 depicts the field operation of Tempus Pro equipment by a soldier.

Figure 1 Field operation of Tempus Pro [17]

Energy management, smart military bases

The IoT technology can be applied in military application and build smart military bases using the concept of smart cities that are already introduced to practice. The smart military bases would be such facilities that are able to optimize the energy resources of the military bases using the inherent properties of the technology. These bases would contribute to the comfort feeling of the employer of the base, monitor the different events in the base and register the entry and exit of the staff. Small projects aiming the optimization of energy support were already running like the 2015 NATO Smart Energy[5] initiative that had a military operation in military training base in Bakony-mountain in Hungary.

Intelligence, C4ISR

The application of IoT technology has the higher benefit in case of C4ISR systems. The C4ISR[6] systems use several millions of sensors on different platforms to ensure developed situational awareness. The highly complex and widespread network including several millions of sensors (sensors in different platforms like unmanned aerial vehicles, radars, video-cameras, infrared or passive infrared sensors, unattended ground sensors, portable devices) provides real time data for combat troops and decision makers. These data can be integrated and used for a common operational picture supporting the decision making by commanders, improved coordination and control on the operational area.

[5] NATO Smart Energy: http://www.natolibguides.info/smartenergy/documents
[6] C4ISR - C4: Command, Control, Communications and Computers –
ISR: Intelligence, Surveillance and Reconnaissance

The energy saving property and lifetime of devices are highly crucial in real combat situation, therefore further development of different hardware, communication protocols and software elements is required for optimization of energy management of devices. The currently running DARPA N-Zero project [14] aims to extend the lifetime of sensors connected to a network in real combat situation from months to years.

The design and operation of devices should fill all requirements related to architecture of military equipments and transfer capabilities. Tactical networks are required that enables encrypted communication and hardly decipherable data transfer. On the other hand, the rate of data transfer of these networks is significantly smaller than that of cellular networks.
Some research projects aim to develop solutions using wideband radiofrequency that fills the IoT requirements. The project granted to Harris has a function to develop new generation radio system [21] for combat situation. The system serves simultaneously more than 200 users and enables high-speed data transfer, while it fulfils special military purposes and encrypting requirements. The high number and different types of data represent a great challenge for the data processing [22].

The concept of combat soldier using intelligence network appeared during the US Nett Warrior program that developed persistent Android devices for US army [8]. These devices correspond to the military equivalent of the commercially available Samsung Galaxy Note II smartphones with the function to enable more precise information via combat military applications like Blue Force Tracking, 3D maps and targeting applications. The main C4ISR data integration platform of US army, the Distributed Common Ground System (DCGS)[7] analyses and combines the data obtained from sensors located in different platforms and gives an overview about position and arrangement of friendly and enemy troops ensuring better coordination and control in combat situation.

IoT technology in Hungarian Defense Forces

Hungary as all other NATO members should be able to participate in network centered operations therefore the Hungarian Defense Forces should be interested in and adapt new technologies.

Although the implementation of IoT technology for Hungarian Defense Forces has not done yet due to mainly financial reasons, but several initial steps to this direction can be already recognized like the participation in NATO Smart Energy program, the smart border barrier with different types of sensors on the Hungarian-Serbian border to control the illegal migration [19], or the MILES system used in the military training. The Zrínyi 2026 defense and development program, which started in January 2017, might eliminate these financial problems as in accordance with the decision of the Hungarian government the military expenses of the budget increases by 0.1% of the GPD each year providing a good basis for rational developments and implementations. Although there is not sufficient public information about the plans of the program, but several acquisitions are expected based on the main tasks of military organizations in 2018 (5/2018, II. 23), and the directive of the Ministry of Defense about the most important trends during the period 2019-2020 [18]. That could help the digitalization of the Hungarian Defense Forces and the introduction of new technologies like the IoT. Today, the greatest challenge for the Hungarian Defence Forces is the protection of the country's borders, which can ensure the defence of the country's population against the illegal immigration, smuggling and terrorism. The application of smart IoT sensors, e.g. acoustic and seismic unattended ground sensors buried in the ground could significantly improve the detection rate of the already

[7] DCGS – Distributed Common Ground System

installed smart fence on the Hungarian-Serbian border. Further possibilities of IoT are the development of a modern, network-integrated custom equipment system that can increase the combat ability of the soldier in the Hungarian Defense Forces [31] and the sensor application in the case of unmanned aerial and ground vehicles.

Summary

The Table 2 summarizes the initial adaptation of IoT technology and the military applications that were described in more detail in this section.

IoT application area	Relevant systems	Applied technologies
Logistics	RF-ITV	RFID, geolocation, RF detector, cloud
Fire-control systems	AEGIS	radar, laser, sensor-networks, geolocation, cloud
Military training	MILES	geolocation, virtual reality, sensors operating in different sensing ranges, servers
Healthcare and health monitoring	Tempus Pro	biosensors, servers
Intelligence, C4ISR	Distributed Common Ground System (DCGS) Nett Warrior	radar, laser, sensor-networks, geolocation, cloud
Energy management, Smart military bases	NATO Smart Energy	Sensor-networks, cloud

Table 2 IoT solutions and technological background used in defense sector

SECURITY CHALLENGES AND POSSIBLE SOLUTIONS

Introduction

The most important concern related to the IoT technology in both civil and military area is the data security. More and more devices are connected in a large extended network and the increase of number of devices and the system complexity provides increasing number of different types of security risks.

It is highly remarkable how important is data security in the IoT strategy of USA [24] and NATO [10] and how the most important strategic principles are postulated for the introduction of IoT devices in military application or the development, operation of special military IoT technologies:

- already during the planning phase should be considered the data security and built-in in the system;
- continuous security updates and vulnerability management;
- following proven practices for the realization of data security;
- facilitating the sharing of proven practices;
- the interoperability should be supported between different devices;
- the education of informatics and data security should be supported.

Features of IoT systems from data security and data protection perspective

As all other new technologies, the Internet of Things represent several challenges besides the undeniable benefits. As the IoT is tightly connected to communication and information technology, therefore the challenges of information security and data protection should be met. Although there are many similarities between the traditional communication systems and IoT

systems, but in point of view of data security and data protection large deviations are expected due to the special features of IoT technology. The common protection mechanisms used in traditional systems (firewalls, IDS/IPS[8] systems etc.) are usually not always sufficient.
In spite of traditional communication systems, the IoT technology has the following features [6]:

- high-number of devices;
- heterogeneous networks;
- the devices can be anywhere and are difficult to protect;
- problems with the limitation of energy resources;
- the increasing number of information results in an urgent challenge to establish reliable data security;
- the intrusion or attack could be more efficient and detrimental due to the high-number of connections between systems;
- dynamic characteristics of systems.

The number of smart devices organized in network exceeds currently the total population of the earth. This represents a great challenge as the network has high-number of heterogeneous nodes and devices: the devices with different energy management, different communication protocols and hardware and software-components made by different producers that makes the implementation of defense mechanisms used for classical systems very difficult.

While the servers and workstations for classical systems are localized in a well-protected inner unit, the PCs, notebooks, sensors in different sizes can be found everywhere and difficult to protect against damages and theft. The IoT devices operate usually with accumulator or solar cells and have low computing capacity and memory. The devices with limited resources are not suitable to handle systems with complex security solutions like complicated encrypting algorithms. The main element of Internet of Things is the universal informatics: the daily used devices became part of our life, collect data about us and share these data by connecting with other devices. All these data transfers represent mostly underestimated potential risk for data security.

The increase in the number of devices organized in a network generates larger and larger volume of data those protection and supplement with user access require more sophisticated solutions. While the extent of tentative attack extends to the border of the system, the security risks affect broader range and include more serious damages in case of IoT technology due to the informatics solutions that are used generally. Further challenge originates from the dynamic, self-organizing property of networks whereby different devices can connect and disconnect anytime to different networks, thus the corresponding data security anti-measure should be always adjusted accordingly.

Cyber-attack against military IoT systems and possible protection mechanisms

The largest drawback of IoT technology is the serious risks in data security. Several studies try to find solutions to problems of different types of vulnerability. As this complex system includes several different technologies, therefore the variation of possible attacks is remarkable high as well. One of the most organized methods of intrusion is the decomposition of IoT technology into layers and the analysis of possible intrusions in individual layers.

This section demonstrates the intrusion possibilities in three layers of IoT occur in military systems (sensing layer, network layer, application layer) and the possible countermeasures

[8] IDS/IPS – Intrusion Detection System/Intrusion Prevention System

against the intrusion (Oracevic, A. et al.[25], Mouaatamid, El. O. et. al.[26], Andrea, I. et al.[27], Jing, Q. et al.[28] and Wrona, K. [29]).

Intrusion in the sensing layer

One of the most vulnerable points of military system for intrusions is the sensing layer. This layer is responsible for data collection and those data collection sensors works in this layer that play also role in data collection and transfer. The sensors of the sensing layer should prevent different types of physical attacks like damage of data collection units and shortening of the lifetime and functionality of sensors. Among in the previous section presented applications areas, the RFID and the intelligence sensor-networks without surveillance represent enhanced risk, because these systems consist of physically exposed sensors with limited resources that communicate with low density performance signal.

The most important intrusion types:

- tampering of nodes: tampering of all or parts of nodes, introduction of new legal node or access to nodes data via electronic or physical connection (USB connection);
- jamming: The intruder perturbs with high density signal the radiofrequency communication between nodes. The node is unable to fulfill its function and it denies finally the service (Denial of Service - DoS);
- physical damage;
- sleep deprivation attack: The most sensing nodes of the IoT system are supplied with replaceable elements, and in absence of communication it switches to sleeping mode to prolong the lifetime of the battery. The intrusion keeps the nodes awake that induces more energy consumption, therefore the nodes are discharged faster.

There are several modes of protection against intrusions in the sensing layer:

- secure boot, node validation: the software and hardware should be validated by low calculation demanding encrypting algorithms;
- checking the data integrity and reliability: A diagnostic tool should be installed in all devices to ensure that data are not damaged, and the data transfer should be achieved with encrypting mechanism;
- the built-in data deleting mechanisms could protect against physical intrusion and data theft

Intrusions in network layer

The communication between nodes is achieved in data transfer media. As it is about very important, confidential data therefore is highly crucial to ensure the confidentiality, integrity and accessibility of the data.

The main types of intrusions in network layer:

- spoofing: the intruder identifies itself as another user of the network and gets unauthorized access to special data;
- sinkhole attack: the intruder deviates the network traffic to one specific target, therefore the data are not transferred to the original address (DoS), and furthermore sometimes they are diverted to an unauthorized user;
- man in the middle attack: The intruder influences the communication between two sensor nodes via the network and monitor the data transfer and collects data;
- denial of service: The network node is bombed by high number of requests therefore it becomes unable to fulfill its function;
- eavesdropping: The enemy detects and decrypts messages between the devices in the network.

There are different types of validating mechanisms as protection measure against intrusion in the detector layer like safety routing solutions and encrypting between end-to-end connections.

Intrusion in the application layer

Trojans, viruses and spy programs can steal, tamper data or results in deny of services via running malicious scripts in the application layer by damaging the devices of the IoT system and the confidentiality of data stored in the system. The intrusion detecting systems, access control lists, key management and firewalls are potential protecting tools against these intrusions. The application of private clouds decreases significantly the risk, but several important factors should be taken into account by operation of cloud services by third-party. Figure 2 summarizes the most important intrusions and possible countermeasures.

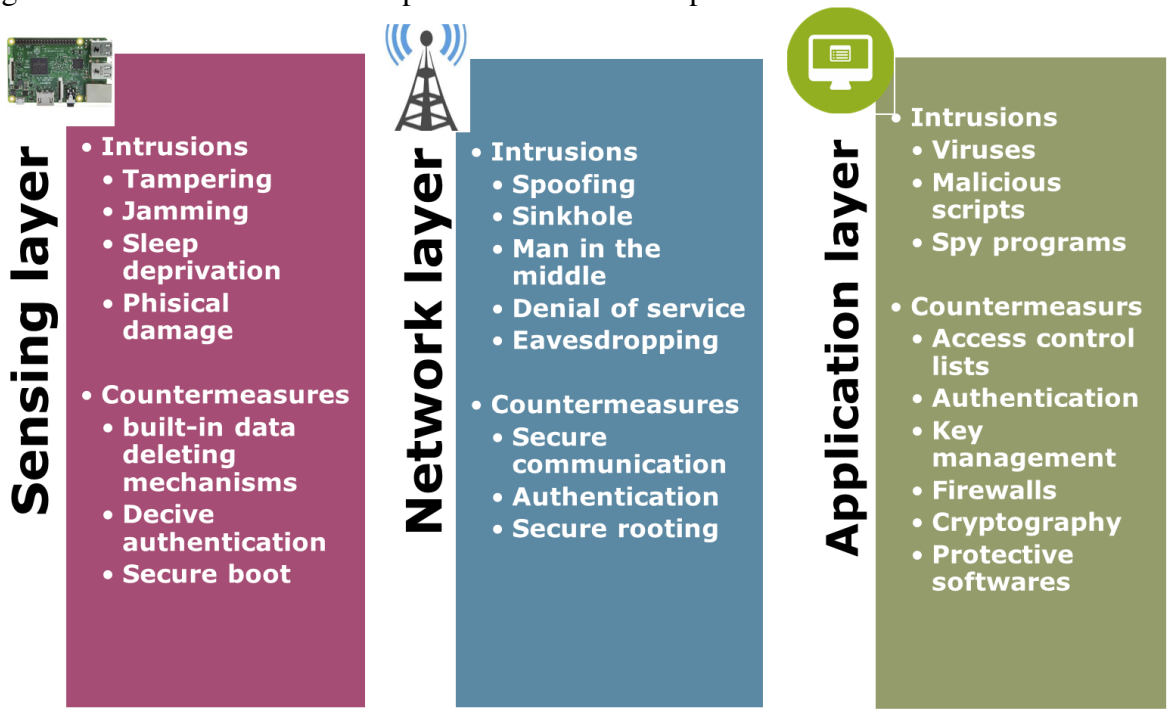


Figure 2 The most important intrusions and possible countermeasures (Made by the author)

SUMMARY

The widespread application of Internet of Things will influence significantly the military operations in the future. The application of smart sensors installed on weapon system on different platforms like ships, unmanned fighters, ground vehicles offers new possibilities for the army. The efficiency of military operations, the quality of different services can be enhanced and cost reduction and saving of human life can be achieved. The commanders can take real time decisions based on IoT technology by meaning of complex military information networks that can be used efficiently for acquiring of more precise situational picture and informational superiority.

The new technology described in this paper offers significant developments in several different military application areas. The recent projects in the comprehensive virtual simulation of military training, the networking soldier, smart health monitoring/healthcare, self-driven vehicles, smart logistic systems, smart military bases, smart energy management, integrated intelligence analysis systems mark the initial trend and important developments on this field is expected in the future.

The most important drawback of the widespread military application of IoT technology is the high vulnerability of these complex systems. Although some research projects have been started on this field, but until now no sufficient safety mechanisms fulfilling the demand of the IoT technology have been elaborated. The recently available solutions focus on the adaptation of mechanisms of traditional PC networks to the devices with smaller energy resources (small cryptographic algorithms with low calculation demands, diagnostic methods, optimized routing solutions in the point of view of energy consumption). I share the opinion that the implementation of comprehensive data security requires a new approach. The project of DARPA LADS [30] is a new, revolutionary initiative, which does not follow the traditional protecting mechanism avoiding the limitation due to the limited energy resources of IoT devices. The program focuses on the development of such a technology that are suitable to associate different types of physical changes like electromagnetic radiation, power fluctuation, thermal output changes to the function of the device. These patterns could serve as a reference later. The abnormal change of the physical modality can be an indicator of the incorrect operation, eventually an intrusion into the system. This problem is a hot-field in the military application research, as the information control provides the most important advantage. The different IoT technologies offer very attracting solutions for this demand. Hungary as a member of the NATO should participate also in this inevitable digitalization development.

REFERENCES

[1] IEEE Internet Initiative: Towards the definition of the Internet of Things (IoT), https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf (letöltve: 2018. 04. 28.)

[2] HUNG, M., Gartner: Leading the IoT: Gartner Insights on How to Lead in a Connected World, https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf (letöltve: 2018. 04. 28.)

[3] IHS Markit: IoT trend watch 2018, https://ihsmarkit.com/Info/0118/iot-trend-watch-2018.html (letöltve: 2018. 04. 28.)

[4] ZHAO, K., GE, L. (2013). A survey on the internet of things security. Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013, 663–667.

[5] ZILLNER, T., STORBL, S.: ZigBee exploited: The good, the bad and the ugly. Black Hat USA, 2015 https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly.pdf (letöltve: 2018. 04. 29.)

[6] KAMRANI, F., WEDLING, M., RODHE, I.: Internet of Things: Security and Privacy Issues, FOI Swedish Defence Research Agency, Defence and Security, Systems and Technology, 2016. FOI-R--4362—SE, https://www.foi.se/report-search/pdf?fileName=D%3A%5CReportSearch%5CFiles%5C0317a384-8808-414a-9e4c-95743fc22436.pdf (letöltve: 2018. 04. 28.)

[7] TORTONESI, M. et al.: Leveraging Internet of Things within the Military Network Environment – Challenges and Solutions. In: Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, 2016, pp. 111-116.

[8] ZHENG, Denise E. – CARTER, William A.: Leveraging the Internet of Things for a More Efficient and Effective Military; A Report of the CSIS Strategic Technologies Program, Rowman & Littlefield, Lanham, 2015.

[9] FRAGA-LAMAS, Paula – FERNÁNDEZ-CARAMÉS, Tiago M. – SUÁREZ-ALBELA, Manuel – CASTEDO, Luis – GONZÁLEZ-LÓPEZ, Miguel: A Review on Internet of Things for Defense and Public Safety. In: Sensors, Vol. 16. Issue 10., 2016, 1644, doi:10.3390/s16101644, http://www.mdpi.com/1424-8220/16/10/1644/pdf (letöltés ideje: 2018.01.07.)

[10] TONIN, M.: The Internet of Things: Promises and Perils of a Disruptive Technology, NATO Report, 2017. https://www.nato-pa.int/document/2017-internet-things-tonin-report-175-stctts-17-e-bis (letöltve: 2018. 04. 29.)

[11] KOLLÁR Csaba.: Az IoT katonai felhasználási lehetőségei és fejlesztés irányai. In: Hadmérnök, XII. évf. 4. szám, 2017, pp. 146-158. http://hadmernok.hu/174_15_kollar.pdf (letöltés ideje: 2018.01.07.)

[12] US DOD and NATO plan Battlefield Internet of Things connecting sensors, wearables, weapons, minitions, platforms and networks for information dominance, http://idstch.com/home5/international-defence-security-and-technology/cyber/internet-things-battlefield/?print=pdf (letöltés ideje: 2018. 05. 01.)

[13] Defense Industry Daily: RFID Technology: Keeping Track of DoD's Stuff, 2010, https://www.defenseindustrydaily.com/rfid-technology-keeping-track-of-dods-stuff-05816/ (letöltés ideje: 2018. 05. 01.)

[14] International Defence, Security & Technology: DARPA's N-Zero extends the lifetime of IoT devices and remote sensors from month to years, 2017, http://idstch.com/home5/international-defence-security-and-technology/technology/energy/darpa-s-n-zero-program-will-allow-unattended-wireless-sensor-network-monitoring-for-years/ (letöltés ideje: 2018. 05. 01.)

[15] BROWNE, J.: Strong Defense Depends On a Technological Edge, 2017, http://www.mwrf.com/systems/strong-defense-depends-technological-edge (letöltés ideje: 2018. 05. 01.)

[16] HAASE, N.: Distributed Common Ground System–Future: Moving into the 22nd Century Today, JFQ 77, 2nd Quarter, 2015, http://ndupress.ndu.edu/Media/News/Article/581879/distributed-common-ground-systemfuture-moving-into-the-22nd-century-today/ (letöltés ideje: 2018. 05. 01.)

[17] Tempus Pro: Tempus Pro: https://www.rdtltd.com/products/tempus-pro-advanced-vital-signs-monitor/ (letöltés ideje: 2018. 05. 01.)

[18] 5/2018. (II. 23.) HM utasítás a honvédelmi szervezetek 2018. évi feladatainak, valamint a 2019-2020. évi tevékenysége fő irányainak meghatározásáról

[19] BOGNÁR E.: Szenzorhálózatok határvédelmi alkalmazása, HADMÉRNÖK XII: (3) pp. 175-187., http://hadmernok.hu/173_16_bognar2.pdf (letöltve: 2018. 05. 02.)

[20] HAIG ZS., KOVÁCS L., VÁNYA L., VASS S.: Elektronikai hadviselés. Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[21] HARRIS: US Special Operations Command Awards Harris Corporation $255 Million IDIQ Contract for Next-Generation Manpack Radios. https://www.harris.com/press-releases/2017/06/us-special-operations-command-awards-harris-corporation-255-million-idiq (letöltés ideje: 2018.01.07.)

[22] MARIANI, Joe – WILLIAMS, Brian – LOUBERT, Brett: Continuing the march: The past, present, and future of the IoT in the military. https://www2.deloitte.com/insights/us/en/focus/internet-of-things/iot-in-military-defense-industry.html (Letöltve: 2018.01.07.)

[23] DEAKIN, Richard S.: Battlespace Technologies – Network-Enabled Information Dominance. Artech House, Boston, 2010. ISBN: 978-1-59693-337-8

[24] US Department of Homeland Security: Strategic principles for securing the internet of things (IoT), 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf (letöltés ideje: 2018. 05. 02.)

[25] ORACEVIC, A. et al.: Security in Internet of Things: A Survey, In.: Proceedings of the International Symposium on Networks, Computers and Communications (ISNCC), Morocco, 2017

[26] MOUAATAMID, EL O. et al.: Internet of Things Security: Layered classification of attacks and possible Countermeasures, E-Ti: Electronic Journal of Information Technology, Issue 9, pp. 66-80. 2016.

[27] ANDREA, I. et al.: Internet of Things: Security vulnerabilities and challenges, In.: Proceedings of the IEEE Symposium on Computers and Communication (ISCC), Cyprus, 2015.

[28] JING, Q. et al.: Security of the Internet of Things: perspectives and challenges, Wireless Networks, Volume 20, Issue 8, pp. 2481–2501, 2014.

[29] WRONA, K.: Securing the Internet of Things A Military Perspective, In: Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015.

[30] DARPA LADS: https://www.darpa.mil/program/leveraging-the-analog-domain-for-security (letöltve: 2018. 05. 02.)

[31] GÁCSER Z.: A katona harci képességét növelő korszerű, hálózatba integrált egyéni felszerelésrendszerének kialakítási lehetőségei a Magyar Honvédségben, Budapest: ZMNE, 2008. (PhD értekezés)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

A NYÍLT FORRÁSÚ INFORMÁCIÓSZERZÉS SZEREPE A KIBERTÁMADÁSOK VÉGREHAJTÁSA SORÁN

THE ROLE OF OPEN SOURCE INTELLIGENCE ON THE IMPLEMENTATION OF CYBER ATTACKS

DEÁK Veronika

(ORCID: 0000-0001-9220-2002)

deak.veronika@uni-nke.hu

Absztrakt

A mindennapi életünk során kulcsfontosságú szerepet töltenek be a különféle adatok, információk, ennek következtében ezek megszerzése és hatékony felhasználása is rendkívül fontos a napi rutin feladataink megoldása és a kibertámadások végrehajtása folyamán egyaránt, ugyanis a megfelelő információk megszerzése éppúgy elengedhetetlen a hétköznapi tevékenységeink elvégzéséhez, mint egy kibertámadás kivitelezéséhez. Az információszerzés a kibertámadások lebonyolításának nélkülözhetetlen eleme, tulajdonképpen az első lépéseként is értelmezhető. Az információszerzés alkalmas a támadás célpontjának megismerésére, ezáltal a különböző sérülékenységek, sebezhetőségek és kockázatok feltárására is, hiszen ezen hiányosságok felfedésével jelentősen növelhető a támadás eredményes végrehajtásának esélye. Továbbá a kibertámadások egyes szakaszainak hatékony megvalósításához számos olyan tervezési, szervezési és végrehajtási tevékenység kapcsolódik, amely során a releváns információk megszerzésével, összegyűjtésével, illetve felhasználásával sokkal eredményesebben, hatékonyabban és gyorsabban kivitelezhető egy ilyen támadás. Jelen tanulmányban áttekintésre kerülnek nyílt forrású információszerzés lehetséges eszközei, formái és a kibertámadásokban betöltött szerepe is.

Kulcsszavak: *nyílt forrású információszerzés, OSINT, kibertámadás, információ*

Abstract

In our daily life, the various data and information play a key role, and as a result, their acquisition and efficient use are crucial to solving our daily routine tasks and during the implementation of cyber attacks, since getting the right information is just as essential to do our everyday activities as to initiate a cyber attack. The acquisition of information is an indispensable element of the implementation of cyber attacks and can be interpreted as its first step. The acquisition of information is a good way to get to know the target of the attack, and to explore the various vulnerabilities and risks, as discovering these shortcomings can significantly increase the chance of a successful attack. In addition, several planning, organizational and enforcement activities are associated with the effective implementation of certain sections of cyber attacks, whereby such an attack can be performed much more efficiently, effectively and faster by acquiring, collecting and using relevant information. This paper reviews the possible tools and forms of open source intelligence and its role played in cyber attacks.

Keywords: *open source intelligence, OSINT, cyber attack, information, cyber defence*

A kézirat benyújtásának dátuma (Date of the submission): 2018.06.01.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.20.

BEVEZETÉS

Napjainkban az információ központi szerepet tölt be életünkben, hiszen jelenleg információs társadalomban élünk, amely azt jelenti, hogy az információ a mindennapi élet alapvető mozgatórugója. Ez a társadalom alapjában véve az információs technológiára épül, működéséhez elengedhetetlenül szükséges ennek megléte. Az általunk felhasznált információk típusainak száma és mennyisége a korábban rendelkezésünkre állókhoz képest a sokszorosára nőtt, tárolásuk pedig igen nagy koncentrációban történik. Az információ a mindennapi tevékenységeink nélkülözhetetlen szereplőjévé vált, többek között jelen van a kommunikációban, a döntéshozatalokban, valamint a különféle folyamatok, eljárások lebonyolításában is. Továbbá a megfelelő információk birtokában a különböző döntések bizonytalansága csökkenthető, ezzel együtt a döntéshozatali folyamat gyorsítható, valamint a többi erőforrás felhasználásának eredményessége és hatékonysága is növelhető, illetve a belső és külső hatásokra való gyors reagálás kulcsfontosságú feltétele. [1] Ezáltal aki a megfelelő információkhoz hozzáfér, óriási előnyhöz juthat. A megfelelő információk megszerzésével információs fölény érhető el, amely lehetővé teszi, hogy a birtoklója az infokommunikációs rendszereit és azok képességeit kihasználva, az élet számos területén előnyre tegyen szert, emellett képes az őt érintő helyzeteket úgy irányítani, hogy ezalatt a másik felet megfossza ezen képességektől. [2]

Az információ értékének növekedésével együtt jár a különböző információk megszerzésére irányuló törekvések megjelenése is, függetlenül attól, hogy az adott információ bizalmasnak tekinthető-e vagy sem. Manapság már mindenkinek lehetősége van a különféle külső, nyílt források segítségével információkat szereznie, amely azonban akár rosszindulatú célra is felhasználhatóak, illetve ezen információk tekintetében a visszaélés lehetősége is fennállhat. Összességében elmondható, hogy a felhasználások céljai nem változtak alapjaikban, viszont tömegessé váltak a különféle információ lopások és az illegális felhasználásuk is. Ennek köszönhetően az információk kezelőinek jelentősen megnövekedett a felelőssége, különösen az állami szerveknél, ahol mind a gazdaság résztvevőiről, mind az állampolgárokról, mind az állami szervekről óriási mennyiségű adat, információ összpontosul.

Az információk számos módon megszerezhetők attól függően, hogy milyen forrásban állnak rendelkezésünkre az adatok. A következőkben a nyílt forrású információszerzés fontossága, céljai, illetve a különféle módszerei, eszközei kerülnek bemutatásra.

A NYÍLT FORRÁSÚ INFORMÁCIÓSZERZÉS

Ahhoz, hogy értelmezni tudjuk az információszerzés célját, egyes módszereit, a megvalósítás lépéseit, illetve ezen módszerek elleni védekezés, vagyis a bizalmas információink védelme érdekében tett intézkedéseket, mindenképpen ismernünk kell az alapvető fogalmakat, jelenségeket.

Az információszerzés típusától függetlenül elsőként azt szükséges tisztázni, hogy mire irányulnak ezen információszerzések, tehát mi a tárgya ennek a tevékenységnek. Ebben az esetben a tevékenység központi célja az adatok, információk gyűjtése, majd pedig saját célra történő felhasználása. Az adat az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas. [3] Az információ értelmezésére számtalan definíció létezik, nincs egységes meghatározása. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény szerint az információ bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott tapasztalat, megfigyelés, vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét átalakítja, megváltoztatja, illetve befolyásolja, továbbá bizonytalanságát csökkenti vagy megszünteti.[3] Egy másik definíció szerint az információ olyan új ismeret, adat, tény, amelynek megismerésekor olyan plusz tudásra teszünk szert, amely addig nem volt a birtokunkban.[4]

A következő fontos fogalom a nyílt forrás (Open Source), hiszen ez fejezi ki az információk származásának eredetét. A nyílt forrás magába foglalja azokat a nyilvánosan elérhető forrásokat, amelyekhez legálisan, törvényes eszközökkel hozzáférhetünk, például megfigyelés, előfizetés, személyes megkeresés, megvásárlás, lekérdezés, internetes keresés által. Ilyen forrásnak tekinthetők a bárki által szabadon elérhető információ-hordozók, például a hagyományos publikált anyagok, könyvek, tanulmánykötetek, napilapok, folyóiratok, fényképek, rádió-és televízióadások, médiahírek, konferenciák, személyek beszámolói, illetve az Internet és egyéb digitális tartalmak is. A nyílt források tárháza igen sokrétű, de napjainkban az Internet robbanásszerű és folyamatos fejlődésének és számtalan előnyének köszönhetően a legtöbb információszerzés az Interneten keresztül valósul meg. [5:13]

Nyílt forrású információnak (Open Source Information) minősülnek mindazon adatok, amelyek az előbb említett források segítségével megszerezhetők, elérhetők. Ilyen információnak tekinthető a még nem feldolgozott, nyomtatott, kisugárzott, szóban közölt, digitális vagy más formájú dokumentum, tény, ismeret, fogalom, meghatározás, tájékoztatás, amelyek a nyílt források által biztosítottak. [5:13]

A nyílt forrású információszerzés (Open Source Intelligence – OSINT) definícióját hazánkban először a hírszerzés és a katonai felderítéstől elkülönítve Lévay Gábor határozta meg, mely definíció szerint az „*OSINT katonai felderítés és a hírszerzés rendszerén kívül létező, a publikum (tehát minden egyén) számára nyilvánosan, legális eszközökkel megszerezhető, vagy korlátozott körben terjesztett, de nem minősített adatok szakmai szempontok alapján történő felkutatását, gyűjtését, szelektálását, elemzését-értékelését és felhasználását jelenti*.” [6]

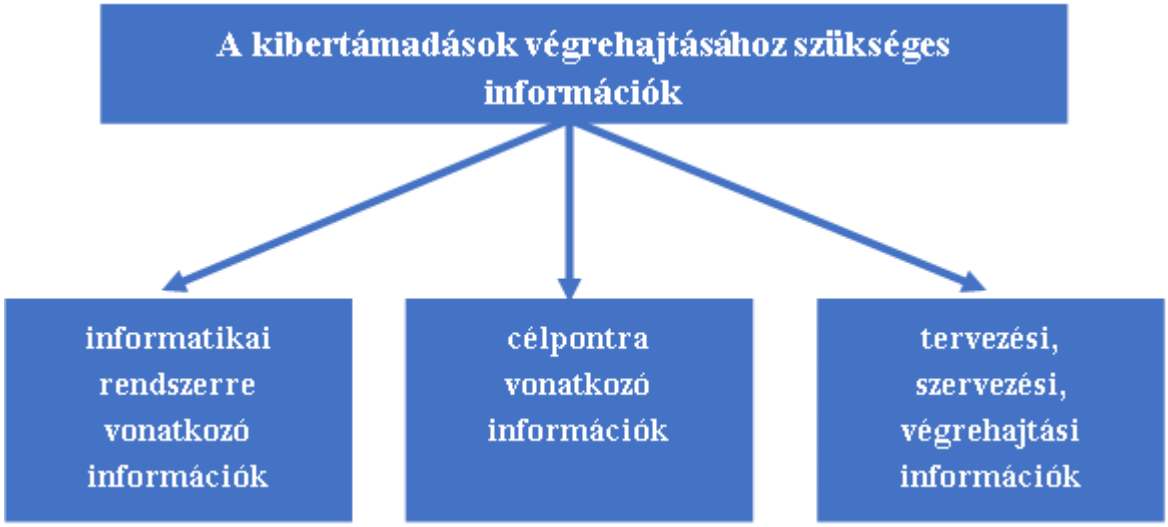
Összegezve tehát az OSINT olyan információgyűjtő eljárás, mely során az információk megszerzése bárki által szabadon hozzáférhető forrásokból történik. Napjainkban az OSINT széles körben elterjedt, gyakran alkalmazzák a mindennapi élet és a kibertámadások előkészítése és végrehajtása során is, azt azonban mindenképp ki kell emelni, hogy ezen módszer segítségével rengeteg információ megszerezhető, így az esetek jelentős részében nem elég csak összegyűjteni az információkat, ezt követően szűrni, szelektálni, rendszerezni, elemezni és értékelni is kell a felhasználás előtt. [7]

A nyílt forrású információszerzés elsődleges célja, hogy a felhasználó információigényeire minél pontosabb teljesebb, hitelesebb választ, visszajelzést tudjon biztosítani. Továbbá, hogy a felhasználó szándékának megfelelő információt szolgáltasson, függetlenül attól, hogy a felhasználó mire használja azt a továbbiakban. A felhasználók céljai sokfélék lehetnek, többek között az információszerzést felhasználhatják tájékoztatásra, döntéselőkésítésre, döntéshozatalra, üzleti célok megvalósítására, terrorcselekmények eredményes megvalósítására, vagy akár a kibertámadások előkészítésére és megvalósítására. [8] Jelen tanulmányban a nyílt forrású információszerzés kibertámadások végrehajtásában betöltött szerepe kerül bemutatásra.

A KIBERTÁMADÁSOK VÉGREHAJTÁSÁHOZ SZÜKSÉGES INFORMÁCIÓK

A kibertámadások nélkülözhetetlen elemeként értelmezhető az információszerzés, hiszen minden támadás alapja a támadás sikeres végrehajtásához szükséges információk megszerzése. Az, hogy pontosan milyen információk megszerzése a cél, az attól is függhet, hogy mi a konkrét támadás motivációja. Egy kibertámadás céljai igen sokrétűek lehetnek, többek között irányulhatnak információk gyűjtésére, módosítására, megváltoztatására, zárolására, törlésére, illetve megsemmisítésére, szolgáltatás, infrastruktúra akadályozására, korlátozására, gazdasági, politikai előny szerzésére, álhírek terjesztésére, hírnévrontásra, károkozásra, bizalomvesztés generálására, vagy akár vallási célok elérésére is. A kibertámadások során az információszerzés célja olyan információk gyűjtése, amelyek biztosítják a támadás céljától függően a sebezhetőségek, kockázatok és sérülékenységek feltárását. Egy kibertámadás alapjául szolgáló információszerzés alapvetően az alábbi ábrán látható információkat célozza. Az információszerzés irányulhat az informatikai rendszerre vonatkozó jellemzőkre és a célpontra vonatkozó információkra,

amelyek kapcsán elsődlegesen a sebezhetőségek, gyenge pontok feltárása a cél, majd ezek alapján következhet a tervezési, szervezési és végrehajtási információk összegyűjtése, rendszerezése.



1.ábra A kibertámadások végrehajtásához szükséges információk
(Saját szerkesztés)

Az *informatikai rendszerre vonatkozó információk* tartalmazzák az adott rendszer felépítésére, működésére vonatkozó adatokat, és a rendszerhez csatlakozó eszközök jellemzőit. Ezen információk megszerzése azért fontos, mert, ha a támadónak sikerül azonosítania az informatikai rendszer vagy az infokommunikációs eszközök sebezhetőségeit, akkor az információk segítségével meghatározható, hogy a rendszer mely pontján kell megvalósítani a támadást a sikeres végrehajtás érdekében. Nem létezik tökéletes biztonság, naponta jelennek meg újabb és újabb támadási módszerek, biztonsági rések, ennek következtében minden kockázatra kiterjedő védelemről sem beszélhetünk. Éppen ezért a technológiai sérülékenységek feltárása minden esetben kulcsfontosságú, hiszen ezek segítségével azonosíthatók az információs rendszerek vagy azok elemeinek gyenge pontjai, és ezáltal a sebezhetőségek orvoslása is időben elkezdődhet. Egy informatikai rendszer esetében kockázatnak tekinthetők többek között a különféle biztonsági rések, lehetséges szoftverhibák, hibás beállítások, gyenge jelszavak, a különböző szintű jogosultságok beállításának a hiánya, illetve hibás hozzáférési szintek megállapítása, a titkosítás hiánya vagy hibája, alkalmazás szintű hibák, mint például a hitelesítési, logikai hibák vagy akár az alkalmazások frissítéseinek elmulasztása. [9] Ezek alapján a fentebb példaként említett sebezhetőségekre és számos további, az informatikai rendszer gyenge pontjaira vonatkozó információk sorolhatók ebbe a csoportba.

A *célpontra vonatkozó információknak* két típusát különböztethetjük meg. Az egyik csoportba tartoznak azok az adatok, amelyek egy *szervezetre jellemzőek*, míg a másik csoportot a személyre utaló információk alkotják. A szervezettel kapcsolatos adatok magukba foglalják a szervezet tevékenységével, munkavállalóival, struktúrájával, illetve elérhetőségeivel kapcsolatos adatokat, amelyek tökéletes kiindulási alapot jelenthetnek a támadó számára a megfelelő személy kiválasztásához, aki rendelkezik a számára szükséges információkkal, vagy esetleg, akit megszemélyesíthet a későbbiekben további információk gyűjtéséhez vagy a konkrét támadás végrehajtásához. A szervezetre utaló információk kapcsán mindenképpen szükséges kitérni a szervezet fizikai jellemzőivel, védelmével összefüggő ismeretek megszerzésére is. Ennek során az információszerzés irányulhat például a szervezet belépési biztonságára, illetve arra, ho-

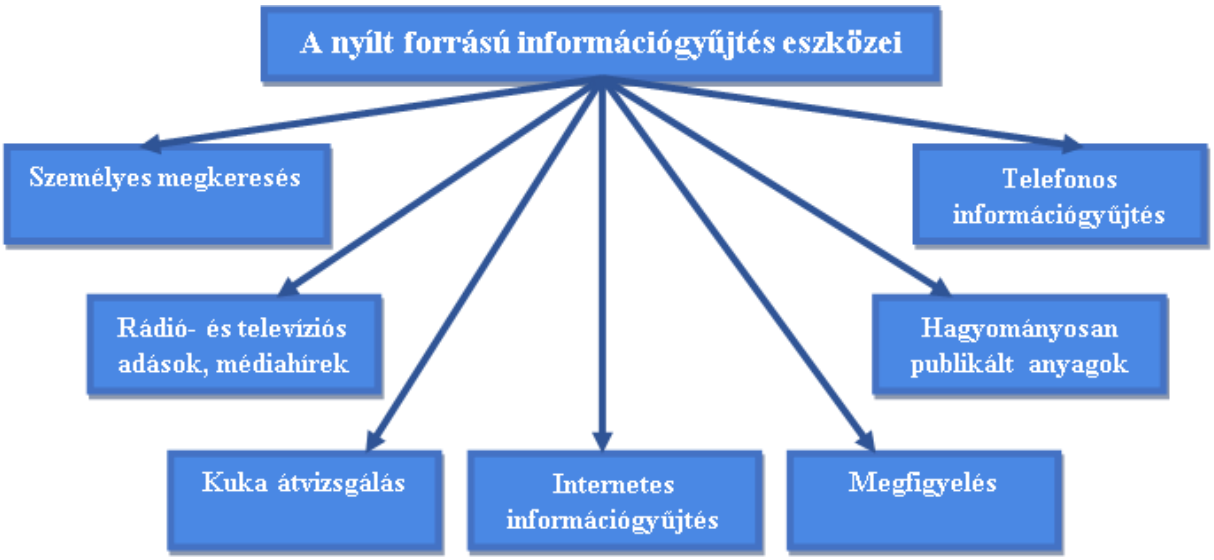
gyan történik a belépési jogosultságok ellenőrzése, milyen beléptető rendszer van a szervezetben, milyen szinten történik a szervezet épületeibe való bejutás ellenőrzése, illetve arra, hogy figyelik-e a szervezet alkalmazottainak indokolatlan bent tartózkodását, valamint, hogyan történik a szervezeten kívüli személyek beléptetése.

A *személyre utaló információk* megszerzése elősegíti a tökéletes célpont kiválasztását, aki a későbbiekben a támadó segítségére lesz a támadás megvalósításában. Ezen információk megszerzése során kerül sor a felhasználók biztonságtudatosságának felmérése, vagyis annak vizsgálatára, hogy mely alkalmazott nem rendelkezik megfelelő szintű információbiztonsági tudással és ezáltal mely munkavállaló segítségével szerezhetők meg a szervezetre vagy az informatikai rendszerre vonatkozó adatok, vagy mely célszemély alkalmas például egy kártékony program aktiválására, működésbe hozatalára. Ezen információk megszerzése során egyfajta profilozás is történik, hiszen az információk megszerzését követően a támadó célja, hogy az összegyűjtött ismeretekből következtetéseket vonjon le a célszemély gyenge pontjait illetően. A gyengeségek azonosítása azért rendkívül fontos, mert ezen ismeretek tudatában megtalálható az a személy, aki a kibertámadás megvalósításában a támadó segítségére lehet, vagy akitől bizalmas információkat lehet megszerezni. Ennek kapcsán az információszerzés kiterjed a célszemély személyes tulajdonságaira, amelyek a támadó által könnyedén kihasználhatók. Ilyen tulajdonságok többek között segítőkészség, naivitás, kíváncsiság, nyitottság, befolyásolhatóság, fáradtság vagy túlterheltség. Vannak olyan jellemzők is, amelyek jelentősen kapcsolódnak az áldozat munkahelyéhez is, ettől függ kialakulásuk, ilyen például, hogy ha valaki napi rutin munkát végez, minden nap ugyanolyan típusú problémát old meg, akkor sokkal nehezebb tesz különbség egy napi rutin feladat és a támadó kérése között. [10: 18-21] Ilyen tulajdonságnak tekinthető még az elégedetlenség, a lefizethetőség vagy például a megzsarolhatóság is, hiszen, ha a munkavállaló nem elégedett a munkájával, (esetleg a munkakörnyezetével, megbecsülésével vagy például a fizetésével) akkor a támadó akár megvesztegetheti vagy befolyásolhatja is az áldozatát, további információk kiadása érdekében. A támadó számára az is előnyös lehet, ha a kiszemelt áldozata szabadságon vagy betegállományban van, hisz ilyenkor a helyettesítő kollégának azt is mondhatja, hogy a betegállományban vagy szabadságon lévő személy ígérte meg neki bizonyos információk kiadását, így, ha a helyettesítő munkavállaló nem ellenőrzi ezt le, a támadó számos értékes információkkal gazdagodhat. Vannak olyan esetek, amikor az felhasználó szakképzetlenségét, jelszóhasználatát, a biztonságtudatosságának hiányát vagy a hanyagságát, illetve az ezekből adódó mulasztásokat használja ki a támadó, éppen ezért az információszerzésnek erre mindenképpen ki kell terjednie. [11]

A célinformációk harmadik nagy csoportját a *tervezési, szervezési, végrehajtási információk* alkotják. Ezen információk magukba foglalják a konkrét támadás kivitelezéséhez szükséges technikai, személyi, tárgyi és pénzügyi feltételeire vonatkozó ismereteket. Ezek egy része külön információszerző tevékenységet igényel, míg másik része a már korábban megszerzett másik két célinformáció csoport alapján kerül meghatározásra. A támadás végrehajtásához szükséges technikai feltételek tartalmazzák az infrastruktúra meglétét, többek között a különféle hálózati eszközöket (router, tűzfal), vezeték nélküli hálózatokat, VPN-t és az energiát is. A személyi feltétel magába foglalja a támadás megvalósításának egyik elengedhetetlen feltételét, vagyis azt a személyt, aki a magas szintű technikai tudásának köszönhetően képes végrehajtani az adott támadást. A tárgyi feltételek a támadás kivitelezéséhez szükséges eszközöket, berendezéseket, szervereket és szoftvereket jelentik. A pénzügyi feltételek az előbb említettek beszerzéséhez, megszervezéséhez szükséges anyagi forrásokat jelölik. Ezen információk megszerzését követően lehet összeállítani a támadás konkrét végrehajtási tervét, amely az előbbiek alapján tartalmazza a támadást kivitelezők körét, az ehhez szükséges technikai, infrastrukturális, tárgyi, pénzügyi feltételeket, a támadás konkrét időpontját, helyét, cselekvési tervét és a támadás konkrét célját.

A NYÍLT FORRÁSÚ INFORMÁCIÓSZERZÉS MÓDJAI, ESZKÖZEI A KIBERTÁMADÁSOK ELŐKÉSZÍTÉSÉBEN

Az információszerzés céljainak ismertetését követően mindenképpen ki kell térni, hogy mely eszközökkel, milyen módszerek segítségével valósítható meg a különféle információk megszerzése. Az alábbiakban az OSINT gyakran alkalmazott módszerei, eszközei kerülnek bemutatásra. A következő ábra a nyílt forrású információszerzés általam vizsgált egyes eszközeit mutatja, a teljesség igénye nélkül, hiszen ezeken kívül számos további módszer alkalmazható.



2.ábra A nyílt forrású információgyűjtés egyes eszközei
(Saját szerkesztés)

Napjainkban a technológia rohamos fejlődésének és az internetszolgáltatás elterjedésének köszönhetően az esetek döntő többségében az Internet segítségével valósítják meg az információszerzést. Ennek oka, hogy rövid idő alatt nagy mennyiségű információ gyűjthető kevés erőforrás felhasználásával, költséghatékonyan. A technikák első nagy csoportja alapvetően az *Internet* nyújtotta lehetőségeket kihasználva teszik lehetővé az adatok gyűjtését.

Az Internet adta lehetőségeknek köszönhetően az egyik legelterjedtebb információszerző és gyűjtő módszer az *internetes keresőrendszerek* alkalmazása. A keresőrendszerek olyan offline vagy online szoftverek, amelyek képesek a különféle adatok, információk találati listáját megjeleníteni a felhasználók számára. A konkrét keresés során különböző tartalmak többek között weboldalak, képek, videók, különféle fájltípusok, adatbázisok és számos további a támadó számára hasznos tartalom jeleníthető meg. A keresőrendszerek egyik típusát a webes keresőszolgáltatások alkotják, a másik csoportba pedig az emberi erőforrás által épített adatbázisok sorolhatók. [12]

Az emberi erőforrás által épített adatbázisok lényege, hogy az emberi tényező segítségével készül el az adatgyűjtemény, így, ha valamilyen változás következik be az adatok tekintetében, akkor azt manuálisan kell felvezetni. Annak ellenére, hogy ez a típus nem minden esetben tekinthető a legnaprakészebb forrásnak, mégis sokszor előfordul, hogy a támadók ezek segítségével gyűjtenek információt. Ilyen adatállományoknak tekinthetők az anyakönyvi, céginformációs vagy akár a telefonszámokat, elérhetőségeket tartalmazó adatbázisok. [12]

A webes keresőszolgáltatás működése három nélkülözhetetlen elemből áll. Az első lépésben a keresőmotor a webpásztázás során összegyűjti az adatokat a weboldalak tartalmáról a weboldalakon található hivatkozásokon keresztül, majd az így összegyűjtött tartalmat a következő lépésben az indexelés folyamatában elemzi és rendszerezi. A már korábban begyűjtött tartal-

makat metaadatokkal látja el, majd egy indextáblát készít, amely segítségével a keresési kritériumok ismeretében gyorsan elkészíthető a hatékony találati lista. A harmadik lépés a keresés, amely megvalósulhat a felhasználó, de akár egy program kérésére is. Ekkor az indexlistából a felhasználó által beírt vagy más programtól kapott kulcsszóhoz, illetve keresőkifejezéshez tartozó weboldalak rekordjainak kikeresése történik. [13: 39] Webes keresőszolgáltatásnak tekinthető a Bing, a Google, a Search vagy akár a Yahoo! is.

Napjaink legnépszerűbb és leggyakrabban alkalmazott keresőszolgáltatása a *Google* világszerte. A Google operátoraival történő keresést Google Hackingnek is nevezik, hiszen segítségével olyan részletes keresésre van lehetőség, amellyel akár a véletlenül nyilvánosságra hozott információk is felkutathatók, és amelyek a támadók számára hasznos információkat szolgáltathatnak. Többféle információt is találhatunk ezzel a technikával a jelszavaktól (felhasználók jelszavai, adminisztrátor jelszavak, alapértelmezett jelszavak) kezdve, elérhetőségeken, a belső használatra szánt anyagokon át, egészen a címlistákig szinte bármit. [13: 56-57] Ezen kívül a Google keresés során számos esetben tártak fel személyes adatokat (személyazonosításra alkalmas információk, bankszámlaszám, cím, telefonszám), e-mail címeket, felhasználóneveket, és a hozzá tartozó jelszavakat, hálózati adatokat, korábbi információbiztonsági auditok jegyzőkönyveit, illetve belsős anyagokat is. Továbbá a Google segítségével személyre szabott keresést valósíthatunk meg, rákereshetünk akár különféle fájltípusokra, képekre, videókra, könyvekre, illetve kereshetünk egy konkrét szövegben, címben vagy URL címben is. A Google Hacking Database egy hackerek által alkalmazott lekérdezéses adatbázis, aminek segítségével információk nyerhetők ki weboldalakról (hálózatbiztonsági információk, bejelentkezési oldalak stb.). Ez az adatbázis az internet segítségével valamilyen módon nyilvánosságra hozott, kiszivárgott, ezáltal a Google által is elérhető információkat, keresési kifejezéseket tartalmazza, a korábban indított lekérdezések katalogizálása által. [14]

A *Google* kapcsán mindenképp meg kell említeni a Street View, vagyis *Utcakép* funkcióját [15], amelynek lényege, hogy a 360 fokos panorámaképek segítségével egyfajta virtuális valóságként magunk előtt láthatjuk a keresett helyet. Ez rendkívül hasznos a támadó számára, mert a vizuális tartalomnak köszönhetően teljesen pontos és aprólékosan kidolgozott képet kaphat például a célszemély tartózkodási helyéről vagy éppen a támadás céljaként szolgáló szervezet fizikai adottságairól. Természetesen ezek a képek nem minden esetben szolgáltatnak naprakész információt, de kiindulási alapként tökéletesen alkalmazhatóak.

Az internetes keresőrendszerekkel kapcsolatban mindenképpen érdemes kiemelni azon keresőket, amelyek *konkrét személy megtalálására is alkalmasak*. Ezen keresők lehetőséget biztosítanak arra, hogy a legkülönfélébb variációkra, mint például vezetéknév, keresztnév, becenév, felhasználónév vagy akár ezek rövidített változatára is rákeressünk. Erre tökéletes példaként szolgálhat a Spokeo, [16] amely olyan kereső szolgáltatás, mely a nyilvános adatbázisok, nyilvántartások, közösségi hálózatok segítségével képes a célszemélyre vonatkozóan információ szolgáltatására. A Spokeo weboldalán történő kereséssel számos hasznos információhoz juthat a támadó a célszeméllyel kapcsolatban, így információt szerezhet a személy címéről, (amelyet egy Google térkép segítségével szemléltetnek) telefonszámáról, koráról, neméről, vallási, politikai meggyőződéséről, családtagokról, az elvégzett képzésekről és számos további személyes jellemzőiről. A Spokeo egyelőre még csak az Egyesült Államokban élő személyek keresésére alkalmas, de előfordulhat, hogy a világ többi részén is elérhetővé válik majd. Ezen kívül konkrét személyek megtalálására is használhatók a különféle közösségi oldalak (pl. Facebook, LinkedIn, Twitter stb.) és internetes keresőrendszerek (pl. Google).

Az Internet alapú információszerzés következő típusát a *közösségi oldalak* alkotják. A népszerűbb közösségi oldalak kitűnő kiindulópontot jelenthetnek, hiszen a kiszemelt áldozatról számos személyes információ begyűjthető. [17] A közösségi hálózatok általi információszerzés különösképp kedvező a támadó számára, hisz ezek segítségével kis költséggel nagy mennyi-

ségű információ szerezhető meg. Éppen ezért és az egyre növekvő alkalmazási kör miatt tökéletes kiindulási alapként szolgálnak egy kibertámadás előkészítéséhez vagy akár megvalósításához is. A támadó nem csak a célszemély személyes adatait és elérhetőségeit (e-mail cím, esetleg telefonszám, lakhely), hanem számos egyéb információt is megszerezhet. Gondoljunk csak arra, hogy első kézből láthatja az ismerőinek, családtagjainak, barátainak nevét, akik nevében egy kártékony programmal megfertőzött üzenetet is küldhet. Sokan megjelenítik a születési dátumukat, és gyakran posztolnak a családtagjaikról, kedvenc háziállatukról, amelyek akár az áldozat jelszavára is utalhatnak. Vannak, akik feltüntetik érdeklődési körüket és szabadidős tevékenységeiket is, így a támadó ennek birtokában tudja, hogy milyen tartalmú veszélyes csatolmánnyal ellátott üzenet küldjön, vagy esetleg a kapcsolatteremtés fázisába hogyan építse ezt be, mint például közös érdeklődési kört. Fontos megemlíteni azt is, hogy a közösségi portálok nem csak az információgyűjtésre alkalmasak, hanem kártékony program csatolására, például egy üzenetben elküldött link vagy fájl formájában, amire, ha rákattint a felhasználó, már aktiválódik is a kártékony program. Sok esetben még a célszemély pontos tartózkodási helye is fellelhető a közösségi oldalakon. Ezen kívül számos információ megszerezhető a leendő áldozat munkahelyi helyzetéről, politikai nézetéről, vallási meggyőződéséről, de akár a családi, párkapcsolati életére vonatkozóan is. A közösségi oldalak további előnye, hogy ha a támadónak nem sikerül hozzáférnie a célszemély biztonsági beállításainak köszönhetően adatlapjához, profilinformációkhoz akkor számos további lehetősége akad, akár információk gyűjtésére, de akár a kapcsolat kiépítésére és fenntartására is, hiszen profil létrehozásával rendelkezésére állnak a különféle fórumok, csoportok és a közvetlen üzenetváltás lehetősége is.

A közösségi oldalak kapcsán mindenképpen érdemes megemlíteni a különféle *párkereső oldalakat* és *alkalmazásokat* is. Ezen felületek is rendkívül sok személyes információt tartalmazhatnak a célszemélyről, a személyes adatoktól kezdve, az érdeklődési körön át, egészen a tartózkodási helyig számos a támadó számára hasznos információ fellelhető ezek segítségével.

Az internet alapú információszerzés további eszköze a *geolokációs helymeghatározást megvalósító applikációk*. Ilyen például a Creepy [7] alkalmazás, amely a földrajzi helyhez kapcsolódó információkat (időpont, hely) gyűjti online forrásokból, a közösségi médiában megjelenő bejegyzésekből, illetve képes azonosítani egy meghatározott IP cím fizikai tartózkodási helyét is. Ez lehetővé teszi meghatározott személyek mozgásának nyomon követését, és további következtetések levonását is, mint például a saját, a család, barátok lakhelyére vonatkozóan. Sok esetben mikor egy közösségi oldalt használunk és különféle bejegyzéseket, képeket, videókat osztunk meg, nem csak az előbb említett tartalmak kerülnek megosztásra, hanem ezzel együtt például a bejegyzés vagy kép készítésének konkrét helye is. A Creepy pontosan ezeket az információkat gyűjti össze és jeleníti meg egy térképen. Az alkalmazás információ szolgáltatásához használja többek között a Twitter, Instagram és a Flickr közösségi platformokat.

A kiszemelt áldozat megismerésének egyik legnyilvánvalóbb módszere az adott *szervezet/cég honlapjának* megtekintése, hiszen manapság már a legtöbb nagyvállalat, állami és nem állami szervek egyaránt rendelkeznek szervezeti weboldallal, amely nem csak a fő profiljuk, tevékenységük bemutatására alkalmas, hanem az ügyfelekkel való kapcsolattartásra is használható. A vállalati weboldalra gyakran kerülnek fel információk a vezetőkről, az alkalmazottakról, sok esetben még e-mail címekkel és telefonszámokkal együtt. Sőt, az is előfordulhat, hogy belső szervezeti ábra vagy telefonkönyv is elérhető a holnapon, ami jelentősen megkönnyíti a támadó számára a megfelelő személy kiválasztását, aki rendelkezik a számára szükséges információkkal, vagy esetleg, akit megszemélyesíthet. Abban az esetben, ha az e-mail címeket is feltüntették az oldalán, akkor akár egy veszélyes mellékletet tartalmazó levelet is küldhet a támadó. [17]

A következő csoportot az *elektronikus levelezés* általi információgyűjtés alkotja. Napjainkra az e-mail az egyik legelterjedtebb kommunikációs formává vált, amelyet az üzleti életben és a saját személyes ügyeink intézésére egyaránt használunk, hiszen leegyszerűsíti az üzenetküldést,

sokkal gyorsabb, költséghatékonyabb szolgáltatást valósít meg, továbbá már nem csak szöveget és képeket küldhetünk, mint a hagyományos levelezés során, hanem elektronikus dokumentumokat, fájlokat is. Az email-en keresztül történő megkeresés során általában a támadó valamilyen kérdőívet töltet ki, amelynek kérdései közé belecsempészi a számára szükséges információra irányuló kérdéseket. A kérdőívezés során a támadó elsősorban a személyes adatokra, születési dátumra, érdeklődési körre kérdez rá. [17]

A fentebb nevesített módszerek mindenféle informatikai, technikai tudás nélkül bárki által szabadon alkalmazhatók, de ezek mellett elérhetőek ingyenes információszerző szoftverek és programok, weboldalak, amelyek segítségével rengeteg olyan további információ gyűjthető, amely a támadás során felhasználható. Ilyen például a Shodan, amely az Internetre kötött infokommunikációs eszközök keresőszolgáltatása. A Sodan keresőmotort úgy tervezték, hogy képes legyen feltérképezni az Internetet, továbbá megpróbálja azonosítani és indexelni az Internetre kapcsolt eszközöket. A kereső lehetővé teszi a felhasználók számára, hogy különböző szűrőket alkalmazva feltárják az Internethez csatlakozó eszközöket (pl. számítógépeket, okostelefonokat, tableteket, szervereket, webkamerákat és azok videóit stb.), illetve még akár azok tartalmát, részletes adatait, sebezhetőségeit is. A Shodan nem csak a mindennapjaink során alkalmazott infokommunikációs eszközök tartalmához fér hozzá, hanem még akár az Internetre csatlakozott ipari vezérlőeszközökéhez is, amely ezáltal rendkívül nagy biztonsági kockázatként is értelmezhető. [18] Egy másik eszköz a theHarvester[7], amely segítségével e-mail fiókok, aldomain nevek, hosztok nyitott portok, bannerek és számos további az informatikai rendszerre vonatkozó információ gyűjthető. Ezen információkat különféle keresőmotorok, (Google, Bing) és más webhelyek, mint például a közösségi oldalak (LinkedIn) segítségével szerzi meg. A fentebb említett alkalmazásokon, szoftvereken kívül rengeteg más ingyenes elérhető program alkalmazható nyílt forrású információszerzésre.

Az Internet alapú OSINT-en kívül az egyik leghatásosabb, de egyben a legveszélyesebb módszer az áldozat *személyes megkeresése*, ugyanis ekkor a legmagasabb a lebukás kockázatának veszélye. Az áldozat közelébe férkőzve számos fontos információt megtudhat a támadó, mint például egy irodai körbenézés során, amikor is a különböző időbeosztások, szervezeti ábrák, szabadságolások, helyettesítések, számlák, infokommunikációs eszközök vagy esetleg a kiragasztott jelszavak is elérhetővé válnak a támadó számára. [10:57] Ezen kívül számos további a szervezet informatikai rendszerére, védelmére és tevékenységére vonatkozó belső és bizalmas információ is megtudható egy személyes beszélgetés által.

A személyes megkereséshez hasonló módszer a *megfigyelés*, amely esetén azonban nem történik meg a kapcsolatfelvétel, ehelyett a célszemély, célpont, vagy akár a szervezet fizikai megfigyelése valósul meg. Ennek előnye, hogy a személyes interakció hiányában a lebukás veszélye is kisebb, emellett rengeteg információ megszerezhető ezáltal. A megfigyelés segítségével információ gyűjthető a célszemély szokásairól, tartózkodási helyéről, szabadidős tevékenységeiről és a munkahelyi tevékenységére vonatkozóan is következtetések vonhatók le. A megfigyelés során a szervezet fizikai jellemzőivel, védelmével kapcsolatos információk is gyűjthetők, például hogyan történik a belépési jogosultságok ellenőrzése, illetve milyen beléptető rendszer van a szervezetben.

Igaz, hogy az Interneten keresztül manapság már szinte minden információt megtalálunk, azonban, ha ez mégsem lenne elegendő, akkor további információkat gyűjthetünk a *telefonos megkeresés* [10: 57] segítségével. Ebben a módszerben a támadó kiadhatja magát ügyfélnek, új munkatársnak, belső munkatársnak vagy egy partner szervezet/cég munkatársának, de akár egy felsőbb vezetőnek is. Az, hogy a támadó kinek a bőrébe bújik, az attól függ, hogy milyen információt akar megszerezni. Sok esetben a támadó célja az adott területen illetékes munkatársak nevükről, elérhetőségükről, hatáskörükről való tájékozódás, de a telefonos segítség kérése vagy az informatikai rendszer védelmének feltérképezése is lehet a cél.

Az információszerzés egy további hatékony módja *kuka átvizsgáló technika*, amelynek keretében számos hasznos információt tudhatunk meg az áldozatról. Az emberek bele se gondolnak, hogy milyen értékes információkat tudhat meg rólunk a támadó az irodai vagy otthoni szemetesünk átvizsgálásával. [10:37-38] Elég csak kidobni egy hivatalos levelet, bankszámla részletezőt, a támadó már tudomást is szerzett a személyes adatainkról, címünkről. De elég, ha csak a jelszavas cetli belekerül a kukába, és máris tudják a belépésünk adatait. Ezeken kívül számtalan olyan egyéb információt kidobhatunk, amelyek a támadónak segítséget nyújt például a személyiségünk ellopásához, vagy kényes információk esetében a zsaroláshoz is.

További információkhoz juthat a támadó a *leselejtezett informatikai eszközök átvizsgálásával* is. Napjainkra már számos olyan szoftver elérhető, amely segítségével a törölt adatok, információk, fájlok könnyedén visszaállíthatók.

Az Internet előnyeinek köszönhetően a nyílt forrású információszerzés az esetek döntő többségében ezen a felületen zajlik, de a *hagyományosan publikált anyagok* (könyvek, tanulmánykötetek, napilapok, folyóiratok) vagy például a *rádió-és televízióadások, médiahírek* segítségével is gyűjthetők hasznos információk, azonban napjainkban egyre kevésbé fordul elő alkalmazásuk. [7]

Az információszerzés lehetőségei rendkívül sokrétűek, azonban az igazán nagy veszélyt az jelenti, hogy a különböző helyről különböző módon összegyűjtött információkat összekapcsolják, és ezt használják a célpont ellen.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Az sebezhetőségek, sérülékenységek feltárása azért kiemelkedő jelentőségű, mert ennek tudatában a támadó fel tudja mérni, hogy a támadást pontosan hol kell végrehajtani. Abban az esetben, ha az információszerzés során sikerül feltárni a célpont sebezhetőségét, például az informatikai rendszerében vagy akár a szervezet egy alkalmazottjában, akkor a támadó egy sokkal személyre/szervezetre szabottabb támadást tud megvalósítani. A mai modern világunkban a különböző informatikai eszközök és rendszerek védelme már nagyon fejlett, így a támadó, ha például nem talál sebezhetőséget a felsőbb szinteken, mindig egy szinttel lejjebb fog menni, és addig csinálja ezt, amíg nem talál egy olyan pontot, ami sebezhető. Így például, ha a célpont informatikai eszközei és rendszerei magas szintű védelemmel vannak ellátva, akkor a támadó egy szinttel lejjebb, a szervezet alkalmazottai között keres sebezhetőséget. Ez azt jelenti, hogy ebben az esetben a támadó olyan munkavállalót keres, aki segítségével könnyedén bejuthat a szervezet rendszereibe, hálózataiba, információt szerezhet a szervezet sérülékenységeiről vagy akár, ha a támadás egy konkrét információ megszerzésére irányul, akkor ennek megszerzése is megvalósulhat az alkalmazott megtévesztésével, kihasználásával. Azokat a támadásokat, amelyek az emberi tényező kihasználásra, megtévesztésére irányulnak, social engineeringnek hívjuk. A social engineer a manipulálás, a befolyásolás, a megtévesztés és a meggyőzés segítségével irányítja áldozatát a céljai elérése érdekében. A támadások céljai igen sokrétűek, irányulhatnak többek között bizalmas információk megszerzésére, módosítására, illetve törlésére, a sérülékenységek és sebezhetőségek feltárására, a célszemély viselkedésének befolyásolására, a belső hálózati hozzáférés, jogosultság megszerzésére, különféle infokommunikációs eszközök rosszindulatú programmal történő megfertőzésére vagy akár egy komplex kibertámadás előkészítésére egyaránt. Éppen ezért a social engineering támadási technikák tökéletesen alkalmazhatók a kibertámadások végrehajtását megelőző információszerzésre.

A különféle infokommunikációs eszközök használata mindennapos tevékenységeink nélkülözhetetlen részévé vált, számtalan előnye mellett azonban a hátrányait és a hozzájuk kapcsolódó veszélyeket is szükséges megismerni. Elengedhetetlen, hogy mindennapjaink során megvédjük az információinkat a jogtalan hozzáféréstől, illetve az esetleges kiszivárgástól vagy megsemmisítéstől. Ahhoz pedig, hogy ez a védelem sikeres lehessen, úgy gondolom fontos, hogy mindenki megismerje az információk megszerzésére irányuló módszereket, hiszen csak

ezek tudatában lehet meghatározni, hogyan tudjuk megelőzni, megakadályozni a bizalmas információinkhoz való jogosulatlan hozzáférést, illetve hogyan kell reagálnunk, a már bekövetkezett eseményekre.

FELHASZNÁLT IRODALOM

[1] BOGNÁR L.: *Az információ fontossága, az információs rendszerek*. 2015. http://slideplayer.hu/slide/2117606/ (A letöltés ideje: 2018.04.02.)

[2] HAIG Zs., KOVÁCS L.: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* 2012. http://hdl.handle.net/11410/285 (A letöltés ideje: 2018. 04. 02.)

[3] 2013. évi L. törvény *az állami és önkormányzati szervek elektronikus információbiztonságáról.*

[4] KRASZNAY Cs.: *Az információbiztonság alapjai*. 2007. http://krasznay.hu/presentation/elte_01.ppt (2018.04.02.)

[5] FERENCZY G. Z.: *Internet alapú nyílt információszerzés elvi rendszertechnikai megvalósítása.* 2007. http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2007/ferenczy_gabor.pdf (A letöltés ideje: 2018.04.02.)

[6] LÉVAY G.: *OSINT (Open Source Intelligence) – Nyílt információs hírszerzés*. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2006.

[7] CHAUHAN, S., PANDA, N. K.: *Hacking Web Intelligence*. Open Source Intelligence and Web Reconnaissance Concepts and Techniques. 2015. https://doi.org/10.1016/B978-0-12-801867-5.00006-9 (A letöltés ideje: 2018. 05. 21.)

[8] KOBOLKA I. (szerk.): *Nemzetbiztonsági alapismeretek*. Budapest: Nemzeti Közszolgálati Egyetem, 2013.

[9] DOLÁNSZKY Gy.: *Informatikai rendszerek sérülékenységvizsgálata*. 2013. http://users.nik.uni-obuda.hu/poserne/ibst/Frissitett_anyagok_2013/20130508_Serulekenysegvizsgalat_eSec_KURT_DGY.pdf (A letöltés ideje: 2018. 04.17.)

[10] OROSZI E.: *Social Engineering*. Budapest: Budapesti Corvinus Egyetem, 2008.

[11] DEÁK V.: *A social engineering humán alapú támadási technikái*. 2017. http://biztonsagpolitika.hu/wp-content/uploads/2017/04/Deak_Veronika_a-social-engineering-hum%C3%A1n-alap%C3%BA-t%C3%A1mad%C3%A1si-technik%C3%A1i.pdf (A letöltés ideje: 2018. 04. 17.)

[12] MINORICS D.: *Internetes keresők*. 2016. https://thepitch.hu/internetes-keresok/ (A letöltés ideje: 2018. 04.22.)

[13] BÓTA L.: *Internetes keresőrendszerek működése*. Eger: Eszterházy Károly Egyetem, 2011.

[14] *Védekezés a GHDB* (Google Hacking Database) *ellen*. https://blackcell.hu/acunetix-web-serulekenyseg-vizsgalo/ (A letöltés ideje: 2018. 04. 22.)

[15] CROSS, M., HARRINGTON, M.: *Google Earth Forensics*. Waltham: Syngress, 2015.

[16] ANDREWS, L.: *I know who you are and I saw what you did. Social Networks and the Death of Privacy*. New York: Free Press, 2011.

[17] LEITOLD F.: Sebezhetőségvizsgálatok a gyakorlatban. Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[18] BODENHEIM, R., BUTTS J., DUNLAP, S., MULLINS, B.: Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. *International Journal of Critical Infrastructure Protection*. 7.2. https://doi.org/10.1016/j.ijcip.2014.03.001A letöltés ideje: 2018. 05. 21.)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

A KIBERTÉR ÉS SZEREPLŐI

THE CYBERSPACE AND ITS ACTORS

GÉMES Csaba

(ORCID: 0000-0003-3012-2175)

gemes.csaba@uni-nke.hu

Absztrakt

„Az információ hatalom” tartja a közkeletű mondás. A hatalom általánosságban a mások befolyásolására való képességként fogalmazható meg, beleértve a mások befolyásának elkerülését is. A hatalom megőrzése, az egyes országok fennmaradása az elmúlt évezredekben csak a megfelelő fizikai erő alkalmazásával volt garantálható.

Az infokommunikációs technológia elterjedése egy új dimenziót nyitott az emberiség számára: a kiberteret.

Az elmúlt évek eseményei azt bizonyították, hogy a kibertérben olyan mértékű lehetőségek és veszélyek rejlenek, amelyek komoly hatást gyakorolhatnak az állam működésére.

Az állam érdekeinek kibertérben való érvényesítése csak a megfelelő kiberképességek kialakításával, illetve fejlesztésével érhető el. A cikk írója ennek lehetőségeit kutatja. Ebben a cikkben a kibertér értelmezését követően áttekinti a kibertér mindazon szereplőinek körét, akiknek szerepe lehet egy integrált nemzeti kiberképesség létrehozásában.

Kulcsszavak: *kibertér, kiberbiztonság kiberhadviselés, kiberképesség*

Abstract

“The information is power" the common saying keeps it. The Power in generality can be describe as an ability to influence others, including avoiding the influence of others. The Conservation of the power, the survival of individual countries in the last millenniums was only guaranteed by the use of the appropriate physical force.

The spread of info-communication technology has opened up a new dimension for the humanity: the cyberspace.

The events of past years have proved that the extent potential opportunities and threats in cyberspace, which they are serious implications for the functioning of the state.

Asserting the claims of the state in cyberspace only the equivalent cyber capability with his forming and his developing can be rached. The author of the article has been researching the opportunities of this. In this article he reviews those actors who may be involved in the creation of an integrated national cyber capability, after the interpreted the cyberspace.

Keywords: cyberspace, cybersecurity, cyberwarfare, cyber capability

BEVEZETÉS

Az „információ hatalom” tartja a közkeletű mondás. Nehéz lenne ezt cáfolni, látva a napjaink információs társadalma által szolgáltatott számtalan példát. Emellett azt is tényként kezelhetjük, hogy az emberiség által felhalmozott információ mennyisége rohamosan növekszik. De hol is találkozhatunk ezzel az óriási mennyiségű információval? A válaszokat keresve elsőként az információt hatalommá változtatni képes emberi elmét kell említenünk. Mivel az emberi elme befogadóképessége véges, így évezredekkel ezelőtt elkezdtük az információ írásos rögzítését, majd kihasználtuk a tárgyiasult formájú információ továbbításának lehetőségét is. Az elektrotechnika megjelenésével mintegy kétszáz éve képessé váltunk az információ egyre nagyobb távolságra való azonnali eljuttatására is. Az informatika megjelenése lehetővé tette az információk automatizált feldolgozását, majd a távközlés vívmányait kihasználva megérkeztünk az internet korszakába. Mindez azért fontos számunkra, mert a tudati és fizikai tér után a hálózatok világága az információ tárolása és feldolgozására egy új dimenziót nyitott meg számunkra: a kiberteret.

Amennyiben az információ felhasználásával elérhető előnyöket szeretnénk kiaknázni, akkor elsődleges szempontként az információhoz való hozzáférés lehetőségét kell megvizsgálnunk. A tudati, a fizikai és a kibertérben elérhető információk hozzáférhetőségét általánosságban összehasonlítva, akár a hozzáférés technikai lehetőségeit, akár az adott térben elérhető információ mennyiségét tekintve megállapíthatjuk, hogy a kibertérben lévő információ kiemelt és egyre nagyobb jelentőséggel bír.

Nem szabad megfeledkeznünk arról sem, hogy a kibertér rohamosan növekvő adattömegében elérhetőek a saját információink is, így az információhoz való hozzáférés nem csak részünkre nyújt kiaknázható lehetőséget, hanem az esetleges ellenérdekű feleknek is, amelynek megakadályozása érdekében célszerű lépéseket tenni.

Ezeket a szempontokat figyelembe véve egyértelmű, hogy a kibertérben rejlő lehetőségek kihasználására, illetve a szükséges óvintézkedések megtételére egyéni, szervezeti (vállalati, üzleti) és állami szinten is egyre nagyobb az igény. Az igény megfogalmazását követően magától értetődően adódik a kérdés:

Hogyan lehet az igényeknek megfelelő kiberképességet létrehozni, kiépíteni, fejleszteni?

Sajnos erre a kérdésre nincs egyértelmű válasz. A téma vizsgálatát megkezdve egyből szembetűnő, hogy a kiberképességek kialakítása több, egymástól különböző szemléletmód mentén kezdődött meg. Habár a különböző szemléletmód mellett kialakított képességek közt számos hasonlóság is felfedezhető mégis egyértelmű, hogy a kibertér nyújtotta lehetőségek optimális kihasználása önmagában is igen összetett feladat így a megoldás keresése is mélyebb elemzést kíván.

Cikkemben ezt a munkát kezdem meg, amelyben célom a kibertér lényegének és összefüggéseinek, illetve a kibertér kihívásaiban érintett szereplők körének vizsgálata. A vizsgálandó kihívások és szereplők körének meghatározásához - a témában kissé előbbre ugorva – a NATO Kibervédelmi Kiválósági Központja[1] által kiadott békeidejű kibertéri állami tevékenységekkel foglalkozó kiadványban [1] szereplő, az állami és a velük együttműködő szereplőkről szóló cikk [2] gondolatmenetét követtem, amely a kiberképességek kialakításának egy lehetséges megoldási módját vázolja fel.

[1] NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCoE)

A KIBERTÉR

A bevezetésben a kiberteret fontossága alapján, a számunkra egyre jelentősebb értéket képviselő „információ” oldaláról közelítettük meg. Az információ természetes közegét jelentő emberi tudat mellett, a történelem előrehaladtával az információ rajzként, majd írásként tárgyiasulva fizikai formában is elérhetővé vált. Az információ elektronikus tárolásának, feldolgozásának és továbbításának lehetősége új dimenziót nyitott az emberiség számára: a kiberteret.

A Kibertér értelmezése

A fogalom eredetét keresve először a görög „*kübernétész*” görög (jelentése: kormányos) szóból eredő kibernetikával találkozunk. A kibernetika egy komplex tudományos irányzat, amely a szabályozás, vezérlés, információfeldolgozás, -továbbítás általános törvényeit kutatja. A kibernetika alapítójának az amerikai matematikus Norbert Wienert tartják, aki a második világháború alatt a légvédelmi rendszerek matematikai problémáival foglalkozva 1940-ben fogalmazta meg a korszerű számítógépekkel szemben támasztott alapkövetelményeket. A kibernetika szóval először az 1946-ban megjelent könyvében [3] találkozhatunk, amelyben az állatokban és a gépekben zajló információáramlás, hírközlés, vezérlés és ellenőrzés kérdéseivel foglalkozik.

A „kibertér” kifejezést William Gibson amerikai-kanadai sci-fi írónak köszönhetjük, aki már az 1970-es években készült első műveiben foglalkozik a kibernetika és a számítógépes hálózatok emberre gyakorolt hatásával. A kibertér fogalmát először az 1982-ben megjelent "Izzó króm” *(Burning Chrome)* című novellájában [4], majd a szélesebb körben ismert 1984-es Neurománc (*Neuromancer)* című regényében [5] használta. Műveiben a „cyberspace” a fizikai világot jelentő „metaspace”-től elkülönült környezetként jelenik meg.

Az idők folyamán számtalan megfogalmazás született a kibertér meghatározására [3]. Ezek alapján általánosságban a kibertér az elektronikus kommunikációs eszközök és rendszerek (számítógép-hálózatok, telefonvonalak, műholdas rendszerek stb.) és a rajtuk található szolgáltatások, információk alkotta virtuális tér, vagy világ összefoglaló neveként értelmezhető [7].

Az internet térhódításával egyre több korábban független kommunikációs hálózat, rendszer, eszköz és szolgáltatás kerül összekapcsolásra, vagy akár kiváltásra az internettel. Ezen folyamat tükrében nem meglepő, hogy a köznapi szóhasználatban a kibertér fogalmát egyre gyakrabban azonosítják az internettel, illetve a világhálón keresztül elérhető virtuális világgal.

Ugyanakkor a fent összegzett általános, illetve a Magyarország Nemzeti Kiberbiztonsági Stratégiájában található hivatalos megfogalmazásból is kitűnik hogy „kibertér” fogalma tágabb területet fed le: „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint e rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.” [8]
Tehát az interneten kívül a kibertér részét képezik az internettől többé-kevésbé független hálózatok, rendszerek és eszközök is amelyek világhálóhoz való csatlakoztatásuk ezután várható, valamint azok is amelyeknél vállalati (ipari, kereskedelmi, stb.) vagy állami érdekből éppen a világhálótól való minél nagyobb függetlenség megőrzése törekednek. A függetlenség igénye többnyire biztonsági okokra vezethető vissza. Legyen az akár a folyamatos és zavartalan működés biztosítása, vagy akár az információkhoz való jogosulatlan hozzáférés, módosítás lehetőségének csökkentése.

A biztonság szempontjából különösen érzékeny pontot jelentenek a mindennapi életünk biztosítása szempontjából kritikusnak tekinthető infrastruktúrák, mint például az energiaszolgáltatás, közlekedés, víz, vagy az agrárgazdaság részeként az élelmiszeripar. Szintén a kritikus infrastruktúrák körében tartoznak az állam működése szempontjából kiemelt

fontosságú elemek, mint például a kormányzás és a védelmi szektor (rendvédelem, honvédelem, nemzetbiztonság) Az egyes kritikus infrastruktúrák működéséhez szükséges információs rendszerek, kiegészülve az önmagukban is kritikus infrastruktúraként értelmezhető hálózatokkal, rendszerekkel és szolgáltatásokkal (mint például telefon- vagy az internetszolgáltatás) külön kiemelt védelmet igénylő csoportot képeznek, kritikus információs infrastruktúraként. Ezen információs infrastruktúrák működési közegét is a kibertér jelenti. A működési közeget említve nem szabad megfeledkeznünk arról sem, hogy az információs rendszereink, eszközeink közötti kapcsolatot biztosító hálózatok, így vezeték nélküli összeköttetéseket biztosító elektromágneses spektrum is kibertér részeként értelmezhető.

A kibertér védelmi oldalról való megközelítésénél találkozhatunk olyan speciális kibertérben megvalósuló jelenségekkel, tevékenységekkel amelyek önálló szakterületként értelmezhetőek, mint például kiberbűnözés (kiberterrorizmus) elleni küzdelem, vagy a kiberhadviselés. Ezen szakterületek speciális feladatrendszere magával vonja a kibertér sajátos, gyakran bővített értelmezését, mint ahogyan az a következő részben látható.

A kibertér katonai és geopolitikai jelentősége

Katonai szempontból a kibertér a korábbi a fizikai térben lévő szárazföldi, tengeri, légi, kozmikus hadszínterek mellett önálló hadszíntérré vált[2]. Ugyan kibertérről csak néhány évtizede, kiberhadszintérről pedig csak néhány éve beszélünk, az elektronikus adattovábbítás. lehallgatás, zavarás már egy évszázada jelen van a hadszíntereken. A híradás, rádiófelderítés és zavarás után megjelent a rádiólokáció, majd az automatizált adatfeldolgozásra épülve az elektronikus irányítású fegyverek, fegyverrendszerek rendszeresítése vált lehetővé. A távközlés és informatikai fejlődése a hadviselésben is drasztikus mértékű változásokat hozott. Napjainkra a szenzorokra épülő felderítő, azonosító és navigációs, illetve vezetés-irányítási és kommunikációs rendszerek komplex – gyakran integrált – rendszerekké fejlődtek. A rendszerek egyes komponenseinek működése illetve az eszközök közötti adatcsere az elektromágneses spektrum különböző tartományaiban valósul meg [9]. Ebből következően nem meglepő, hogy a kibertér katonai értelmezéseiben kiemelt helyet foglal el az elektromágneses spektrum használata. A Magyar Honvédség kibervédelmi koncepciójában [10] a kibertér meghatározásának középpontjában kifejezetten az elektromágneses spektrum használata áll[3], amely a „kiberkörnyezet" fogalmaként[4] egészül ki a felhasználók, a hálózatok, hardver- és szoftverelemek, folyamatok, szolgáltatások, illetve a kibertérben tárolt és továbbított adatok körével. A elektromágneses spektrum és kibertér elválaszthatatlanságát jól példázza az USA hadserege által alkalmazott „kiber-elektromágneses tevékenységek" terminológia[5], amelynek megfelelően a kibertéri műveletek és az elektronikai hadviselést közös direktíva[6] tárgyalja [11] [12].

[2] 2016 júniusában a NATO varsói csúcstalálkozóján az elektronikus formában lévő információ létezési közegét jelentő kiberteret hivatalosan is elismerik ötödik műveleti dimenzióként a korábbi négy fizikai (szárazföldi, légi, tengeri, kozmikus) hadszíntér mellett.

[3] 0 2. 8) pont szerint: „A kibertér: az elektromágneses spektrum használatával meghatározható, dinamikusan változó tartomány, mely az összekapcsolt hálózatok, eszközök és kiegészítő fizikai infrastruktúrák közötti adatok kezelésére szolgál."

[4] 0 2. 8) pont szerint: „Kiberkörnyezet: felhasználók, valamint a kibertérben lévõ hálózatok, eszközök és minden szoftver, folyamat, tárolt vagy továbbított adat, alkalmazás, szolgáltatás, továbbá a hálózatokhoz közvetlenül vagy közvetetten csatlakozó hálózat"

[5] Cyber Electromagnetic Activities (CEMA)

[6] már a [11] direktíva címében is megjelenik, illetve az ezt kiváltó [12] direktíva is követi a terminológiát

A kibertér katonai értelmezését és jelentőségét röviden áttekintve láthattuk, hogy az elektronikus eszközök és az elektromágneses spektrum használata már a „kibertér" és a „kiberhadviselés" kifejezések megjelenése előtti évtizedekben is általános részét képezte a hadviselésnek. Joggal vetődik fel a kérdés, hogy az állami működés egyéb területein mikor és hogyan vált jelentőssé a kibertér használata, illetve vált geopolitikai tényezővé.

A kibertér geopolitikai szerepének sokáig nem tulajdonítottak jelentőséget, sőt az internet úttörői által létrehozott mozgalmak a 90-es években kibontakozó elméleteik szerint az internetet a vadnyugathoz, mint az amerikai demokrácia bölcsőjéhez hasonlítva az internet szuverenitását hirdették, amelyben a világ kormányainak törvényei nem alkalmazhatóak.

Az internet szabadságát hirdető, napjainkban is fennálló elmélet[7] amely szerint az internet nyitott felépítése, erősen decentralizált, központ nélküli működése éppen a szabad információcsere és szólásszabadság jegyében lett létrehozva annak érdekében, hogy az információ szabadon tudjon áramlani, bármilyen akadály ellenére is. Eszerint az internet olyan világ, ahol minden az emberi elmétől származik, ennek megfelelően újratermelhető és terjeszthető anélkül, hogy pénzbe kerülne [13]. Ez a szabadelvű megközelítés képezi a napjainkban is működő hacktivista mozgalmak alapját. Habár az internet használatával összefüggő fenyegetések már ebben e kezdeti időszakban ismertek voltak, az általuk okozott károk nem érte el azt az ingerküszöböt, hogy az internet szabadelvű használata ne uralkodó nézetként maradjon fenn.

A szabad használat korlátozása elsőként a kiberbűnözés elleni védelem területén jelent meg. A számítógépes bűnözéssel összefüggő paragrafusok az egyes országok törvényeiben már a 80-as években megjelentek. Nemzetközi szinten az első lépést az Európai Tanács 1992-ben elfogadott Maastrichti Szerződése alapján létrejött hárompilléres rendszer megalkotása jelentette, amelynek pilléreit a kiberbiztonság mellett a közös kül- és biztonságpolitika, illetve a kiberbűncselekményekkel kapcsolatos szabályozás képezte.

Az első gyakorlati szempontból jelentős nemzetközi szintű megállapodásként az Európa Tanács Számítástechnikai bűnözésről szóló egyezmény (Budapesti Egyezmény) aláírása 2001-ben került sor, amely a kiberbűncselekmények szabályozása kapcsán a nyugati világ számára egyöntetűen elfogadott etalont jelent [14][14].

A kiberbűnözés számos lehetőséget biztosít a terrorizmus támogatására is. A 2001. szeptember 11-ei események hatására a kiberbűnözésből kiválva – mint annak sajátos és szélsőséges formája – a kiberterrorizmus önálló területként jelent meg. A 2000-es évek kiberterét – a kiberbűnözés és kiberterrorizmus veszélyit ugyan szem előtt tartva – az információs társadalom, illetve az ehhez szükséges infrastruktúra kiépítése jellemezte.

A kibertér védelme szempontjából az első kiberháborúnek tekintett 2007-es észtországi kibertámadás-sorozat jelentette a fordulópontot. Az eset rávilágított arra, hogy a kibertérből érkező koncentrált támadás a polgárok létszükségleteit kielégítő ellátórendszert, illetve ezen keresztül az állam egészének működésképtelenségének mértékét is elérheti. Az eset következtében új lendületet kapott a kritikus infrastruktúrák védelme, illetve egyértelművé tette az állami szerepvállalás jelentőségét kibervédelemi feladatok kapcsán [15]

A következő jelentős esemény a Stuxnet névre keresztelt vírushoz köthető, amely 2010-ben jelentősen visszavetette az iráni atomprogramot. A vírus működésének elemzése több, biztonsági szempontból mérföldkőnek tekinthető tényre mutatott rá. Az igen összetett, nagy szakértelemmel megírt vírus több nulladik napi sérülékenységet kihasználva képes volt úgy

[7] Alix Desforges francia geopolitikus elmélete, amely szerint az internet szabadságága az 1960-as évek kulturális forradalmából eredeztethető.

széles körben rejtetten terjedni, hatását – célzott támadásként– csak a kiválasztott típusú radioaktív izotópok dúsítására használt gázcentrifugákban fejtje ki. A vírus a hálózati kapcsolatokon túl képes volt fertőzni az ipari rendszerek frissítésére használt USB eszközökön át, bizonyítva hogy a hálózatoktól gondosan szeparált rendszerek is sikeresen támadhatóak. Az eset az ipari vezérlők sérülékenységén keresztül rávilágított az ilyen típusú informatikai elemeket tartalmazó – korábban szeparáltságuk miatt is biztonságosnak tartott – kritikus infrastruktúrák fokozott kiszolgáltatottságára. Az eset mérföldkövet jelent a abból a szempontból is, hogy a korábbi kibertámadások csak ”soft” (azaz közvetett módon) okoztak károkat, míg a Stuxnet a gázcentifugák túlpörgetésével közvetlen módon, valódi fizikai kárt tudott okozni, bizonyítva hogy a kiberterrorizmus kapcsán korábban csak elméleti feltételezésként megjelenő „hard” típusú támadások is indíthatóak a kibertérből. [16] 223-227. o.]

A 2010-es Wikileaks kiszivárogtatási botrány, majd az az Edward Snowden által 2013-ban kirobbantott lehallgatási ügy rávilágított arra, hogy a kibertér magában hordozza a nagy mennyiségű érzékeny információ megszerzésének és széles körű megosztásának oly mértékű lehetőségét is, amely alkalmas lehet az egyes országok közötti viszonyok megváltoztatására is.]

A katonai vonatkozásban már a 90-es évek óta komoly jelentőséggel bírnak a kibertérben megvalósuló információs műveletek. Habár az emberi tudat kibertéren keresztüli befolyásolása már az elektronikus média (rádió, TV) megjelenésével megkezdődött, az igazi jelentőségét az internet elterjedésével érte el. Eleinte csak a böngészési előzményeken alapuló reklámok, majd a közösségi média, bloggerek, trollok, és egyéb álhír terjesztők befolyásolták a tudatunkat. A kibertéren keresztüli befolyásolási képesség napjainkra már elérte a felső szintű politika közvetlen befolyásolásának szintjét. [17]

A KIBERTÉR SZEREPLŐI

Az egyes országok kormányai, hadseregei, vállalatai és polgárai az elmúlt évek példáin keresztül szembesültek a kibertér egyre növekvő jelentőségével. A kibertér sajátos környezetében látott példák egyszersmind rávilágítottak a saját érdekek megvédésének szükségére és a lehetőségek megragadásában rejlő előnyökre is.

Ez különösen igaz az állam egészének esetében, amelynek érdeke szemben áll a virtuális ér többi szereplőjével, ezen belül a nem állami szférához tartozó szereplőkkel (kiberbűnözőkkel, a hackerekkel, aktivistákkal, másként gondolkodókkal, a nagy magánvállalatokkal) vagy éppen más államokkal. [2]

A felismerést megfontolt elgondoláson alapuló tettek kell hogy kövessék, Az elgondolást célszerű stratégiagént megfogalmazni, amely felvázolja a jelenlegi állapotot, kitűzi az elérni kívánt célokat, valamint ezek alapján kijelöli a célok eléréséhez vezető utat. A célok eléréséhez szükséges kiberképességek kialakításához több út is vezethet.

Az útkeresés egyik fontos szempontját a kezdeti állapotként rendelkezése álló, illetve a kiberképességek kialakítása során igénybe vehető erőforrások jelentik. A kibertér különböző szereplőit tekintve feltételezhető, hogy az erőforrások elosztásában jelentős különbségeket találhatunk, elég akár csak a rendelkezésre álló anyagi háttérre, vagy akár a szaktudásra gondolni. A kibertér szereplőinek az eltérő státuszukból adódóan a jogi értelemben vett lehetőségei is különbözőek. Ugyanakkor egy állam egy adott kiberképességének létrehozásában több szereplő is érintett lehet függetlenül attól, hogy az állami, vagy nem állami szférához tartozik.

Ennek megvalósítási lehetőségeit vizsgálta Alexander Klimburg [18] is, a különböző szereplők tevékenysége közötti hasonlóságokból kiindulva. Klimburg szerint a számítógépes

bűnözés, a számítógépes terrorizmus és a számítógépes hadviselés közös technikai alapokra épül, hasonló eszközöket, logisztikát, és működési módszereket, ugyanazon közösségi hálózatokat és infrastruktúrákat használva, hasonló célokból. Az egyes kibertevékenységek közötti különbség legtöbbször alig felfedezhető. A kiberhadviselés szemszögéből nézve a kiberbűnözés a technikai, (szoftvereszközök és logisztikai támogatás), a számítógépes terrorizmus pedig társadalmi alapot jelenthet (személyes hálózatok és motiváció) az ellenséges csoportok vagy államok számítógépes hálózatainak megtámadására. A nemzet kibertérben történő erőkifejtése három dimenzióra osztható. Elsődlegesen a kormányzat által kordinált működtetési és szabályozási környezet, a nemzetközi szövetségek illetve nemzetközi jog környezete, valamint a nem állami szereplőkkel történő együttműködés. Habár ezekből az állam számára az első két dimenzió tekinthető alapvetően fontosnak, a kibertér természete olyan, hogy a kiberképességek jelentős része a közvetlen kormányzati ellenőrzésen kívül eső üzleti és a civil szektorban rejlik. A kormányzati és a nem állami szektor együttműködésével integrált nemzeti kiberképesség hozható létre.

A nyugati demokráciák képesek motiválni, vonzani a saját állampolgárait, ami alapvető fontosságú az egész nemzeten alapuló kiberképesség létrehozásához. Az „egész nemzet" (whole of nation) biztonságpolitikai megközelítés a kormányzati és a nem állami (üzleti és civil) szektor a közös célok elérése érdekében tett integrált (egész társadalmat érintő) erőfeszítéseit jelenti, amelynek alkalmazása csak mintegy tíz éve kezdődött az Amerikai Egyesült Államokban. A nyugati országok viszonylag lassan ismerték fel az integrált nemzeti képesség fontosságát Ezzel szemben Oroszország és Kína magasan szinten és jól látható módon alkalmazza a nem állami kiberképességeket. [18]

Nem kétséges tehát, hogy a kiberképességek kialakításának tervezéséhez az első lépést a kibertér állami és nem állami szereplőinek megismerése kell, hogy jelentse.

A kibertér állami szereplői

A kibertér állami szerepét vizsgálva kiindulópontként tekinthetjük azt a tényt, hogy az egyes országok kialakulását és fennmaradását az erőszakszervezeteken a közigazgatáson alapuló hatalom koncentrált gyakorlása biztosítja[8]. A hatalom általánosságban a mások befolyásolására való képességként fogalmazható meg, beleértve a mások befolyásának elkerülését is. Az állam szempontjából a hatalom a nemzeti célok és törekvések megvalósításának eszköze a kormány kezében. [2]; 1.o.] Az állam monopol helyzetét biztosító hatalom megőrzését évszázadokon át a koncentrált fizikai erő garantálta. A kibertér katonai és geopolitikai jelentőségét meghatározó események bizonyítják, hogy a kibertértérben rejlő befolyásoló erő hatalmi tényezővé vált. Ennek nyomán egyre több ország felismerte, hogy az állami érdekek érvényesítéséra a kibertérben is szükség van.

Az állam kibertérben játszott szerepe három fő tevékenységi területe osztható: a kiberbűnözés elleni védelem, a titkosszolgálatokok tevékenységére és a honvédelemre.

A bűnüldözés és jogérvényesítés

A bűnözés elleni védelem, tágabb értelemben a jogrend érvényesítése a kibertérben is elengedhetetlen az állam és polgárainak védelme érdekében.

[8] Max Weber általánosságban használt meghatározása alapján az állam „a fizikai erő legitim használatának monopóliumával egy adott területen belül", amely tartalmazhatja a fegyveres erőket, társadalmi szolgáltatásokat, állami bürokráciát, bíróságokat és a rendőrséget.

Az információs technológia elterjedésével a kibertér használatának előnyeivel párhuzamosan nőtt a visszaélés lehetősége is. A technológia által nyújtott lehetőségek kártékony hatású kihasználása ellen a jogérvényesítés eszközeivel illetve az ezt támogató műszaki módszerekkel lehet fellépni. A jogi eszközök kibertérben történő érvényesítésének első lépése a jogszabályalkotás. Ennek kezdeti lépésit jelentették a számítógépes bűncselekmények korai szabályozása, majd a kiberbűnözés fentebb tárgyalt részletesebb nemzetközi és állami szinten történő szabályozása. Napjainkban a kiberteret érintő jogi környezet részét képezik a kibertér jelentőségét deklaráló és az elérendő célokat, a fő irányokat meghatározó stratégiák, valamint a célok eléréséhez szükséges szervezet- és feladatrendszert rendelő, illetve a szabályokat rögzítő törvények és egyéb jogszabályok.

A jogszabályalkotás az adott ország állami felépítésétől, illetve az adott jogszabálytól függően parlamenti, kormányzati, ágazati feladat. A jog érvényesítése a végrehajtó hatalom, jellemzően a bíróságok feladata. A jogérvényesítés sarkalatos kérdése a bizonyítékok szolgáltatása, amely igen összetett feladatot jelent az ezért felelős nyomozóhatóságok és a bevont szakértők számára. A megbízhatónak tekinthető bizonyítékok gyűjtése az egyéb védelmi szabályok érvényesítésével együtt egyes információkezelő rendszerek üzemeltetőinek a feladata. A rendszerek védelmi feladatai egyaránt igen komoly műszaki és jogi kihívást jelentenek a jog- és egyéb védelmi szabályok alkalmazásért felelős üzemeltetőkre, a jogszabályalkotásért és az egyéb alacsonyabb szintű szabályozás kialakításért felelős, illetve a szabályok érvényesülésének ellenőrzésért felelős felügyeleti szervekre.

A kiberbűnözés elleni küzdelem feladatai általában a rendvédelmi szervek hatáskörébe tartoznak, Ettől eltérően más szervezetek is érintettek lehetnek. A bűnmegelőzés kapcsán kiemelt fontosságú felhasználói tudatosság kialakítása, vagy a megfelelő szaktudás biztosítása kiegészülve az azt megalapozó kutatási feladatokkal, amelyben az oktatási szféra, különösen az egyetemek és a kutatásokban részt vevő szervezetek érintettek. [18]6 o.]

A kiberbűnözés a kiberbűncselekmények mellet magában foglalja a kiberterrorizmus elleni védelmet is. [18] 4, o.] A kibertetrrorizmus elleni védelem, illetve az egyéb kiberbűnözéshez kapcsolódó feledatokban a nemzetbiztonsági szolgálatok is érintettek lehetnek.

A nemzetbiztonsági szolgálatok

Az államok közötti kémkedés közös és meglehetősen hagyományos tevékenység, amely nemzetközileg elfogadott állami gyakorlat, még akkor is, ha a cselekményt mint olyat általában a nemzeti jogrendekben bűncselekménnyé nyilvánítják. A kémkedéssel szinte egyidős az azzal szembenálló elhárítás is. A hírszerzési és elhárítást tevékenységet végző nemzetbiztonsági szervek természetes módon mindig is kihasználták a technika adta lehetőségeket. Az infokommunikációs technika fejlődésével a lehetőségek kiszélesedésében az információk elérhetősége és mennyisége mellett óriási jelentősége van az anonim lehallgatás és beavatkozás lehetőségének. Ugyan a nemzetbiztonsági szervek konkrét képességei általában rejtettek a külvilág számára, az Edward Snowden által kiszivárogtatott adatok rávilágítottak a kibertér nemzetbiztonsági szempontú kihasználáságának mértékére. [2]; 14. o.]

A fegyveres erők

A kibertér katonai alkalmazása az elektronikai hadviselés területén már egy évszázados, a számítógépes rendszerek védelme területén néhány évtizedre nyúlik vissza.

A kibertérben a védelmi a felderítő és a támadó tevékenységek is egyértelműen értelmezhetőek, ennek ellenére a NATO és az egyes országok csak egy-két éve kezdték a kiberteret önálló hadszíntérként értelmezni. Ez részben visszavezethető a kibertér azon sajátosságaira amely jelentősen eltér a hagyományos fizikai térben lévő (szárazföld, tenger, légi, kozmikus) hadszínterektől.

A kibertérben komoly problémát jelent a bizonyíthatóság hiánya. Ez egyaránt igaz a támadást indító eszközök és azok fizikai helyének egyértelmű azonosítására. Ennél is nagyobb

problémát jelent a szemben álló fél személyének, szervezeti hovatartozásának, országának azonosítása. Nincs közös nemzetközi jogalap arra sem, hogy milyen típusú célpontok ellen, milyen jellegű illetve mértékű támadás tekinthető katonai értelemben vett kibertámadásnak.[15]; 35-38].

A kibertér nem állami szereplői

Hackerek

Az internet fejlődése a hackerek felemelkedésével járt. A hackerek az informatikai iránt érdeklődő, többnyire a fiatalabb generációkba tartozó személyek, akik informatikai rendszerek, szolgáltatások feltörésével kezdtek foglalkozni, elsősorban a kíváncsiság és a felfedezés öröme által hajtva. A hackerek figyelemre méltó célpontok kiválasztásával, látványos módon történő feltörésével, vagy az onnan megszerzett adatok által hírnévre tettek szert. Fontos megemlíteni hogy maga a hackelés sokáig nem számított bűncselekménynek. A bűntető törvénykönyvek többnyire nem a hackelés cselekményét rögzítették annak hatása alapján. Ha az esetek kivizsgálására került sor akkor legfeljebb más jogi normák, például a szerzői jogok megsértése, vagyontárgyakban okozott károk képezték a jogalapot.

A jogi megítélés alapján szokássá vált a hackerek megkülönböztetése. A jogszabályok keretein belül tevékenykedő ártalmatlan hackereket fehér, az azokat átlépő rosszindulatú tevékenységet folytatókat fekete, illetve a mindkét oldalon tevékenykedőket szürke kalapos hackerként emlegetve. A valóságban igen nehéz különbséget tenni, sok esetben a jogi megítélés egyértelműen nem tisztázható. Gyakran előfordul, hogy a politikai, vagy a média általi megítélés dönti el az egyes esetek, vagy a hackerek megítélését. Az infokommunikációs technológiák és a szolgáltatások globális piaccá válásának köszönhetően a rendszerekkel és szolgáltatásokkal szembeni rosszindulatú tevékenység, az adatok megszerzéséhez jövedelmező szakmává vált, sokakat arra ösztönözve, hogy erre a területre szakosodjanak.

Napjainkra kialakult az a jogi szempontból is elfogadott etikus hackelésnek nevezett tevékenység amely a biztonsági üzletág keretein belül segít megvédeni az ügyfeleket a rosszindulatú szereplők ellen. Az etikus hackelés során úgynevezett (sérülékenységi) teszt keretében az ügyfelek beleegyezésével tesztelik a rendszer biztonsági mechanizmusait, amelyek célja a biztonsági szint emelését segítő javaslatok megfogalmazása. Másrészt az informatikai biztonsági szakértőknek is szüksége van hackerek támadási technikáinak ismeretére, ezzel szilárd alapot nyújtva a támadások gyakoriságának és általuk az okozott károk csökkentésére vagy megakadályozása, vagyis a megfelelő védelem kialakításához. Az informatikai biztonsággal foglalkozó oktatásra is specializálódott cégek napjainkban már széles körben elérhetővé tették a tanúsított etikus hacker[9] és hálózabiztonsági[10] képzéseiket.

A szürke kalaposként említett hackerek céljukként a kibertér biztonságosabbá tételét tekintve, a szélesebb közösség érdekében használják képességeiket. Ugyan tevékenységüket a rosszindalatú felekkel szemben fejtik ki, cselekedeteiket ugyanúgy jóváhagyás nélkül végzik, így az egyes rendszerekben szolgáltatásban felhatalmazás nélkül elkövetett beavatkozásuk, jogi értelemben ugyanúgy bűnnek számít. Tetteik igazolását – mint a jó szándéktól vezérelten a magasabb eszmék megvalósításaként – az egyes szolgáltatások, az internet és kibertér biztonságosabbá tételére való törekvésükre való hivatkozásban látják. A szürke kalaposok néha azzal is kárt okoznak, hogy a rendszerek, szolgáltatások sérülékenységeit nyilvánosságra hozzák vagy kiszivárogtatják, viszont ők ezt megelőzően általában kapcsolatba lépnek az

[9] CEH: Certified Ethical Hacking
[10] CNDA: Certified Network Defense Architect

érintett tulajdonosokkal, üzemeltetőkkel, akár a biztonsági hibák elhárításához szükséges információkat is megosztva velük.

A fekete kalapos hackerekkel is előfordul hogy felkeresik az érintetteket, viszont azt többnyire zsarolási szándékkal teszik. A fekete kalapos hackereket elsősorban személyes haszonszerzésre használják készségeiket és tudásukat. Hírnevük többnyire arra vezethető vissza, hogy valamilyen ellenszolgáltatás fejében tesznek, vagy éppen nem tesznek meg valamit. [2]

Kiberbűnözők

A 20. század végét jellemző jelentős infokommunikációs beruházásoknak, informatikai biztonsági fejlesztéseknek köszönhetően, illetve a nagyobb rendszerekben megvalósítható jogosulatlan hozzáféréshez szükséges készségszint jelentősen megnőtt. Ugyanakkor a rohamosan növekvő számú – jellemzően alacsony biztonságtudatossági szinttel rendelkező – internetfelhasználók gyakran a megfelelő védelem nélkül alakították ki a számítógépes rendszereiket. Ez a jelenség gyökeresen megváltoztatta a számítógépes bűnözés jellegét.

Ezen túlmenően a számítógépes bűnözés nemzetközi szabályozásának, és a már elfogadott egyezmények országonkénti alkalmazásának hiánya, illetve a korlátozott együttműködés, nagymértékben segítették az óriási bevételeket produkáló globális számítógépes bűnözés kialakulását.

Az elmúlt két évtizedben olyan rejtett gazdaság alakult ki, amelyben viszonylag alacsony összegért bárki hozzájuthat bűncselekmények elkövetéséhez használható szoftverkomponensekhez, adatbázisokhoz, és akár támogató szolgáltatásokhoz is. Ráadásul ezek viszonylag alacsony számítógépes ismeretekkel is komoly eredményeket produkáló kiberbűncselekmények elkövetésére alkalmas eszközzé állíthatóak össze. [2]

Hacktivisták

A hacktivizmus (hacktivism) a hackelés (hacking) és az aktivizmus (activism) kifejezéséből összeállított mesterséges szó, amelyet 1996-ban alkotott meg a Cult of the Dead Cow[11] hackercsoport egyik tagja.

A hacktivizmus a szólásszabadság, az emberi jogok és az információ szabadsága jegyében. számítógépes hálózatokon (általában az interneten) a hackerek által használt eszközöket alkalmazó aktivista mozgalom, Lényegét tekintve a hagyományos demonstrációk és polgári engedetlenség digitális megfelelői.

A hacktivisták a szürke kalapos hackerekhez hasonlóan, az írott jog szempontjait az etikai, illetve morális szempontoknak rendelik alá. Célpontjaik azok a mozgalom ellenfélként azonosított szervezetek, vállalatok és egyének, amelyek a hacktivista csoport rendelkezésre álló eszközökkel sikeresen támadhatók, és annak eredménye a figyelem felkeltésére alkalmas. A sikeresen támadott célpontok között számos nagyváros honlapja mellett már szerepelt a Sony, az USA szenátusa és hadserege, a CIA, az FBI, és számtalan más szervezet, amelyek támadása nagy hírveréssel járt.

Az alapvető hacktivista módszerek három csoportra oszthatók. Ezek közül legalapvetőbb az adott ügy melletti tömegtámogatás demonstrálására használt túlterheléses támadás[12], amelyet lényegében az ülősztrájk virtuális megfelelőjének tartanak .

A második – talán legjellemzőbb – hacktivista eszköz a weboldalak feltörése és átalakítása (defacement), ami a túlterheléses támadással szemben konkrét üzenetek megfogalmazására

[11] Cult of the Dead Cow: (A Döglött Tehén Kultusza) Az egyik első nevezetessé vált, 1984-ben a Texasban alakult hackercsoport

[12] DDoS: Distributed Denial of Service

alkalmas, ráadásul ezzel a módszerrel az üzenet közvetlen megjelenítése, közzététele, magán a megtámadott felületen történik. A weboldalak feltörésének és átalakításának eredeti – fizikai térben megvalósuló – a falfirka, vagy plakátok felülragasztása, átalakítása.

A hacktivista eszköztár harmadik csoportját a betörés, Információszerzés és kiszivárogtatás jelenti, ami tulajdonképpen a klasszikus hacker módszerek hacktivista csoportok általi használatát jelenti. Ebben az esetben a cél a weboldalak, adatbázisok, e-mail fiókok feltörése és az így szerzett információ kiszivárogtatása, nyilvánosságra hozatala.

A 2010-es évek elején elindult változás során a korábbi kisebb hacktivista csoportok hálózatba szerveződve olyan globális hacktivista mozgalmakká álltak össze mint az Anonymous, a LulzSec, az Indignados, vagy az Occupy

Közös vonásuk, hogy alapvető céljuknak tekintik a szabad terek megteremtését, legyen szó a kibertérről, vagy a közterekről, a politika, vagy a közbeszéd tereiről, ezért összefoglaló néven a „Terek Mozgalmaiként" nevezik őket.

Létrejöttükkel – kihasználva a kor technikai lehetőségeit – az alulról építkező civil hálózatok korábban nem látott globális kiterjedtségét és egyidejű szervezettségét valósították meg. A Terek Mozgalmai a 2011-ben, illetve az azóta kibontakozó világméretű tüntetéshullámok során példátlan összehangoltságról tettek tanúbizonyságot. [2] [20]

A felhasználók

A kiberszereplők ismertetésének végén – de nem utolsó sorban – szót kell ejtenünk az átlagos felhasználóról, aki egyrészt saját eszközeivel, információival, profiljával, tudati befolyásával és befolyásolhatóságával megjelenik a kibertérben. Másrészt a felhasználó mindennapi élete függ azoktól a kritikus infrastruktúráktól, amelyek mögött sérülékeny infokomunikációs rendszerek működnek. A felhasználó részese lehet a kibertérben folyó támadásoknak akár elkövetőként (ha nincs is tudatában) vagy áldozataként. A felhasználónak saját érdeke, hogy ezek ellen lépéseket tegyen. Ugyanakkor az államnak is felelőssége van abban, hogy az állam – beleértve a polgárai – kibervédelméről gondoskodjon.

ÖSSZEFOGLALÁS

Az egyes országok tekintetében az állam képezi a hatalom megtestesülését. A hatalom megtartását, az álam fennmaradást évszázadokon keresztül fizikai erővel kellett garantálni. A cikkben kiemelt események rávilágítottak arra, hogy az információtechnológi fejlődésével a kibertérben olyan mértékű lehetőségek és veszélyek rejlenek amelyek – akár az infrastuktúrákon, akár az állampolgárokon keresztül – komoly hatást gyakorolhatnak az állam működésére. A kibertér megnövekedett jelentőségét az egyes országok és szervezetek, szövetségek felismerték és lépéseket tesznek az érdekeik kibertérben is megvalósuló érvényesítése érdekében. Az ennek érdekében megfogalmazott stratégiai célok csak a megfelelő kiberképességek kialakításával illetve fejlesztésével érhetők el. A kiberképességek kialakítása már elgondolás szintjén is igen komoly feladatot jelent, mivel a megvalósítás a legtöbbször csak igen összetett és sajátos, sokszor még ismeretlen megoldásokon keresztül történhet. Célom ezen kiberképességek kialakításának kutatása, amelynek keretében ebben a cikkben a kibertér értelmezésén kívül áttekintésre kerültek a kibertér azon szereplői, amelyek jelentős szerepet játszhatnak az egyes kiberképességek kialakításában.

A kibertér szereplőinek áttekintése alapján megállapítható, hogy azok tevékenysége közös technikai alapokra épül. Hasonló eszközöket és működési módszereket, valamint többnyire ugyanazon infrastruktúrákat, hálózatokat és szolgáltatásokat használják. A különbségek jellemzően a motivációban a tevékenység társadalmi elfogadottságában és jogszerűségében, illetve az adott keretek közt elérhető eredményekben fedezhető fel. Az állami oldalon világosan körvonalazódik a kibertér feletti érdekérvényesítő képesség megszerzésének és fenntartásának szükségessége. Ehhez rendelkezésre áll az állam saját szervezeteinek képességei, amelyek

alkalmazásához biztosítottak a jogi keretek, kiegészülve a nemzetközi együttműködés lehetőségeivel. Ezzel szemben a nem állami szereplők között felfedezhetők társadalmi vagy etikai szempontból elfogadhatónak tartott, mégis egyes esetekben a jogszerűség határát súroló tevékenységek is. Ugyanakkor ezek a képességek igen hatásosak, viszont az állam – a jelenlegi jogi keretekből adódó korlátok miatt – azokat közvetlenül nem használhatja. Mivel az államnak szüksége lehet a nem állami képességek – akár közvetett módon történő – kiaknázására is, célszerű lehet amerikai, orosz és kínai példákkal alátámasztott integrált nemzeti képességek alkalmazási lehetőségeit vizsgálni.

FELHASZNÁLT IRODALOM

[1] ZIOLKOWSKI, K (Ed.): *Peacetime Regime for State Activities* In: *Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013. https://ccdcoe.org/sites/default/files/multimedia/pdf/PeacetimeRegime.pdf (letöltve: 2017.10.09.)

[2] CZOSSECK, C. *State Actors and their Proxies in Cyberspace* In: ZIOLKOWSKI, K (Ed.): *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013. pp. 1-29.

[3] WIENER N.: Cybernetics or Control and Communication in the Animal and the Machine The Massachusetts Institude of Technology, Cambridge, 1961, p. 212, ISBN: 0-62-230007 https://uberty.org/wp-content/uploads/2015/07/Norbert_Wiener_Cybernetics.pdf

[4] GIBSON, W.: *Izzó króm*, In: GIBSON, W.: *Izzó króm*, ford.: Bárday Tamás, Gáspár András, Hoppán Eszter, Szántai Andrea, Szántai Zsolt, Valhalla Páholy, 1997, pp. 133-163., ISBN 9639039284)

[5] William GIBSON: *Neurománc*, ford.: Ajkay Örkény, Valhalla Páholy Kft., Budapest, 1992, p.344 ISBN: 963-7632-05-0

[6] HAIG Zs.: *Információ, társadalom, biztonság.* NKE Szolgáltató Kft., Budapest, 2015. 978-615-5527-08-1

[7] HAIG Zs.: VÁRHEGYI I.: *A cybertér és a cyberhadviselés értelmezése*. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 18: (Elektronikus szám) 2008. pp. 1-12. http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf (letöltve: 2017.10.16.)

[8] A Kormány 1139/2013. (III. 21.) Korm. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról http://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf (letöltve: 2017.11.08.)

[9] HAIG Zs, Kovács L, Ványa L, Vass S, Németh András (szerk.).: *Elektronikai hadviselés* Budapest: Nemzeti Közszolgálati Egyetem, 2014. 271 p. (ISBN:978-615-5305-87-0) https://opac.uni-nke.hu/webview?infile=&sobj=9276&source=webvd&cgimime=application%2Fpdf%0D%0A (letöltve: 2017.11.08.)

[10] 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról. Hivatalos Értesítő, a Magyar Közlöny melléklete, 2013. 48. sz., Magyar Közlöny Lap- és Könyvkiadó, 2013. pp. 13873-13882. http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2013/10.pdf (letöltve: 2017.11.22.)

[11] FM 3-38 *Cyber Electromagnetic Activities,* Headquarters, Department of the Army Washington, DC, 12 February 2014. https://fas.org/irp/doddir/army/fm3-38.pdf (letöltve: 2017.11.22.)

[12] FM 3-12 *Cyberpace and Electronic Warfare Operations,* Headquarters, Department of the Army Washington, DC, 11 April, 2017. https://fas.org/irp/doddir/army/fm3-12.pdf (letöltve: 2017.11.22)

[13] DOUZET, F.: *Geopolitika a kibertér megértéséhez*, In: Pintér István (szerk.) Műhelymunkák: A virtuális tér geopolitikája. 367 p. Budapest: Geopolitikai Tanács Közhasznú Alapítvány, 2016. pp. 19-41. (ISBN:978-963-9816-34-3) http://mek.oszk.hu/16100/16182/16182.pdf (letöltve: 2017.12.27.)

[14] DORNFELD L.: *A kibertér főbb nemzetközi és nemzeti szabályozásai,* In: Pintér István (szerk.) Műhelymunkák: A virtuális tér geopolitikája. 367 p. Budapest: Geopolitikai Tanács Közhasznú Alapítvány, 2016. pp. 43-88. (ISBN:978-963-9816-34-3) http://mek.oszk.hu/16100/16182/16182.pdf (letöltve: 2017.12.27.)

[15] KOVÁCS L, ILLÉSI Zs.: Cyberhadviselés HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA XXI.:(1-2.) pp. 29-41. (2011) http://www.mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_5.pdf (letöltve: 2017.12.14.)

[16] KOVÁCS L, SIPOS M.: A Stuxnet és ami mögötte van II.: Célok és teendők HADMÉRNÖK VI:(1) pp. 222-231. (2011) http://www.hadmernok.hu/2011_1_kovacs_sipos.pdf

[17] KOVÁCS L, KRASZNAY Cs: *Mert övék a hatalom: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során*, STRATÉGIAI VÉDELMI KUTATÓ KÖZPONT (ELEMZÉSEK) / CENTER FOR STRATEGIC AND DEFENSE STUDIES ANALYSES Budapest, 2017:(9) (2017) pp. 1-11. http://archiv.netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-9-az-internet-politikat-is-befolyasolo-hatasa-a-2016-os-amerikai-elnokvalasztas-soran-kovacs-l-krasznay-cs.original.pdf (letöltve: 2018.01.15.)

[18] KLIMBURG A.: *Mobilising Cyber Power*, Survival - Global Politics and Strategy, London, 2011. pp.41-60. (letöltve: 2017.12.27.) http://users.clas.ufl.edu/zselden/coursereading2011/klimcyber.pdf (letöltve: 2018.01.15.)

[19] KRASZNAY Cs.: *A rendvédelmi szervek helye a kibervédelemben* MAGYAR RENDÉSZET XIII:(különszám) (2013) pp. 109-118. http://krasznay.hu/presentation/rendvedelem_krasznay.pdf (letöltve: 2018.01.15.)

[20] A Terek Mozgalmai – Kezdőoldal http://hu.occupy.wikia.com/wiki/Occupy-wiki (letöltve: 2018.01.22.)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

A SZEMÉLYES ADATVÉDELMI MEGFELELÉS ELLENŐRZÉSE ÉS A BEKÖVETKEZETT ADATVÉDELMI INCIDENSEK KEZELÉSÉNEK FELADATAI AZ UNIÓS SZABÁLYOZÁS KERETEIN BELÜL

CONTROL OF PERSONAL DATA PROTECTION CORRECTIONS AND TASKS OF MANAGING DATA PROTECTION INCIDENTS UNDER THE UNION REGULATORY FRAMEWORK

MÓGOR-KRÓZSER Terézia

ORCID: 0000-0002-0272-1985

mogor.krozser.terezia@uni.nke.hu

Absztrakt

A publikáció rövid áttekintést ad az Európai Parlament és a Tanács 2016/679 rendelete (a továbbiakban: GDPR /Rendelet) bevezetésével, gyakorlati megvalósításával kapcsolatos egyes kérdésekről. A cikk bemutatja a személyes adatvédelmi megfelelés ellenőrzésének lehetőségeit és a bekövetkezett incidensek kezelésének legfontosabb feladatait. A publikáció révén szeretném kihangsúlyozni, hogy az adatvédelmi jogszabályoknak való megfelelőség alapvető eszköze az ellenőrzés, melynek alkalmazásával lehetővé válik a feltárt hiányosságok korai kezelése. Mindez hozzájárulhat az adatvédelmi mulasztások bekövetkezésének megelőzéséhez vagy a bekövetkezett incidensek számának csökkentéséhez.

Kulcsszavak: *adatvédelmi szabályozás, személyes adatkezelés, adatvédelmi megfelelés ellenőrzése, incidenskezelés.*

Abstract

This publication gives a brief overview of certain issues related to the implementation and practical implementation of Regulation 2016/679 of the European Parliament and of the Council (hereinafter the "GDPR"). The article describes the possibilities of controlling personal privacy compliance and the most important tasks of managing incidents. Through the publication, I would like to emphasize that compliance with data protection legislation is a fundamental tool for control, which will enable the early management of detected shortcomings. This can contribute to preventing the occurrence of data breaches or to reduce incidents.

Keywords: *data protection, personal data management, compliance with data protection compliance, incident management.*

A kézirat benyújtásának dátuma (Date of the submission): 2018.07.08.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.26.

BEVEZETÉS

Az utóbbi évtizedek technikai és technológiai fejlődése és az elmúlt két évtizedben létrejött digitális, vezeték nélküli és vezetékes kommunikációs módok lényegesen hozzájárulnak ahhoz, hogy az emberek személyes adataikat, információikat napi rendszerességgel és bátrabban osztják meg, mint korábban. Ez a korábbinál nagyobb veszélyeket hordoz személyes adatainkkal kapcsolatos védelem vonatkozásában.

Az Európai Parlament és Tanács (EU) 2016/679 számú rendelete (a továbbiakban GDPR[1]/Rendelet) 2018. május 25-től kötelezően alkalmazott szabályozás, amely nem csak visszaadja a polgároknak a személyes adataik feletti ellenőrzést, hanem számos lehetőséget biztosít a vállalkozások terén is, így az európai polgárok és vállalkozások lehetőséget kapnak arra, hogy a digitális gazdaság nyújtotta előnyöket maradéktalanul kihasználhassák.

MIÉRT VOLT SZÜKSÉGES AZ UNIÓS ADATVÉDELMI REFORM, MILYEN ELŐNYÖKKEL JÁR?

A korábbi adatvédelmi szabályok[2] bevezetése óta több mint 20 év telt el a GDPR megalkotóinak az is célja volt, hogy a kis – és középvállalkozások adminisztrációs terheit csökkentsék, továbbá törekedtek arra, hogy a jogszabály kövesse a „kockázatalapú megközelítést”[3].

Szakértői anyagok támasztják alá, hogy a GDPR jelentős változást hoz azáltal, hogy egy, az Európai Unió egész területén egységesen alkalmazandó adatvédelmi szabályozást ír elő. Az új szabályozás biztosítja, hogy a vállalkozásoknak 28 jogszabály helyett csupán egyet kell alkalmazniuk, ami az adminisztratív terhek egyszerűsítése mellett a pénzügyi kiadások mértékét is csökkentheti[4]. Becslések szerint az új szabályok alkalmazása megközelítőleg 2,3 milliárd euro hasznot is hozhat.[1]

A financiális kiadások csökkenése mellett az új rendelet egyrészt nagyobb betekintést és jogokat biztosít a magánszemélyek részére adataik kezelésével kapcsolatban, másrészt a cégek ez irányú kötelezettségeit növeli, a mulasztásokat pedig az eddiginél jelentősebb pénzbüntetéssel sújtja. [2]

MIT ÉRDEMES TUDNI AZ ADATVÉDELMI MEGFELELÉS ELLENŐRZÉSÉNEK LEHETŐSÉGEIRŐL?

Akár a bírság, akár a kártérítési felelősség veszélye miatt az egyes vállalkozásoknak érdemes a GDPR előírásaihoz igazítaniuk a személyes adatokkal kapcsolatos működésüket, rendszereiket, folyamataikat. Ebben a fejezetben bemutatom annak lehetőségeit, hogy milyen módon ellenőrizhető saját vállalkozásunk adatvédelmi megfelelése.

Elsőként érdemes figyelmet fordítani az adatkezelésünk átvilágítására úgy, hogy feltérképezzük az összes adatbázisunkat. A teljesség igénye nélkül szeretnék kiragadni néhány fontos példát [3]:

---

[1] General Data Protection Regulation

[2] Az információs önrendelkezési jogról, és információszabadságról szóló 2011. évi CXII. törvény (Infotv.). és a 95/46/EK adatvédelmi irányelv.

[3] Ha a GDPR előírja egy vállalkozás számára az érintett jogait és szabadságait érintő kockázat felmérését, akkor a kockázat valószínűségét és súlyosságát objektív értékelés alapján, az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében kell meghatározni.

[4] A korábbi szabályozás alapján ugyanis az a cég, aki több tagállamban szeretett volna árukat eladni vagy szolgáltatást nyújtani, mindenhol meg kellett, hogy feleljen a helyi adatvédelmi szabályozásnak és hatósági követelményeknek.

- Adatkezelői szinten vizsgálni kell a munkatársak személyes adatainak munkaviszonyból eredő kezelését. Ide sorolható a munkahelyi telefonhasználat vagy e-mail tartalmak ellenőrzése, továbbá a beléptető rendszer működtetése, alkohol-drogteszt vagy a munkaviszonnyal kapcsolatos adattovábbítások.
- A legtöbb vállalkozás végez toborzási tevékenységet, mely során természetes személyek személyes adatait kezeli. A Rendelet követelményeinek értelmében az érintetteket5 előzetesen tájékoztatni kell az adatkezelés körülményeiről. Hozzájárulásuk megadása előtt tudniuk kell azt, hogy személyes adataikkal mi történik: pontosan ki kezeli, feldolgozza-e, ha igen milyen célból teszi azt, kik férnek hozzá az érintett személyes adataihoz? Szeretném kihangsúlyozni, hogy hozzájárulás nélkül még az illetékes személy nyilvános közösségi profiljáról sem gyűjthető adat.
- Adatvédelmi szempontból aggályos lehet a személyazonosító iratok másolata. Amennyiben a másolást jogszabály nem írja elő, ez a gyakorlat szükségtelen adatkezelésnek minősül, így jogellenessé válik ez a tevékenység.
- Vizsgáljunk meg egy olyan vállalkozást is, amely közvetlen üzletszerzésre is támaszkodik. Ebben az esetben is számos kérdést kell tisztázni. Lényeges, hogy cégeket vagy magánszemélyeket keres meg, milyen formában éri el az érintetteket, mert más szabályok vonatkoznak az e-mailes, a postai, és mások az sms-beni vagy telefonos megkeresésekre.
- Az előző esetekhez hasonlóan számos kérdést felvet a honlapon keresztül fogadott álláspályázatra történő jelentkezés menete, melyet Adatvédelmi Szabályzatban kell rögzíteni. Minden esetben meg kell nevezni az adatkezelés jogalapját, célját, időtartamát, címzettjeit, és az érintetti jogokat is ismertetni kell.
- Adatvédelmi szempontból fontos körülmény, hogy kinek továbbítják a személyes adatokat. Ennek vonatkozásában naprakész nyilvántartással kell rendelkezni. A GDPR szerint például harmadik országba is továbbítható személyes adat, de ebben az esetben is fontos a megfelelőség biztosítása valamint erről az érintett tájékoztatása.
- Végül egy olyan lényeges összetevőt emelek ki, amelyet a megfelelésre való felkészülés során is szem előtt kell tartani: ellenőrizni kell, hogy az adatkezelő rendelkezik-e a törvényben megkívánt valamennyi nyilvántartással. Ezek a következők: adatkezelés nyilvántartása, adattovábbítási nyilvántartás, adatkezelési tevékenység megszüntetésére irányuló érintetti kérelmek nyilvántartása, incidens nyilvántartás. Az elszámoltathatóság elvének érvényre juttatásának céljából további nyilvántartások is rendelkezésre állnak: mint például az érintetti hatósági megkeresések nyilvántartása. Ezekben a nyilvántartásokban fel tudjuk tüntetni a megkereséseket valamint azokat az intézkedéseket is, amelyeket a feltárt problémák orvoslására tettek meg.

INCIDENSKEZELÉS AZ UNIÓS SZABÁLYOZÁS KERETEIN BELÜL

Az adatvédelmi incidens[6] az adatvédelem egyik központi eleme, amelynek jelentését a GDPR az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényhez (a továbbiakban Infotv.) képest kismértékben megváltoztatta. A Rendelet 4. cikk

[5] Az a természetes személy, aki adatok útján beazonosított vagy beazonosítható.

[6] Az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

12. pont értelmében: *„Az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi”.*

Már maga a definíció is jelzi, hogy rendkívül összetett feladatot jelent az adatvédelmi incidensek megelőzése. Sajnos a kiküszöbölésre tett óvintézkedések ellenére bekövetkezhetnek incidensek, ezért a GDPR nem csak a megelőzésre, de az adatvédelmi incidensek összetett kezelésére is nagy hangsúlyt fektet. A Rendelet 33. cikkének (5) bekezdése szerint az adatkezelő nyilvántartja az adatkezelési incidenseket, feltünteti az azokhoz kapcsolódó tényeket, annak hatásait és orvoslására történt intézkedéseket. E nyilvántartás segítségével a felügyeleti hatóság ellenőrizheti a GDPR-nak való megfelelőséget. Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban Hatóság) tölti be a felügyeleti hatóság szerepét az adatvédelmi szabályok betartása felett.

A Rendelet egyértelművé teszi, hogy az adatkezelő[7] feladata az incidenskezelés, az adatfeldolgozó[8] ebben nem vesz részt, de adatvédelmi incidens bekövetkezése esetén haladéktalanul értesítenie kell az adatkezelőt.

A bekövetkezett incidens után az adatkezelőnek a Rendeletben meghatározott alábbi eljárásrendet kell követnie:

- Első lépésként meg kell határozni, hogy az incidens az érintett személyek jogára és szabadságára milyen hatással van.
- Második lépésként a bejelentést követően ne felejtsük el nyilvántartásba venni az incidenseket.
- Ezt követően az adatkezelő késedelem nélkül, de legfeljebb 72 órán belül bejelenti az incidenst a felügyeleti hatóságnak. Kivételt képez az az eset, amely során az adatvédelmi incidens vélhetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.
- A Rendeletben meghatározott eljárásrend szerint meg kell határozni az incidens bekövetkezéséhez hozzájáruló potenciális forrásokat, hiányosságokat, felelősségeket, át kell vizsgálni a vállalkozás szabályozását, IT rendszerét, vagyis lépéseket kell tenni arra vonatkozólag, hogy a jövőben az adatvédelmi incidensek megelőzhetők lehessenek.

ADATVÉDELMI INCIDENSEK SZANKCIONÁLÁSA

A GDPR az adatvédelmi kötelezettségeket, a mulasztás és jogsértés jogkövetkezményeit is jelentősen átalakította. Ez a felügyeleti eszköz nagyon rosszul érinti a vállalkozásokat. Az Infotv. szerint bírság kiszabása esetén a kiszabott bírság mértéke százezertől húszmillió forintig terjedhet. Az Infotv. szerint a hatóság figyelembe veszi az eset összes körülményét a bírság mértékének megállapításában, különös tekintettel figyel az érintettek számára, a jogsértés súlyára, valamint a jogsértés ismétlődő jellegét is mérlegeli. A hatósági gyakorlat a GDPR bevezetése előtt meglehetősen elnéző volt, az általános bírság súlyosabb esetben egymillió forint körül mozgott. Maximális bírság kiszabására csupán néhány esetben került sor.

A GDPR kötelező alkalmazása óta a szankciók köre jelentősen megváltozott. A Rendelet 58. cikke szerint a szankciók alkalmazása mind adatkezelőkre, mind adatfeldolgozókra egyaránt vonatkozik. A hatóság több módszert alkalmazhat, például figyelmeztet, elmarasztal

[7] Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az érintett személyes adatait kezeli.

[8] Az adatkezelő tevékenységét segíti, önálló rendelkezési, döntési joga az adatok felett nincsen.

vagy megtilt, emellett természetesen lehetőség van bírság kiszabására is. Bírság kiszabása esetén fontos, hogy a bírság mértéke arányos legyen az incidens mértékével, valamint megfelelő visszatartó erővel kell bírnia. A bírság kiszabása azért is kockázatos a vállalkozások számára, mert súlyos esetben elérheti a húszmillió eurot vagy a vállalkozás előző pénzügyi éve teljes világpiaci forgalmának 4%-át.

Egy 2018. 05. 29-én benyújtott törvényjavaslat szerint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény jogharmonizációs célú módosításáról szóló törvényjavaslat szerint az Infotv. a következő 75/A. §-sal egészülhet ki:

„A Hatóság az általános adatvédelmi rendelet 83. cikk (2)-(6) bekezdésében foglalt hatásköreit az arányosság elvének figyelembevételével gyakorolja, különösen azzal, hogy a személyes adatok kezelésére vonatkozó – jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott – előírások első alkalommal történő megsértése esetén a jogsértés orvoslása iránt – az általános adatvédelmi rendelet 58. cikkével összhangban – elsősorban az adatkezelő vagy adatfeldolgozó figyelmeztetésével intézkedik.”[4]

Ez alapján kiemelendő tehát, hogy a Hatóság a számára rendelkezésre álló hatásköröket az arányosság elvének figyelembevételével gyakorolja, amely azzal valósul meg, hogy a Hatóság a jogsértés első alkalmával elsősorban – az eset összes körülményére, így a jogsértés súlyára, annak ismétlődő jellegére valamint az érintetti kör nagyságára is figyelemmel – az adatkezelő vagy adatfeldolgozó figyelmeztetésével intézkedik. Az arányosság elvének alkalmazása nagymértékben segítheti a kis-és középvállalkozásokat az őket megterhelő financiális szankciók elkerülése érdekében.

KÖVETKEZTETÉSEK

Az adatvédelmi reformot követően az adatvédelmi jogszabályok 2018. Május 25 – től minden uniós országban azonosak. Ez közvetlen költségmegtakarítást és jogbiztonságot eredményez.

A szabályozás közvetlenül alkalmazandó minden olyan szervezetnél, amely személyes adatot kezel.

Az uniós rendelet hatályba lépése, az új irányelveknek való megfelelés jelentős átszervezési folyamatokat igényelt, új szervezeti változásokat követelt, új beruházások, infrastruktúra kialakítások váltak szükségessé.

A jogszabály a korábbinál szigorúbb elvárásokat támaszt az adatokat kezelőkkel, felhasználókkal szemben. Ezzel együtt sokkal nagyobb ellenőrzési lehetőséget kapnak a felhasználók saját személyes adataik és azok felhasználása felett, mint amivel korábban rendelkeztek.

A cikk segítséget nyújt a vállalkozásoknak adatvédelmi megfelelésük ellenőrzéséhez, rámutat arra is, hogyan kell eljárni egy előforduló incidens esetén, és milyen formában történhet az adatvédelmi incidensek szankcionálása.

HIVATKOZÁSOK

[1] *Az uniós adatvédelmi reform: Milyen előnyökkel jár a vállalkozások számára Európában?* Európai Unió 2016, ISBN: 978-92-79-60207-8 http://ec.europa.eu/justice/data-protection/index_en.htm Letöltés ideje: 2017. 12. 21.

[2] https://ado.hu/rovatok/cegvilág/gdpr-mire-kell-figyelni Letöltés ideje: 2017. 12. 21.

[3] *Adatvédelem a gyakorlatban* HVG Kiadó Zrt. 2018, p. 22.

[4] „*Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényjogharmonizációs célú módosításáról”*

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

A KIBERBIZTONSÁGI INFORMÁCIÓCSERE INTEROPERABILITÁSI KÉRDÉSEI

INTEROPERABILITY QUESTIONS OF CYBERSECURITY INFORMATION EXCHANGE

MUNK Sándor

(ORCID: 0000-0001-8576-308X)

munk.sandor@uni-nke.hu

Absztrakt

Napjaink társadalmi, gazdasági, és mindennapi tevékenysége egyre növekvő mértékben függ a kiberteret alkotó, globálisan összekapcsolt, decentralizált informatikai rendszerek és hálózatok által nyújtott szolgáltatásoktól.
A kiberbiztonság megteremtése és fenntartása a kiberbiztonsági szervezetek, az informatikai rendszereket, hálózatokat működtető szervezetek, az állampolgárok, és a média kiemelt jelentőségű közös feladata, amely több szereplőre kiterjedő és széleskörű együttműködést igényel.
Jelen publikáció – egy háromrészes sorozat zárásaként - a kiberbiztonsági szervezetek közötti információcsere interoperabilitási problémáit, követelményeit mutatja be, elemzi, kiemelten a kiberbiztonsági eseményekre, sérülékenységekre vonatkozó információk cseréjéhez kapcsolódóan.
A publikáció a KÖFOP-2.1.2-VEKOP-15-2016-00001 'A jó kormányzást megalapozó közszolgálat-fejlesztés' projekt támogatásával, a Kiberbiztonsági Ludovika Kiemelt Kutató-műhely keretében készült.

Kulcsszavak: *kiberbiztonság, kiberbiztonsági szervezetek, kiberbiztonsági információcsere, interoperabilitás*

Abstract

Today's social, economic, and every-day activities are increasingly dependent on the services provided by globally interconnected, decentralized IT systems and networks, the cyberspace.
Ensuring cyber security is a common task of cybersecurity organisations, IT system-network operators, citizens, and media, which requires wide range, extensive cooperation of these actors.
Recent paper – as a closing part of a three-part series - presents and analyses interoperability problems and requirements for information exchange between cyber security organizations, especially for cyber security events and vulnerability information.

Keywords: *cybersecurity, cybersecurity organisations, cybersecurity information exchange, interoperability*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.03.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.20.

BEVEZETÉS

Napjaink társadalmi, gazdasági, és mindennapi tevékenysége egyre növekvő mértékben függ a kiberteret alkotó, globálisan összekapcsolt, decentralizált informatikai rendszerek és hálózatok által nyújtott szolgáltatásoktól. Az informatikai szolgáltatások egyre jelentősebb mértékben járulnak hozzá az állami működés hatékonyságának, a vállalkozások eredményességének és versenyképességének, valamint az állampolgárok életminőségének javításához. A növekvő függőség egyben növekvő kiszolgáltatottságot, kockázatot is jelent, mivel az informatikai rendszerek, hálózatok, és az általuk kezelt adatok, információk biztonságának (bizalmasságának, sértetlenségének, és rendelkezésre állásának) megsértése maga után vonja az informatikai szolgáltatásokra épülő rendszerek, folyamatok, szolgáltatások biztonságának sérülését is, ami jelentős kihatással lehet az átfogó biztonság politikai, katonai, gazdasági, pénzügyi, és társadalmi dimenzióira is.

A kibertérben világszerte növekvő mértékben jelentkező kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a nemzeti kritikus infrastruktúra működtetésének biztosítására minden államnak, így – Magyarország Nemzeti Biztonsági Stratégiájában megfogalmazottak szerint – hazánknak is készen kell állnia. A kiberbiztonság megteremtése és fenntartása nem csak a kiberbiztonsági (információbiztonsági, informatikai biztonsági) szervezetek, hanem az informatikai rendszereket, hálózatokat működtető szervezetek, az állampolgárok, és a média kiemelt jelentőségű feladata.

A kibertér informatikai rendszereinek, hálózatainak globális, szövevényes összekapcsolódása következtében az egyik rendszer biztonságának sérülése elvezethet egy másik (más országban, más ágazatban működő) rendszer biztonságának sérüléséhez. Egy magán vállalkozás által üzemeltetett informatikai infrastruktúra támadásával támadhatóvá válnak az infrastruktúra szolgáltatásait igénybevevő kormányzati, gazdasági, és más informatikai rendszerek is. Az Internet lényegében bárhonnan könnyű útvonalat biztosít kibertámadások, kiberbűncselekmények végrehajtásához. Mindebből következik, hogy a kiberbiztonság fenntartása több szereplőre kiterjedő és széleskörű együttműködést igényel.

Jelen publikáció egy szélesebb körű, a kiberbiztonsági szervezetek információcsere igényeit, és az ehhez kapcsolódó interoperabilitási követelményeket vizsgáló kutatás harmadik részét képezi. Az elsőben rendszerezésre kerültek a kiberbiztonsági szervezetek főbb típusai, és ezek funkciói, feladatai. A második pedig a kiberbiztonsági szervezetek által kezelt, illetve a köztük áramló információk, és az információcsere alapvető jellemzőit tárgyalta.

Ezen publikáció célja a kiberbiztonsági szervezetek közötti információcseréhez kapcsolódóan felmerülő interoperabilitási problémák, követelmények bemutatása, elemzése, annak vizsgálata, hogy az információcserében érintett felek között milyen területeken vannak eltérések, amelyek – megfelelő megoldás alkalmazása nélkül – megnehezítik, vagy lehetetlenné teszik a jelentésmegőrző információcserét. Ennek érdekében a következőkben:

- összegezzük az interoperabilitás alapjait, a jelen publikációban is felhasznált legfontosabb fogalmait, állításait, majd megvizsgáljuk ennek a kiberbiztonsági információcserére vonatkozó sajátosságait;
- röviden értékeljük az interoperabilitás helyzetét a kiberbiztonsági információcsere során, és meghatározzuk jövőbeni alakulásának néhány lehetséges irányát;
- végül általában, illetve a két kiemelt információkörre vonatkozóan elemezzük az interoperabilitási követelményeket és a legfontosabb, megoldásra váró problémákat.

AZ INTEROPERABILITÁS ALAPJAI

Az interoperabilitás korunk népszerű, megkerülhetetlen szakkifejezése, amelynek jelző nélküli és jelzős változataival széles körben találkozhatunk. Bár e kifejezések értelmezéseiben sok a

közös, de számos eltérés is tapasztalható. A következőkben bemutatjuk az interoperabilitás jelen publikációban alkalmazott fogalmi alapjait, amelyek alapvetően egy korábbi publikációnkban [1] foglaltakra épülnek.

Az ***interoperabilitás*** általános értelemben együttes tevékenységre (működésre) való kölcsönös képesség. Az együttes tevékenység (együttműködés) értelmezhető tudatosan tevékenykedő szereplők (emberek, szervezetek), vagy meghatározott rendeltetéssel működő technikai rendszerek (eszközök, részegységek) között. Az előbbihez kapcsolódik a szervezeti/működési interoperabilitás fogalma, ami egyeztetett cél megvalósítása érdekében együttműködő szereplők között fennálló viszony, az eredményes és hatékony együttműködést biztosító átfogó, kölcsönös képesség, míg az utóbbit technikai interoperabilitásnak nevezzük. A szervezeti/működési interoperabilitás megvalósítása számos részterületen fennálló interoperabilitást igényel, ezek egyike – mivel együttműködés nem lehetséges információcsere nélkül – az információs interoperabilitás.

Az *információs interoperabilitás* különböző szereplők kölcsönös képessége információk közös értelmezésen alapuló, a hatékony együttműködéshez szükséges cseréjére. A meghatározásból láthatóan az információs interoperabilitás két alapvető összetevője az információcserére való képesség, és a kicserélt információk közös értelmezésére való képesség. Ezekhez kapcsolhatóak a nyelvi interoperabilitás, fogalmi interoperabilitás, és szellemi interoperabilitás fogalmai is.

Az információk közös értelmezésén alapuló cseréjére vonatkozó képesség ***három, egymásra épülő információs interoperabilitási szintre*** tagolható, amelyek a következők:

- az anyagi (fizikai) információ reprezentációkhoz kapcsolódó technikai;
- a logikai információ reprezentációkhoz (adatokhoz) kapcsolódó szintaktikai;
- valamint az információ reprezentációk jelentéséhez kapcsolódó szemantikai.

A legalsó szintet a *technikai szintű információs interoperabilitás* képezi, amely az információt hordozó anyagi (fizikai) reprezentációk cseréjére – előállítására, továbbítására, fogadására, megjelenítésére – vonatkozó képességek összessége. Ennek feltétele az adott fizikai reprezentációnak megfelelő, egymással "interoperábilis" technikai eszközök[1] megléte és rendeltetésszerű működése.

A *szintaktikai szintű információs interoperabilitás* az információkat hordozó adatok cseréjére vonatkozó képességek összessége, amelynek lényege az alkalmazott adatcsere formátumok előírásainak megfelelő[2] adatok kezelésére – előállítására, a technikai szint szolgáltatásaira épülő továbbítására, fogadására, és formai feldolgozására – vonatkozó képesség.

Az informatikai eszközök segítségével történő információcsere esetében az információk reprezentációi (adatok) bonyolult, egymásra épülő struktúrát alkotnak, amelynek alapja, elemi szintje napjainkban a bitsorozat, bitfolyam. Erre épülnek – akár több szinten – az információcsere során alkalmazott adat- és üzenetformátumok. Ennek feltétele az alkalmazott formátumokat kezelni képes szoftver összetevők megléte, és rendeltetésszerű működése.

Végül a *szemantikai szintű információs interoperabilitás* a legfelső szint, amely különböző szereplők kölcsönös képessége a hatékony együttműködéshez szükséges információ-reprezentációk – esetleges átalakítások közbeiktatásával történő – jelentésmegőrző cseréjére. Az együttműködő felek közötti információcsere során az információkat egyezményes jelrendszernek

[1] Vezetékes, vagy vezetéknélküli adatátviteli eszközök, adathordozók előállítására (írására) és felhasználására (olvasására) alkalmas berendezések.

[2] Pld. bináris, vagy karakteres számformátumok; karakterkészletek; dokumentum formátumok; hang-, kép-, video formátumok; formatizált üzenetformátumok, stb.

megfelelő adatokká kell alakítani, így továbbíthatóak, és a fogadónál az adat értelmezése során áll elő a továbbítani szánt információ.

A szemantikai szint lényege az információcsere során használt adatokhoz rendelt jelentés együttműködéshez szükséges mértékben azonos értelmezése. Vagyis hogy ugyanazon adathoz minden szereplő ugyanazt a jelentést rendelje[3], és azonos információkat azonos adatok formájában jelenítsen meg. Az adatok szándékolt, egyeztetett jelentésének feltétele a felek fogalomrendszerének kellő szintű azonossága, legalább harmóniája, ami ki kell terjedjen az adatcsere során közvetlenül nem is használt fogalmakra, információkra (pld. incidens, káros, alárendeltje, stb.)

Érdemes kihangsúlyozni, hogy az információs interoperabilitás és különböző szintjei vizsgálatának igazából csak akkor van jelentősége, kialakítására és fenntartására akkor van csak szükség, ha az együttműködő szereplők között valamilyen szempontból ***heterogenitás (különbözőség)*** áll fenn. Szervezetek, emberek közötti információcsere esetében ez a heterogenitás – a szinteknek megfelelően – fennállhat a közös (azonos) értelmezés, az alkalmazott adatformátumok, vagy a rendelkezésre álló technikai adatcsere lehetőségek hiányában, vagy ezek együttműködés szempontjából nem elégséges minőségében, szintjében.

Az ***informatikai interoperabilitás*** az információs interoperabilitáshoz kapcsolódó sajátos, informatikai eszközök, rendszerek között fennálló, az általuk kezelt adatok szándékolt jelentésüket, értelmezésüket megőrző - esetleges átalakítások közbeiktatásával történő – cseréjére vonatkozó kölcsönös képesség. Szerepe azzal született meg, hogy a szereplők már nem feltétlenül (egyes körülmények között nem is elsősorban) közvetlenül cserélnek információt egymással, hanem közvetve, akár kezdeményezésük, tudomásuk nélkül informatikai eszközeiken, rendszereiken keresztül. Erre példa lehet közzétett információk lekérdezése egy szereplő informatikai rendszeréből, vagy informatikai rendszerek közötti automatizált – ütemezett, vagy feltételek bekövetkeztétől függő, kötött, vagy dinamikusan változó tartalmú – adatcsere.

Az informatikai interoperabilitás alapja az informatikai rendszerek által kezelt adatok szándékolt jelentése, aminek megőrzése, átvitele a cél. Ez azonban a szemantikus technológiák, az információk (adatok) jelentésére vonatkozó meta-információk (meta-adatok) alacsonyabb elterjedtsége miatt napjainkban még nem könnyen adható meg, ismerhető meg[4]. Azonban a gyakorlatban, az együttműködés során az eltérő értelmezések jó része napvilágra kerül.

Az együttműködő, információt cserélő felek közötti információs heterogenitás, eltérések interoperabilitási problémákként merülnek, merülhetnek fel[5], amelyekre ***interoperabilitási megoldást*** kell találni. Az interoperabilitási problémák egyik lehetséges, napjainkban leggyakrabban alkalmazott megoldása a *szabványosítás*: a széles körben, vagy egy adott alkalmazási körben elfogadott szabványos megoldások alkalmazása. Ez kiküszöböli a különbözőségeket, minden fél a szabványos megoldást (pld. besorolási rend, kódrendszer, mértékegységek, stb.) alkalmazza. A megoldás feltétele a szabvány megléte, a teendő a szabvány alkalmazása a saját tevékenység során, a saját informatikai rendszerben.

A szabványosítás azonban nem minden esetben jelent megoldást, a heterogenitás nem mindig küszöbölhető ki, vagy nem célszerű kiküszöbölni. Ebben szerepet játszhat a szabványosítás,

---

[3] A gyakorlatban a fogadó félnél a kapott adat értelmezésével általában nem pontosan a küldött információ, a szándékolt jelentés áll elő, de erre nincs is szükség, mert elegendő az együttműködéshez elegendően pontos értelmezés, tartalom.

[4] Mindenkinek lehetnek személyes tapasztalatai egy adatbázisban, vagy formatizált üzenetben szereplő adatok értelmezési problémáiról (pld. a hőmérséklet Fahrenheit, vagy Celsius, a név tartalmazza-e valamennyi utónevet, stb.).

[5] Annak eldöntése, hogy ezek a különbözőségek, eltérések az együttműködést, és az ahhoz szükséges tartalmú és minőségű információcserét akadályozó, nehezítő jellegűek-e, az érintett felek joga, lehetősége.

illetve a szabvány szükséges módosításainak előzetes egyeztetés- és időigénye, illetve a szabvány, vagy annak változásai átvezetésének feladata a már meglévő informatikai rendszerekben. Az információs interoperabilitás esetében a szabványosítás sokkal könnyebben valósítható (és ahogy látható valósul is meg) a technikai és a szintaktikai szinten, mivel az alkalmazás szintjét ez – amennyiben korlátozásokkal nem jár – közvetlenül nem érinti.

Jóval nehezebb a szabványosítás, esetenként nem is kivitelezhető a szemantikai szinten. Ehhez ugyanis az szükséges, hogy az információcsere során alkalmazott fogalomrendszer minden szereplő számára egységesen elfogadható, alkalmazható legyen. Értelemszerűen a szabványosítás könnyebb tartós együttműködésben álló, azonos, vagy hasonló jellegű szereplők között, mint lazább együttműködésben lévő, eltérő szakterületekhez tartozó szereplők között. Az egyes szereplők fogalomrendszere ugyanis a szakterületük, feladataik igényeihez igazodó, amely általában szerves fejlődés eredményeként alakult ki, és megváltoztatása csak alapvető körülmények módosulása esetében és akkor is csak hosszabb idő alatt lehetséges.

Amennyiben a szabványosításra teljes körben nincs lehetőség, az interoperabilitás megvalósítására a közbenső átalakítások, *egyeztetett (adatszintű) közvetítő reprezentáció alkalmazása* ad lehetőséget. Ennek lényege, hogy minden együttműködő fél megtartja a saját (belső) fogalomrendszerét, adat-, esetleg üzenetformátumait, azonban ezeket információ küldése során átalakítja az egyeztetett közvetítő reprezentációra, illetve információ fogadása esetén az egyeztetett közvetítő reprezentációból átalakítja a saját belső formátumára. Ezzel az interoperabilitás – a tartalmi feltételek megléte esetén (pld. a továbbítandó információ valamilyen formában rendelkezésre áll a rendszerben) – az informatikai rendszerek módosítása nélkül is megvalósítható.

A KIBERBIZTONSÁGI INFORMÁCIÓCSERE INTEROPERABILITÁSÁNAKALAPJAI

Az interoperabilitási kérdések, problémák, követelmények, megoldások minden olyan területen vizsgálhatóak, ahol az együttműködő felek egymással információt cserélnek, nincs ez máshogy a kiberbiztonsági szervezetek közötti információcsere esetében sem. Alkalmazási területenként, szakterületenként, vagy információkörönként is eltérhet azonban az interoperabilitási kérdések szerepe, jelentősége, és eltérhetnek az interoperabilitási problémák, az elért interoperabilitási szintek következményei. A következőkben ezeket a kérdéseket elemezzük a kiberbiztonsági szervezetek közötti információcseréhez kapcsolódóan.

Az ***interoperabilitás szerepe, jelentősége a kiberbiztonsági szervezetek közötti információcserében*** ezen szervezetek rendeltetéséből, jellegéből vezethető le. A kiberbiztonsági eseménykezelő központok egy nézőpontból olyan tudás-intenzív szervezeteknek tekinthetőek, amelyek az ügyfélkörükbe tartozó szervezetek terheit csökkentik, az ügyfeleik által üzemeltetett informatikai rendszerek, hálózatok biztonsága megőrzésének eredményességét és hatékonyságát növelik.

Elvileg az egyes üzemeltető szervezetek informatikai és hálózatbiztonsági szerveinek önállóan is képesnek kell lenniük a biztonság fenntartására, a sérülékenységekre, és bekövetkezett incidensekre vonatkozó információk begyűjtésére, és ennek alapján a szükséges tevékenységek rendszabályok megvalósítására (akkor is, ha nincs őket támogató kormányzati, ágazati, vagy más kiberbiztonsági eseménykezelő központ), azonban ehhez jellemzően korlátozottabbak a kapacitásaik, illetve az információhoz jutási lehetőségeik.

A kiberbiztonsági eseménykezelő központok tevékenységüket – elsősorban a biztonsági események kezelése területén – eredményesen csak *egy eseménykezelő központ hálózat részeként*, a hálózat többi elemeivel szoros együttműködésben, egymás kölcsönös informálásával képesek végezni. Ennek hiányában csak a támogatott szervezeteikre vonatkozó eseményinformációkra támaszkodhatnának, azonban a globálisan összekapcsolt kibertérben a kiberbiztonsági fenyegetések számára a szervezeti határok nem léteznek, és a hálózati határok (még elkülönült hálózatok esetében) sem átjárhatatlanok.

A kiberbiztonsági eseménykezelő szervezetek szerepe azonban *nem elsősorban az egyszerű információ elosztás, továbbítás* (nem lehetnek kéretlen levélküldők). Ezzel kibővítik ugyan a támogatott szervezetek információs lehetőségeit, de nem vesznek le terheket a vállukról, sőt növelik azokat. Alapvető szerepük a beérkező – akár incidensekre, akár sérülékenységekre vonatkozó – információk szűrése, ellenőrzése, összevetése, szintetizálása, majd ezt követően az érintett támogatott szervezetek kiválasztása, és azok közvetlenül felhasználható, tevékenységet igénylő (az ENISA szóhasználatával 'actionable') információkkal történő ellátása.

Mindezen feladatok ellátásához a kiberbiztonsági eseménykezelő szervezeteknek széleskörű, megbízható, és egyértelműen értelmezhető információkra van szükségük. És bár új kiberbiztonsági információkat esetenként – például lefolytatott sérülékenység vizsgálatok, vagy tárgyi leletek vizsgálatának eredményeképpen – maguk is állíthatnak elő, tevékenységük alapját a szervezeten kívülről érkező információk, bejelentések, tájékoztatások, riasztások adják. Ebből következően az információk együttműködő partnereikkel, támogatott szervezeteikkel közös értelmezésen alapuló cseréjére vonatkozó képességeik, a velük fennálló információs interoperabilitásuk szerepe, jelentősége kiemelkedő.

Az ***információs interoperabilitás hiányának, alacsonyabb szintjének következményei*** számos formában megjelenhetnek, amelyeket az interoperabilitási követelmények meghatározása során, elsősorban az információkat fogadó fél szempontjából, figyelembe kell venni. Amennyiben egy adott információkörre vonatkozóan, vagy adott együttműködő partnerekkel egyáltalán nem biztosítható az interoperabilitás, az azt jelenti, hogy bár rendelkezésre állnak elvileg elérhető információk, azok nem férhetőek hozzá a fogadó számára, vagyis tevékenységét *kevesebb információ* birtokában képes végezni.

Az alacsonyabb szintű interoperabilitás, amikor az információ forrásától kapott, vagy az általa megosztott, hozzáférhetővé tett információt hordozó adatok formátuma eltér a fogadó fél által alkalmazott formátumtól (legyen ez elektronikus, vagy hagyományos), vagy amikor az információ értelmezése tér el a fogadó fél értelmezésétől, mindenképpen *többletmunkát* igényel: az eltérő formátumot át kell alakítani, az értelmezési különbségeket fel kell oldani.

Azon túl, hogy a többletmunka nem gazdaságos, okozhat *időbeniségi problémát* is. A beérkező információk lassabb feldolgozása egyes esetekben beleférhet a kiberbiztonsági szervezetek előírt minőségű eljárásrendjébe, azonban más esetekben – például súlyos minősítésű biztonsági események kezelése, vagy súlyos fenyegetésekről történő értesítések kiadása során – a tevékenység kicsúszhat az elvárt időkeretekből, amelynek következménye több károkozás is lehet.

Az interoperabilitás alacsonyabb szintje járhat olyan következménnyel, hogy az információk tartalma, teljessége, pontossága sérül. Ennek káros volta nem igényel különösebb indoklást, kiemelendő azonban a több szereplőn keresztül áramló információk minőségének folyamatos romlása, akár az egyes szereplők számára releváns érdemi információtartalom elvesztése is. Incidens bejelentések esetében ennek egy megoldási lehetősége lehet például a kiberbiztonsági szervezet által alkalmazott formátum mellett az eredeti bejelentés továbbítása is.

A KIBERBIZTONSÁGI INFORMÁCIÓCSERE INTEROPERABILITÁSÁNAK HELYZETE, JÖVŐJE

A kiberbiztonsági szervezetek között történő információcsere megvalósítási módjait folyamatos változások, új megoldások megjelenése és elterjedése jellemzik. Ez a folyamat még csak a fejlődési pálya kezdeti szakaszában van, amely a 'hagyományos' információcsere megoldásoktól a kiberbiztonsági szervezetek által alkalmazott informatikai rendszerek közötti automatizált információcseréig terjedhet. Természetesen ez utóbbira csak a biztonsági szempontok, a minősített információk kezelésére vonatkozó szabályok, a szervezeti információ-megosztási politikák keretei között, az adott szervezet mindenkori felügyelete alatt kerülhet majd sor.

A következőkben röviden összegezzük, elemezzük a kiberbiztonsági szervezetek közötti információcsere interoperabilitásának jelenlegi helyzetét, és tervezett, vagy várható jövőbeni irányait. A helyzet értékelése során csak röviden, szemléltetésképpen mutatjuk be a kapcsolódó interoperabilitási megoldásokat, mert ezek részletes vizsgálata egy későbbi kutatás tárgyát képezi. A helyzet, és a jövőbeni irányok vizsgálatát az információs interoperabilitás 'könnyebben megvalósítható' technikai és szintaktikai, illetve 'jelentősebb feladatot képező' szemantikai szintjére tagoljuk.

Előzetesen szükséges kiemelnünk azt a tényt, hogy az interoperabilitás, és annak bármely szintje kölcsönös – két, vagy több fél között fennálló (vagy hiányzó) – képesség, vagyis egy kiberbiztonsági szervezet interoperabilitásának helyzete csak a partnereivel fennálló információcsere kapcsolatok konkrét interoperabilitási viszonyainak együtteseként értékelhető. Egyes szervezetekkel magas szintű, másokkal közepes, vagy alacsony szintű lehet az interoperabilitás[6], amiből előállítható egy összegzett interoperabilitási értékelés is.

A kiberbiztonsági információcsere technikai és szintaktikai interoperabilitási kérdései az alkalmazott fizikai adatátviteli megoldásokhoz, valamint adatcsere formátumokhoz kapcsolódnak. A – változatlanul szerepet játszó – hagyományos információcsere megoldásokkal jelen publikációban nem foglalkozva a ***technikai interoperabilitás*** megítélésének alapja napjainkban az, hogy van-e adatátvitelt biztosító hálózati kapcsolat az információcserében érintett felek között, vagy csak adathordozók cseréjével oldható meg az információcsere. A hálózati kapcsolat ugyanis gyakorlatilag egyet jelent a szinte kizárólagos szerepet betöltő IP-alapú kapcsolattal, ami minden informatikai eszköz képességei között megtalálható. Így a technikai interoperabilitás általában minden partnerrel alapszinten biztosított.

A technikai interoperabilitás körébe tartozik megítélésünk szerint a *védett adatátvitel* képessége is, mivel a kiberbiztonsági információk (az ezeket hordozó adatok) nyilvánossága lehet korlátozott, illetve ezek az információk lehetnek minősítettek is. Ennek megfelelően két fél között, vagy felek egy együttműködő körén belül a technikai interoperabilitás helyzete lehet: nincs közvetlen adatátviteli lehetőség, nyílt adatátviteli lehetőség van, nyílt és védett adatátviteli lehetőség is van.[7]

Összességében megállapítható, hogy a kiberbiztonsági szervezetek közötti technikai interoperabilitás – a védett összeköttetés esetleges problémáitól eltekintve – napjainkban alapvetően adott, nem jelent problémát, és ilyen a jövőben sem várható. A technikai interoperabilitás kialakítása és fenntartása – nevének megfelelően – a kiberbiztonsági szakterülettől független, technikai kérdés.

A ***szintaktikai interoperabilitás*** megítélésének alapja a különböző adatformátumok fogadására, hasznosítására, illetve előállítására való képesség. Ezen belül jelentős csoportot képeznek – és várhatóan a jövőben sem tűnnek el – a *strukturálatlan (jellemzően szabad szöveges) adatok*, amelyek kezelése bonyolult szintaktikai feladatot nem igényel. Ezekhez kapcsolódóan interoperabilitási kérdésként egyrészt az alkalmazott karakterkészlet, másrészt az alkalmazott nyelv merül fel. Az eltérő karakterkészletek kezelése az alkalmazott alap- és alkalmazói szoftverek szolgáltatása kell legyen. A Unicode karakterkészlet elterjedésével ennek az interoperabilitási problémának a jelentősége folyamatosan csökken.

A nyelvi interoperabilitás megvalósítása napjainkban még alapvetően felhasználói, humán feladat, de a jövőben várhatóan megjelennek majd gépi fordítási megoldások. Megjegyzésre

[6] Az interoperabilitás szintjének meghatározására, értékelésére különböző interoperabilitási érettségi modellek, interoperabilitási skálák léteznek (lásd pld. [2])

[7] Ez a besorolás nem kiberbiztonsági szervezetek közötti információcserére specifikus.

érdemes, hogy a gépi fordítás az emberi "fordításhoz" hasonlóan lehetséges azonos nyelv, de eltérő szakmai, kiberbiztonsági terminológia – eltérő szaknyelvek (?) – esetében is.

A strukturálatlan adatok hasznosítása során a jövőben megjelenhet a természetes nyelvi feldolgozás eszköztára is, amely a szabad szövegből (például egy incidens bejelentésből), strukturált adatok együttese formájában képes kiemelni a kiberbiztonsági szervezet számára fontos információkat, sőt ezekre építve besorolásokat is készíthet, jelzéseket, riasztásokat is kiadhat.

A szintaktikai interoperabilitás szempontjából köztes csoportot képeznek a *félig strukturált adatok*, amelyek meghatározott struktúrába rendezett szabad, vagy bizonyos szabályoknak eleget tevő szöveges összetevőkből épülnek fel. Ilyen például szinte valamennyi sérülékenység leírás[8]. Nyilvánvalóan a szintaktikai interoperabilitás eltérő szintjét jelenti az, ha az adott kiberbiztonsági szervezet ezeket a leírásokat 'olvasni' és szövegként 'írni' tudja, vagy ha ezeket képes feldolgozni, strukturált (adatbázisba tárolásra alkalmas, vagy formatizált üzenet) formába alakítani, illetve strukturált formából a félig strukturált formátumot automatizáltan előállítani.

A szintaktikai interoperabilitás *strukturált adatok* esetében a formatizált üzenetekben, valamint az adatbázisokban tárolt információkhoz, illetve az ezeket kezelni képes szoftver megoldásokhoz kapcsolódik.[9] Az interoperabilitás fennállásáról akkor beszélhetünk, ha az adott szervezet megfelelő informatikai rendszere, alkalmazása képes:

- meghatározott formátumú üzeneteket fogadni, formai szempontból feldolgozni, a benne szereplő adatokat szükség esetén a szervezet által alkalmazott formára átalakítani, és ilyen üzeneteket a rendelkezésére álló adatok alapján előállítani;
- illetve kiberbiztonsági információkat együttműködő felek által hozzáférhetővé tett adatbázisból lekérdezni, a lekérdezett adatokat szükség esetén a szervezet által alkalmazott formára átalakítani, és kiberbiztonsági információkat meghatározott felépítésű, tartalmú adatbázisban mások számára hozzáférhetővé tenni.

A kiberbiztonsági információcsere szintaktikai kérdéseinek legnagyobb része a különböző egyeztetett, *szabványos üzenetformátumokhoz*[10] kapcsolódik. Az üzenetformátumok kezelésére vonatkozó képességek két szintre bonthatóak: a keretet képező általános adatcsere formátum, valamint az erre épülő kiberbiztonsági üzenetformátum kezelésének képessége. Az előbbi területén napjainkra egyeduralkodóvá vált az XML[11] formátum, amelynek kezelése a fizikai adatátvitel IP megoldásához hasonlóan az informatikai rendszerek, eszközök képességei között megtalálható, így ennek alkalmazása esetén interoperabilitási probléma jellemzően nem merül fel.

A kiberbiztonsági információcserében azonban léteznek jelentős üzenetszabványok, amelyek nem XML alapra, hanem például JavaScript-hez kapcsolódó JSON adatcsere formátumra[12] épülnek. Ebben az esetben természetesen biztosítani kell az ezen formátum kezeléséhez szükséges szoftver összetevőket is (ami ebben az esetben szintén általában infrastrukturális szinten rendelkezésre áll).

A speciális kiberbiztonsági üzenetformátumokhoz kapcsolódó szintaktikai interoperabilitási képesség, amennyiben az alapját képező általános adatcsere formátum kezelésének képessége

[8] Lásd például a MITRE cég, vagy a Kormányzati Eseménykezelő Központ által közreadott sérülékenység listákat.
[9] Sok esetben szintaktikai interoperabilitásról erre az értelmezésre leszűkítve beszélnek.
[10] Ezek az üzenetformátumok a kiberbiztonsági információcsere esetében szinte kizárólag karakteres típusúak.
[11] Az eXtensible Markup Language, Kiterjeszthető Jelölő Nyelv.
[12] JavaScript Object Notation (JSON), amelyre épül például a fenyegetések, leírására alkalmas nyelv (Structured Threat Information Expression, STIX).

meg van, viszonylag egyszerűnek nevezhető szoftver fejlesztési feladat. Az adott üzenetformátumhoz így kialakítható egy olyan interfész, amely az üzenetből további feldolgozásra, tárolásra, megjelenítésre alkalmas formában képes kiemelni a kiberbiztonsági információkat hordozó egyes adatelemeket, illetve a rendelkezésre álló adatokból képes összeállítani az üzenetformátum szabványnak megfelelő üzenetet.

A ***szemantikai interoperabilitás*** a kiberbiztonság területén is az interoperabilitás kialakításának és fenntartásának, a jelentésmegőrző információcsere biztosításának kulcskérdése. Az együttműködő feleket nem a kiberbiztonsági információk cseréje során alkalmazott fizikai, és adatformátumok érdeklik, érintik, hanem az ezek segítségével továbbított, ezek által hordozott információk. Szemantikai interoperabilitási feladat akkor jelentkezik, amikor az információt cserélő felek eltérő fogalomrendszereket használnak, eltérés van köztük az adatok értelmezésében, vagy a közös környezet ugyanazon dolgait különböző módon modellezik. Amennyiben ugyanis ezek megegyeznek, a technikai és szintaktikai megoldások könnyen megtalálhatók, az alkalmazói szintet érdemben nem is befolyásolják.

A szemantikai interoperabilitás megvalósításának kiinduló feltétele az egyes felek által használt fogalmak pontos definiálása, ami magában foglalja az érdeklődésre számot tartó dolgokra, a dolgokat leíró tulajdonságokra, valamint a dolgok között fennálló kapcsolatokra vonatkozó fogalmak definiálását. Együttműködés esetében meg kell állapodni az információcsere hátterében álló, egyeztetett, egyértelműen definiált fogalomrendszerben, ami kisebb, vagy nagyobb mértékben eltérhet az egyes felek saját fogalomrendszerétől. Ebben az esetben az érintett felek feladata a saját fogalomrendszerről a közvetítő (információcsere) fogalomrendszerre történő, illetve az ellenkező irányú átalakítás megvalósítása. A feladatot nehezíti, hogy egy szereplő több együttműködési kör része is lehet, így többféle átalakítást kell biztosítania.

Az együttműködő felek, vagy a felek és a közvetítő fogalomrendszer közötti *szemantikai eltérések típusai* között kiemelt szerepet játszhatnak a következők:

- terminológiai eltérések (azonos dolgok eltérő módon, különböző dolgok azonos módon történő megnevezése);
- alapfogalmak tartalmának eltérései (ugyanazon dolgokhoz pld. biztonsági eseményhez szűkebb, vagy tágabb tartalom rendelése);
- kategorizációs eltérések (dolgok kategóriákba sorolása eltérő részletességgel, vagy egymással nem teljes mértékben összehangolható módon);
- értékkészlet eltérések (dolgok ugyanazon tulajdonságának leírása eltérő módon);
- kapcsolatok eltérései (dolgok közötti kapcsolatok leírása eltérő módon, vagy eltérő részletezettséggel).

A szemantikai interoperabilitási problémák és megoldásaik a kiberbiztonságban az eseménykezelő szervezetek közötti szervezettebb együttműködés, információcsere kialakulásához kapcsolódóan már megjelentek. Elsőként, és azóta is elsősorban a kategorizációs, besorolási eltérések feloldását szolgáló *kötött értékkészletek, taxonómiák* kialakítása jelentette és jelenti a szemantikai interoperabilitás megvalósításának eszközét. A 2000-es évek elején már megjelentek javaslatok szabványos kiberbiztonsági információcsere formátumokra, azonban ahogy azt egy 2006-os ENISA tanulmány is megfogalmazta, a legnagyobb információ megosztási problémát a felek által alkalmazott eltérő taxonómiák, osztályozási rendszerek képezték. [3, 28. o.] Azóta különböző célú taxonómiák, kötött értékkészlet listák sora jelent meg, amelyek közül egyesek szélesebb, mások szűkebb körben kerülnek alkalmazásra.

A jövőben is várhatóan több kiberbiztonsági besorolási rend marad alkalmazásban, így a feladat ezek lehetséges mértékű összehangolása, illetve a jelentésmegőrző átalakítás biztosítása köztük. Az 'egyszerű' taxonómiák mellett várhatóan megjelennek, és előtérbe kerülnek a fogalomrendszerek formalizált leírását biztosító ontológiák, valamint az ezekre épülő szemantikus szolgáltatások, funkciók (pld. automatikus átalakítás fogalomrendszerek között).

KIBERBIZTONSÁGI ESEMÉNYEKHEZ KAPCSOLÓDÓ INTEROPERABILITÁSI KÖVETELMÉNYEK, PROBLÉMÁK

Mint azt egy előző publikációban már tárgyaltuk, a kiberbiztonsági szervezetek információkat tárolnak, kezelnek, és használnak fel a felügyeletük alá tartozó, általuk támogatott szervezetek kiberbiztonsági eseményeiről. Ezen információk egy részét különböző együttműködő partnereknek is továbbítják jelentési/tájékoztatási kötelezettség, figyelmeztetés, további teendők végrehajtása céljából, illetve ilyen információkat fogadnak együttműködő partnerektől hasonló okokból.

A kiberbiztonsági szervezetek eredményes és hatékony működésének alapvető feltétele, ***általános interoperabilitási követelménye***, hogy az együttműködő partnereknek képesek legyenek kiberbiztonsági eseményekre vonatkozó információkat megküldeni az előírt/egyeztetett formában és tartalommal, illetve a partnerektől képesek legyenek ilyen információkat fogadni, megfelelő módon értelmezni, és feldolgozni, hasznosítani. Mindez kiterjedt együttműködési kapcsolatokkal rendelkező szervezet számára – eltérő adatcsere formátumok esetében – több önálló interoperabilitási követelményt jelent.

A kiberbiztonsági eseményekhez kapcsolódó ***információk az interoperabilitási eltérések szempontjából*** három csoportba oszthatóak. Az első azon információk csoportja, amelyeknek az együttműködő felek által használt *tartalma és formátuma érdemben nem tér el*.[13] A korábbi publikációban bemutatott információk közül ilyenek a következők:

- bejelentő neve, elérhetőségei, képviselt szervezete;
- észlelés, bekövetkezés, befejeződés (stb.) időpontja, helyreállítás várható időtartama;
- hálózati azonosítók (IP címek, nevek);
- hatások mennyiségi jellemzői, a kár becsült összege.

A második csoportot azon szakterület, kiberbiztonság specifikus információk alkotják, amelyek *tartalma, értelmezése azonos, de formája eltér*. Ide a kiberbiztonsági események információi közül a földrajzi helyek, valamint az operációs rendszer platform, és alkalmazott javítócsomagok azonosítása tartoznak.

Végül a harmadik csoportba azon információkat sorolhatjuk, amelyek esetében az együttműködő felek között *szemantikai, értelmezési eltérések* állnak fent. Ezek elsősorban: az esemény osztályozása; az esemény által érintett összetevő típusa; az érintett összetevő rendeltetése; és az esemény hatásának mértéke (a szolgáltatásokra, illetve a kezelt információkra).

A következőkben sorra vesszük a harmadik csoportba tartozó ***információk interoperabilitási problémáit***. Ezek között kiemelt szerepet *a kiberbiztonsági esemény osztályozása* játszik. A kiberbiztonsági szervezetek ezen információ alapján döntenek arról, hogy az adott esemény milyen prioritással tart (egyáltalán tart-e) számot érdeklődésükre; kiknek kell információkat továbbítaniuk az eseményről; és ezt is felhasználva készítenek helyzetértékelő statisztikákat. Mivel napjainkban egységesen elfogadott osztályozási rendszer (taxonómia) nem létezik, alapvető interoperabilitás feladat a különböző rendszerek közötti jelentésmegőrző átalakítás biztosítása.

A kiberbiztonsági esemény által érintett ('áldozat', 'sérült') informatikai rendszer *összetevő típusa* szintén fontos szerepet játszik a kiberbiztonsági tevékenységben. A szervezetek ez alapján kereshetnek sérülékenységeket az esemény következményeinek elhárítása során; ez alapján; figyelmeztethetik a felügyeletük alá tartozó, támogatott szervezeteket a fennálló fenyegetésre;

[13] Ebben az értelmezésben nem tekintjük érdemi eltérésnek pld. a szöveges adatok karakterkészletében, mennyiségi adatok mértékegységében, vagy a dátum- és időadatok formátumában fennálló különbözőségeket, amelyekre a tartalomtól független átalakítási eljárások állnak rendelkezésre.

és értesíthetik az érintett gyártót; illetve ez az információ is fontos csoportosító tényező a kiberbiztonsági helyzetértékelő statisztikák elkészítése során. Mivel napjainkban még nincs széles körben elterjedt besorolási rendszer, sőt gyakran ez az információ kötetlen szöveges formájú, fontos interoperabilitási feladat annak átalakítása egy kötött értékkészletű saját besorolási rendszerre.

Az érintett *összetevő rendeltetés szerinti besorolása* (pld. kiszolgáló eszköz, munkaállomás, hálózati kapcsoló eszköz, vagy ennél részletesebb besorolás) az esemény értékelése, súlyossága, az események közötti prioritások meghatározásának egyik fontos kiinduló alapja. Ez az információ elsősorban a kiberbiztonsági eseménykezelő központ, és az eseményt elszenvedett, ügyfélkörébe tartozó szervezet között áramlik, azonban továbbításra kerülhet jelentések, tájékoztatások részeként is. A rendeltetés szerinti besorolásra sincs széles körben alkalmazott osztályozási rendszer, a különböző rendszerek közötti átalakítás mellett itt is felmerül a kötetlen szöveges formáról történő átalakítás feladata.

Végül *a kiberbiztonsági esemény hatásainak besorolása* – amennyiben nem más, mérhető jellemzők alapján kerül meghatározásra – szintén jelentős információ a különböző szintű kiberbiztonsági szervezetek számára feladataik prioritásának meghatározásához. A gyakorlatban 3-5 szintű skálák kerülnek alkalmazásra, amelyek között biztosítani kell a lehető legjobban jelentésmegőrző átalakítást, illetve speciális interoperabilitási feladatként merülhet fel a hatás súlyosságának besorolásából, az eredetileg alkalmazott besorolási feltételek esetén (visszakövetkeztetés alapján) egyes mennyiségi jellemzők, vagy azok értéktartományai meghatározására.

SÉRÜLÉKENYSÉGEKHEZ KAPCSOLÓDÓ INTEROPERABILITÁSI KÖVETELMÉNYEK, PROBLÉMÁK

A kiberbiztonsági szervezetek által kezelt információk között jelentős szerepet töltenek be a sérülékenységekre vonatkozóak is. A kiberbiztonságot megsértő események a legtöbb esetben az érintett informatikai rendszer összetevőiben megtalálható sérülékenységeket kihasználva következnek be. Emiatt a sérülékenységekre vonatkozó információk kezelése minden kiberbiztonsági szervezet alapvető feladata. A kapcsolódó információk általában az érintett rendszer összetevők gyártóitól, bejelentésekből, illetve más kiberbiztonsági szervezettől érkeznek, de keletkezhetnek az adott szervezetnél is.

A kiberbiztonsági szervezetek eredményes és hatékony működésének – az előző pontban foglaltak mellett – alapvető feltétele, ***általános interoperabilitási követelménye*** az is, hogy képesek legyenek együttműködő felek által küldött, vagy hozzáférhetővé tett sérülékenység információkat fogadni, átvenni, megfelelő módon értelmezni, és hasznosítani, illetve együttműködő partnereknek, támogatott szervezeteknek egyeztetett formában átadni, mivel a sérülékenységekre, illetve az elhárításukra vonatkozó információk nélkül nem lehet hatékony eseménykezelést megvalósítani.

A sérülékenységekhez kapcsolódó ***információk az interoperabilitási eltérések szempontjából*** szintén az előző pontban már meghatározott három csoportba oszthatóak. Azon információk közé, amelyeknek az együttműködő felek által használt *tartalma és formátuma érdemben nem tér el*, a következők tartoznak: sérülékenység azonosítók; az érintett összetevő megnevezése; valamint verziószáma, módosítása, kiadása. Sérülékenységekhez kapcsolódó *azonos tartalmú, de eltérő formátumú információnak* minősíthető az érintett összetevő gyártójának megnevezése.

A témánk szempontjából legfontosabb, *szemantikai, értelmezési eltérésekkel bíró információk* csoportja a következőket foglalja magában: a sérülékenység típusa, az érintett összetevő típusa; a sérülékenység potenciális következményeinek minősítése; illetve a sérülékenység súlyossága. Ezek közül több is megegyezik az eseményekre vonatkozó információkkal, hiszen az eseménykezelés és a sérülékenység nyilvántartás egymással szoros együttműködésben vannak.

A ***szemantikus interoperabilitási problémákat hordozó információk*** közül a *sérülékenységek osztályozása* rendszerező szerepet játszik a sérülékenységek nyilvántartásában, a különböző forrásokból származó sérülékenység információk összevetésében, sérülékenységek azonosságának, viszonyának feltárásában. Bár ezen a területen a Gyengeségek Felsorolása (CWE) lista alkalmazása széleskörű, de mellette léteznek más – az összetevők teljes körére, vagy csak egyes csoportjaira (pld. JAVA kódolási sérülékenységekre) kiterjedő – osztályozások, besorolások is.

Az *érintett összetevő típusa* kiemelt szerepet játszik a sérülékenység kezelésben. Ez segít a más forrásokból kiszűrni az adott kiberbiztonsági szervezet számára jelentőséggel bíró sérülékenységeket. Ez utóbbiak közé csak azok tartoznak, amelyek által érintett összetevők léteznek az eseménykezelő szervezet által támogatott szervezetek informatikai rendszereiben. A hatékony működés érdekében az összetevő típusának a sérülékenység nyilvántartásban szereplővel interoperábilis módon kell szerepelnie az informatikai erőforrások nyilvántartásában is.

A *sérülékenység következményeinek minősítése* a minden kiberbiztonsági szervezet által elvégzendő kockázatelemzés kiinduló adata. Ennek meghatározása az érintett szervezet feladata, ehhez azonban felhasználhatja a más szervezetek által megadott besorolásokat. Ehhez megfelelően értelmezni kell tudni az eltérő skálán meghatározott hatásszinteket, és átalakítani a saját skálára.

Végül *a sérülékenység súlyosságának besorolására* szintén nincs egységesen elfogadott skála és besorolási rendszer. A kapcsolódó interoperabilitási feladatok hasonlóak, mint amit a sérülékenység hatásának minősítésénél, illetve a kiberbiztonsági események hatásainak besorolásának bemutattunk.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Összegzésképpen megállapíthatjuk, hogy a kiberbiztonsági szervezetek közötti interoperabilitási problémák alapját az együttműködő felek közötti eltérések képezik, amelyek megnehezítik, vagy lehetetlenné teszik a jelentésmegőrző információcserét. Az információcserét befolyásoló, akadályozó eltérések megjelenhetnek a fizikai kapcsolatok technikai szintjén, az adatformátumok szintaktikai szintjén, valamint az adatok által hordozott jelentés szemantikai szintjén. Az interoperabilitási problémák egyik lehetséges, napjainkban leggyakrabban alkalmazott megoldása a szabványosítás, ami azonban nem minden esetben jelent megoldást, a heterogenitás nem mindig küszöbölhető ki, vagy nem célszerű kiküszöbölni.

A kiberbiztonsági eseménykezelő központok nézőpontjából az interoperábilis információcsere alapvető jelentőségű, tevékenységüket – elsősorban a biztonsági események kezelése területén – eredményesen csak egy eseménykezelő központ hálózat részeként, a hálózat többi elemeivel szoros együttműködésben, egymás kölcsönös informálásával képesek végezni. Az interoperabilitás hiánya azt jelenti, hogy az érintett szervezet tevékenységét csak kevesebb információ birtokában tudja végezni, vagy az átvett információk feldolgozása többletmunkát igényel, és több időt vesz igénybe.

Az interoperabilitási problémák a technikai és szintaktikai szinteken alapvetően megoldottak, vagy megoldhatóak, ezzel szemben a szemantikai szinten jelentős megoldatlan problémák állnak fent. A kiberbiztonsági szakterületen különböző célú taxonómiák, kötött értékkészlet listák sora jelent meg, amelyek közül egyesek szélesebb, mások szűkebb körben kerülnek alkalmazásra. A jövőben is várhatóan több kiberbiztonsági besorolási rend marad alkalmazásban, így a feladat ezek lehetséges mértékű összehangolása, illetve a jelentésmegőrző átalakítás biztosítása köztük.

FELHASZNÁLT IRODALOM

[1] MUNK S.: *Katonai informatikai rendszerek interoperabilitásának aktuális hadtudományi kérdései. MTA doktori értekezés.* – Magyar Tudományos Akadémia, 2007

[2] SARANTIS, D.-CHARALABIDIS, Y.-PSARRASM, J. Towards Standardising Interoperability Levels for Information Systems of Public Administrations. – In. Charalabidis, Y.-Panetto, H.-Loukis, E.-Mertins, K. (szerk): *eJETA Special Issue on "Interoperability for Enterprises and Administrations Worldwide"*, Athens, 2008

[3] *CERT cooperation and its further facilitation by relevant stakeholders.* – European Union Agency for Network and Information Security, 2006.

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

BASIC OF CYBERSECURITY PENETRATION TEST

KIBERVÉDELMI PENETRATION TESZT ALAPJAI

PARÁDA István

(ORCID ID: 0000-0002-3083-6015);

parada.istvan@uni-nke.hu

Abstract

Nowadays it is common and self-evident that organizations strive to secure their IT and communications systems. Part of this is testing and checking systems. One of the most important elements of cyber security testing is the penetration test. Penetration tests show the extent to which IT security is threatened by attackers. Attacks and security measures can provide adequate IT security. Measures to improve IT security are needed to overcome the threats. In line with corporate IT security policy, all such measures are described in the IT security concept for the entire organization. It is important to understand the process of penetration testing within cage protection and that it is not equal to public hacking. Penetration Test is a complex process that technically provides a comprehensive and realistic picture of the vulnerabilities of the infocommunication system. This article describes the basics of the penetration test, the location and role of the vulnerability analysis, and the basic parameters of the test.

The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance.

Keywords: *cybersecurity, penetration test, vulnerability analysis*

Absztrakt

Napjainkban általános és magától értetődő dolog, hogy a szervezetek az informatikai és kommunikációs rendszereik biztonságára törekszenek. Ennek egy része a rendszerek vizsgálata és ellenőrzése. A kiberbiztonsági tesztek egyik legfontosabb eleme a penetrációs teszt. A penetrációs tesztek azt mutatják, hogy az informatikai biztonságot milyen mértékben fenyegetik a támadók. A támadások és a biztonsági intézkedések képesek-e megfelelő informatikai biztonságot nyújtani. A fenyegetések leküzdéséhez az informatikai biztonság javítására irányuló intézkedésekre van szükség. A vállalati IT biztonságpolitikával összhangban minden ilyen intézkedést az egész szervezetre vonatkozó informatikai biztonsági koncepció ír le. Fontos megérteni a kibervédelmen belül a penetrációs tesztek folyamatát, és hogy nem egyenlő a köztudatban megjelent hack-eléssel. A penterációs teszt egy összetett folyamat, mely technikai úton átfogó és reális képet ad az infokommunikációs rendszer sérülékenységeiről. Ez a cikk bemutatja a penetráció teszt alapjainak meghatározását, a sebezhetőségi elemzés helyét és szerepét, valamint a teszt alapvető paramétereit.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

Kulcsszavak: *kiberbiztonság, penetrációs teszt, sérülékenységelemzés*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.07.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.05.19.

INTRODUCTION

Penetration testing has been in use for years and there are several methods for testing the technical security of the system. However, it is easy to confuse other forms of technical security testing, especially vulnerability analysis. Many organizations offer security features and terms such as security audit, network or risk assessment, and overlapping test overlays or application. Security surveys are a risk assessment, that is, services to identify the vulnerability of systems, applications and processes. Penetration testing has been in use for years and there are many methods to test the technical security of the system. However, it is easy to coordinate technical security tests in other forms, especially vulnerability analysis.

Nowadays there are many free and commercial security scanners, most of which contain updated databases due to known hardware and software failures. These tools are suitable to identify the vulnerability of the systems under investigation and therefore determine the risks associated with them. Typically, information provided by such devices includes a technical description of security vulnerability and provides instructions on how to eliminate weak points or points by changing configuration settings or updating system components. [1]

PENETRATION TEST KEY CONCEPTS

Definition of penetration test

Penetration testing uses several manual and automated techniques to simulate an organization's security information systems attack. This must be done by a qualified and independent penetration testing expert, sometimes referred to as an ethical security tester. Penetration testing takes advantage of known vulnerabilities, but it also needs testing expertise to identify specific weaknesses in the organization's security systems - unknown vulnerabilities. [2] The penetration testing process is an active analysis of the target system due to possible vulnerabilities that result from incorrect or incorrect system configuration, known and unknown hardware or software failures, and operational weaknesses in process or technical countermeasures. This analysis is typically carried out in the perspective of a potential attacker and could include the exploitation of vulnerabilities. So, the penetration test is a way to simulate methods an attacker can use to take over security management of our system or access it to a higher level of access. The process itself involves filtering and collecting vulnerabilities and security risk factors, then exposing them to attack by exploiting them. The penetration test more than, test runs over scanners or automated tools and then writes a report about it. The penetration test evaluates whether the vulnerability is real or false. For example, an audit or a survey may use scanning tools that result in hundreds of possible vulnerabilities on multiple systems. The penetration test attempts to attack these vulnerabilities in the same way as a malicious hacker to check which vulnerabilities are real, reducing the realistic list of system vulnerabilities for some security deficiencies. The most effective penetration tests are those that target a very specific system that has a very specific purpose. [3]

Penetration testing, often abbreviated as pentest, is a process that is performed to thorough safety assessment or audit. The methodology defines rules, practices, and procedures followed and implemented by the information security audit program. The penetration testing methodology defines a timetable, that provides practical ideas and best practices that can be tracked when assessing the true security situation of a network, application, system, or any combination thereof. Penetration testing can be performed individually or as part of an IT security risk management process that can be integrated into the regular development lifecycle. It is essential to note that product safety is not only dependent on factors related to the IT environment but also relies on product-specific security practices. This includes the

implementation of appropriate security requirements, risk analysis, code surveys, and operational safety measurements. The penetration test is the last and most aggressive form of security assessment. They must be trained by qualified professionals and can be performed with or without prior knowledge of the targeted network or application. The penetration testing output usually consists of a report that is divided into several parts that address the weaknesses found in the current state of the target environment and then recommend potential countermeasures and other recovery suggestions. The use of the methodological approach has extensive benefits for the tester to understand and critically analyze the integrity of the current defense throughout each stage of the testing process. The reason behind the penetration testing methodology is the fact that most attackers follow a common approach, when they enter the system. In the penetration test, the tester is limited by resources: time, skilled resources and access to equipment as outlined in the penetration testing agreement. The penetration test simulates the methods used by the intruder that give unauthorized access to the organization's network and compromise them. This includes the use of own and open source tools. In addition to automated techniques, intrusion tests include manual techniques for testing targeted systems and ensuring that there is no security vulnerability that has not been detected before. [4]

Vulnerability scanners

Vulnerability Analysis (also known as "Scanning") is the use of automated tools to identify well known security vulnerabilities in the system. Vulnerability assessment tools investigate information systems to determine whether security settings are turned on and applied, and that appropriate security patches have been applied. The vulnerability test is typically used to validate the minimum level of security - and is often the forerunner of a more specialized penetration test. It does not use the identification of attacks to re-engage the real attack and does not consider the general security of system-based management processes and procedures. This is the process of scanning network devices, operating systems, and applications to identify known and unknown vulnerabilities. Vulnerability is a gap, error, or weakness in system design, use, and protection. If a vulnerability is exploited, it may result in unauthorized access, prerogative, denial of service on the device, or other results. Vulnerability surveys typically break when a vulnerability has been found, so the tester does not perform an attack on the vulnerability to make sure it is real. The vulnerability assessment results with potential recovery steps as well as possible risks associated with any vulnerability. There are a number of solutions, such as Kali Linux, which can investigate vulnerabilities based on system / server type, operating system, open ports, and other devices(for exaple OpenVAS[1], MBSA[2] Secunia PSI[3], Nipper[4], Retina[5], Nexpose[6] GFI Lan Guard[7].)[5]

[1] The Open Vulnerability Assessment System (OpenVAS) is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. The actual security scanner is accompanied with a daily updated feed of Network Vulnerability Tests (NVTs), over 33,000 in total (as of December 2013). All OpenVAS products are Free Software. Most components are licensed under the GNU General Public License (GNU GPL). The OpenVAS is available for FREE and for Linux, Windows and other operating systems.

[2] The Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations. MBSA 2.3 release adds support for Windows 8.1, Windows 8, Windows Server 2012 R2, and Windows Server 2012. Windows 2000 will no longer be supported with this release. MBSA is a FREEWARE and is available only for Windows operating system.

Vulnerabilities are only useful when calculating the risk. The disadvantage of many security audits is the result of vulnerability testing, which makes security checks longer, without providing real value. Many vulnerable scanners show false results or identify vulnerabilities that do not really exist. This is because they are incorrectly identifying the operating system or looking for special fixes to fix vulnerabilities, but they do not investigate interchangeable fixes (multiple minor fixes) or software modifications. This means that the vulnerabilities reported by the automatic devices must be checked. Vulnerability Assessment is a process that can measure internal and external security audits by identifying threats that severely affect your organization's assets. Internal vulnerability assessment provides assurance of internal systems while external vulnerability assessment demonstrates border protection. In both test criteria, all elements of the network are strictly tested against multiple attack vectors to identify unattended threats and quantify reactive actions. Depending on the type of assessment to be performed, unique testing processes, tools and techniques are used to automatically detect and identify the vulnerability of information assets. This is achieved through an integrated vulnerability management platform that provides up-to-date security vulnerabilities and can test various types of network devices while retaining the integrity of configuration and change management. [6]

Penetration test vs vulnerability analysis

The key difference between vulnerability and penetration testing is that penetration tests go beyond the level of vulnerability identification that leads to exploitation process, increasing entitlements, and maintaining access to target systems. On the other hand, evaluation of vulnerability provides a broad picture of system errors, without considering the impact of these errors on the system being tested. The other two significant differences between the two terms are that the penetration test is much more rough than evaluating vulnerability and aggressively uses all the technical methods to take advantage of the IT environment. The vulnerability assessment process, however, carefully identifies and quantifies all known vulnerabilities in a non-invasive manner.

---

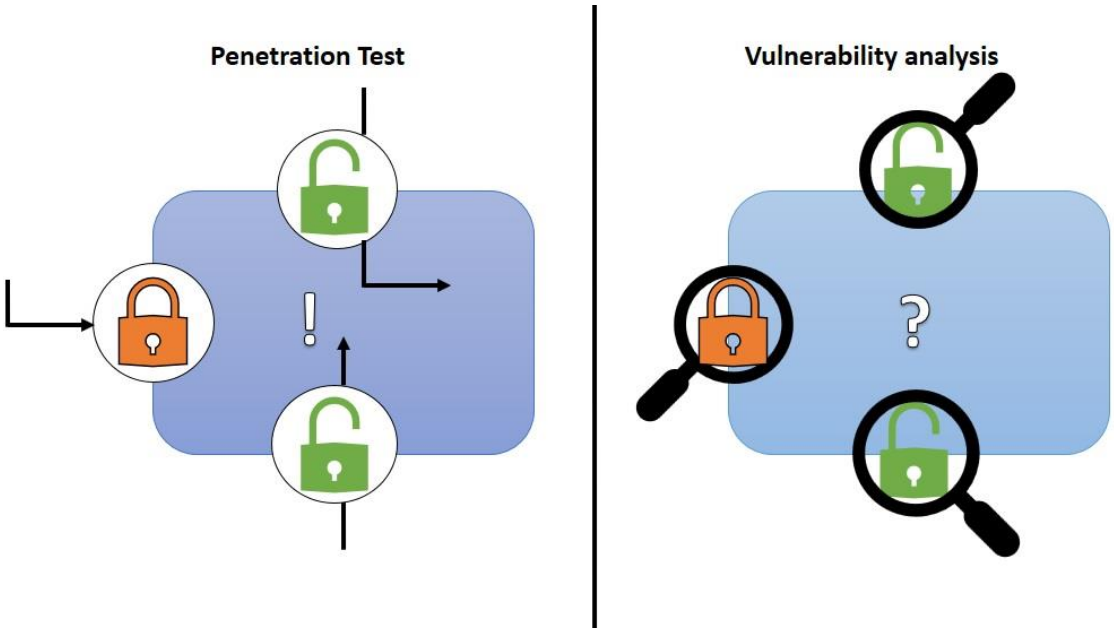
[3] The Secunia Personal Software Inspector (PSI) is a free security tool designed to detect vulnerable and out-dated programs and plug-ins, which expose your PC to attacks. Once installed, the Secunia PSI can help you patch vulnerable programs and stay secure. Secunia PSI is available for free and works only with Windows operating system.

[4] Nipper (short for Network Infrastructure Parser, previously known as Cisco Parse) audits the security of network devices such as switches, routers, and firewalls. It works by parsing and analyzing device configuration file which the Nipper user must supply. This was an open source tool until its developer (Titania) released a commercial version and tried to hide their old GPL releases (including the GPLv2 version 0.10 source tarball). Nipper is available for Windows, Apple MAC OSX, Linux and is a PAID software.

[5] With over 10,000 deployments since 1998, Beyond Trust Retina Network Security Scanner is the most sophisticated vulnerability assessment solution on the market. Available as a standalone application or as part of the Retina CS unified vulnerability management platform. Retina Security Scanner enables you to efficiently identify IT exposures and prioritize remediation enterprise-wide.

[6] Nexpose, the vulnerability management software, proactively scans your environment for mis-configurations, vulnerabilities, and malware and provides guidance for mitigating risks. Experience the power of Nexpose vulnerability management solutions by knowing the security risk of your entire IT environment including networks, operating systems, web applications, databases, and virtualization.

[7] GFI LanGuard scans and detects network vulnerabilities before they are exposed, reducing the time required to patch machines on your network. GFI LanGuard patches Microsoft ®, Mac® OS X®, Linux® and more than 50 third-party operating systems and applications, and deploys both security and non-security patches. GFI Lan Guard is a paid software and only works on Windows operating.



1. Figure Penetration test versus vulnerability analysis

So by scanning the vulnerability you will find individual vulnerabilities; penetration testing, however, tries to verify whether these vulnerabilities can be exploited in the target environment. Penetration testing in the area of security assessments goes one step beyond the vulnerability tests. Vulnerability Testing - a process that examines the security of individual computers, network devices, or applications - the penetration test evaluates the security model for the entire network. Penetration testing reveals the potential consequences for network administrators, IT managers, and executives for a real attack on the network. Penetration tests highlight the typical safety deficiencies that have been omitted during the vulnerability test. The penetration test points out the vulnerabilities and documents that these weaknesses can be exploited. It also shows that an attacker can exploit a number of minor vulnerabilities that compromise computers or the network. Penetration testing highlights the lack of organizational security modeling and helps organizations strike a balance between technical performance and business functions for potential security injuries. This information is also useful for disaster recovery and business continuity planning.[7]

Most vulnerabilities are evaluated only by software and do not evaluate other types of potential security issues. Human factors and processes can be important sources of vulnerabilities, just as technology or software vulnerabilities. By using social engineering techniques, intrusion tests may reveal whether employees can routinely allow people to enter into enterprise facilities without unauthorized access and unauthorized access to a computer system. Exercises applied during the patch management cycle can be evaluated during the penetration test. The penetration test is an ethical attack simulation designed to demonstrate or enforce the effectiveness of security controls in a given environment through exploitable vulnerabilities that pose real risks. It is built around a manual testing process that aims to move on through general responses, false positive results, and incomplete automated app ratings (such as tools used in vulnerability assessments). [8]

MAIN PARAMETERS

Objectives

In the case of a successful penetration test for the customer's expectations, a clear definition of the goals is indispensable. If the goals can not be achieved or are not effectively achieved, the tester should inform the customer during the preparatory phase and recommend alternate procedures. The result of the IT penetration test should therefore be more than just a list of existing vulnerabilities; Ideally, it should also provide concrete solutions and suggestions.

Intrusion testing is performed by an organization to achieve the following goals:

- Improving the safety of technical systems
- Identify vulnerabilities
- Confirming IT security by an external third party
- Improving the security of organizational and personnel infrastructure
- Test and confirm the safety and control efficiency
- Ensure availability of the organization's internal and external vulnerabilities
- Provide useful information to audit teams that collect data to comply with legislation
- Minimizing the costs of security controls by providing comprehensive and detailed, realistic evidence of business capability
- Promote the relevance of relevant patches for reported or known vulnerabilities
- Disclosing the existing risks of the organization's networks and systems
- Evaluating the effectiveness of network security tools, such as firewalls, routers, and web servers
- Develop a comprehensive approach to prepare for preventing future exploitation
- Find out if any existing software, hardware or network infrastructure needs to be modified or upgraded

Most penetration tests are commissioned to improve the safety of technical systems. Tests are limited to technical systems such as firewalls, routers, web servers, etc. The organizational and personnel infrastructure is generally not specifically tested. The penetration test can also be performed for confirmation from an independent external third party. It is important to note that the penetration test reflects the situation only at a certain point in time and can not, therefore, give a statement about the future security level. [9]

What makes a good penetration test?

The following activities ensure good penetration:

- Define the parameters of the penetration test, such as goals, limitations, and justification for the procedures
- Recruit highly trained and experienced professionals
- Appoint a legal penetration tester who follows the rules in the termination agreement
- Select a suitable test package that balances costs and benefits
- Follow up a well-designed methodology with documentation and documentation that documents the results carefully and makes them understandable to the customer. An intruder tester should be available to answer any questions when needed.
- The final report provides a clear description of the findings and recommendations

Limits

Performing penetration test runs will help you examine some of your security measures and improve your development, but there are limitations. For example, a penetration test:

- It covers only the targeted application, infrastructure, or the selected environment
- Focuses on the discovery of technical infrastructure,
- It covers only a small part of the human resources screening, specifically (social enginnering)
- Just snapshot from a system at a given time
- By legal or commercial considerations, the width or depth of the test can be limited
- You cannot detect all security weaknesses, for example due to limited scope or inappropriate testing
- Provides results that are often of a technical nature and need to be interpreted in a business context

Challenges

In general, organizations have encountered the following difficulties:
Determining the depth and width of the test coverage

- Determine what type of penetration test is required
- Understand the difference between vulnerability and pentest
- Identify the risks associated with possible system failures and disclosure of sensitive data
- Frequency of goals and tests
- To improve the vulnerabilities discovered during the penetration test, the system will really be "safe"

The need

The main drivers of penetration testing include a high level of concern about:

- Increasing compliance requirement
- The impact of serious (often Internet) security attacks on similar organizations
- Utilize the number and variety of outsourced services
- Significant changes in business processes
- Awareness raising about potential cyber security attacks. [10]

CONCLUSIONS

The summary should briefly summarize the conclusions, the results, possible suggestions and other new research orientations. The summary is also a mandatory element of the publications. The cybersecurity penteration test provides a thorough study of IT systems. As a result of today's trends, this choice of test methods provides complex analysis that covers the system and the organization's IT-related questions. It shows significant differences in testing vulnerabilities but provides a more comprehensive approach from the attacker's point of view. With this test, the identified safety deficiencies are not only collected but also exploited. the attacker goes on to exploit the vulnerability analysis as it may go further, get new information, and do more attacks. Then a comprehensive report is prepared, including suggestions.
Penetration Test is one of the most important technical tests of cyber security to ensure system security. Considering a number of international standards, however, there are many definitions and rounding differences. Standards are, of course, a major direction, but there are a lot of differences. This is because, on the one hand, these are recommendations, are not

binding. On the other hand, the penetration test itself depends on the attacking nature and expertise, so it can be said to try the objective test, but there are subjective elements in it. That is why I thought it important to define basic definitions, goals and features. This publication has collected the basic understanding of the penetration test, the differences between the fragility test and the penetration test. This includes the benefits, goals, and limitations associated with the test.

BIBLIOGRAPHY

[1] FEDERAL OFFICE FOR INFORMATION SECURITY (BSI) STUDY: *A Penetration Testing Model;* Bonn p.8.

[2] JASON C, IAN G.: *A guide for running an effective Penetration Testing programme* April (2017) p.8.

[3] GEORGIA W.: *Penetration testing A Hands-On Introduction to Hacking*; San Francisco ISBN-10: 1-59327-564-1 ISBN-13: 978-1-59327-564-8 (2014) pp.31-36.

[4] LEE A, TEDI H, SHAKEEL A.: *Kali Linux – Assuring Security by Penetration Testing*, Birmingham ISBN 978-1-84951-948-9; (2014) pp. 51-52.

[5] EC-COUNCIL CERTIFI ED SECURITY ANALYST PRESS*: Penetration Testing Procedures and Methodologies* ISBN-13: 978-1-4354-8367-5 ISBN-10: 1-4354-8367-7, USA (2011) p.23.

[6] JOSEPH M, AAMIR L.: - *Web Penetration Testing with Kali Linux;* Birmingham. ISBN 978-1-78216-316-9 (2013) p.13.

[7] LEE A, TEDI H, SHAKEEL A.: *Kali Linux – Assuring Security by Penetration Testing,* Birmingham ISBN 978-1-84951-948-9; (2014) pp. 53-54.

[8] JASON C, IAN G.: *A guide for running an effective Penetration Testing programme* April (2017) p.9.

[9] EC-COUNCIL CERTIFI ED SECURITY ANALYST PRESS: *Penetration Testing Procedures and Methodologies* ISBN-13: 978-1-4354-8367-5 ISBN-10: 1-4354-8367-7, USA (2011) p.24.

[10] JASON C, IAN G.: *A guide for running an effective Penetration Testing programme* April (2017) pp.10-12.

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

KIBERBIZTONSÁGI VÁLTOZÁSOK A FIZETÉSI SZOLGÁLTATÁSOKNÁL

CYBERSECURITY CHANGES IN THE PAYMENT SERVICES

SZÁDECZKY Tamás; VÁCZI Dániel

(ORCID: 0000-0001-7191-4924); (ORCID: 0000-0001-6770-6954)

szadeczky.tamas@uni-nke.hu; vaczi.daniel@hotmail.com

Absztrakt

A tanulmányban elemezzük a fizetési szektort a jövőben várhatóan jelentősen megváltoztató Payment Services Directive 2 (PSD2) Európai Uniós irányelvet. Megvizsgáljuk az előzményeit, a létrejöttének hátterét, és a várható hatását a fizetési szolgáltatások informatikai biztonságára. A szakma által sok pontban vitatott irányelvvel kapcsolatban megvizsgáltuk a főbb lefedett témaköreit, különös tekintettel az emberi tényezőre, mint e rendszer gyenge láncszemére.
Szembe állítjuk ezzel a jelenleg hatályos bankkártyás fizetésre vonatkozó szabályozás, a Payment Card Industry Data Security Standard (PCI DSS) különböző információbiztonsági előírásait.
Az Emberi Erőforrások Minisztériuma ÚNKP-17-4-III-NKE-26 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.

Kulcsszavak: *PSD2, PCI DSS, elektronikus fizetés, bankkártya, hitelkártya, információbiztonság*

Abstract

In our paper, we are analyzing the European Union's Payment Services Directive 2 (PSD2), which will probably change the payment sector shortly. We investigated its predecessors, background and its probable impact on the information security of payment services. We examined the main topics discussed in the directive, including the human factor as a weak element of the security.
We are comparing the PSD2 with the information security requirements of the Payment Card Industry Data Security Standard (PCI DSS), which is the current regulation defining the rules of credit card payment.
Supported by the ÚNKP-17-4-III-NKE-26 New National Excellence Program of the Ministry of Human Capacities.

Keywords: *PSD2, PCI DSS, electronic payment, bank card, credit card, information security*

A kézirat benyújtásának dátuma (Date of the submission): 2018.06.06.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.25.

BEVEZETÉS

A 2000-es évek második felében rohamosabb fejlődés volt tapasztalható az IT rendszerek minőségében, számában, funkcionalitásában, mint korábban. Minden az új és jobb felé mutat, azonban sok esetben ezek sem biztonsági fejlesztésekkel, sem jogi szabályozásokkal nem lettek megfelelően támogatva. Különböző folyamatok indultak el, amik az IT szektor szegmenseinek védelmében a fejlesztéseket célozták meg. Egyre jobban előtérbe került a biztonság, mind technikai, mind jogi oldalról. Ez a folyamat a piaci szegmensen és a nemzeti problémákon is túlmutatott. Ennek megoldására európai szintű szabályozásra volt szükség. Ezzel párhuzamosan a 2000-es évek pénzügyi válságai eredményeképpen 2010-től beindult a pénzügyi szektor szabályozása az operatív működés biztonságának szempontjából is. [1] Így más területek mellett, a bankszektor elektronikus pénz alapú fizetési módszereinek biztonságosabbá tétele is előtérbe került.

PÉNZFORGALMI SZABÁLYOZÁS

Az Európai Bizottság 2007-ben adta ki az *Európai Parlament és a Tanács 2007/64/EK irányelve (2007. november13.) a belső piaci pénzforgalmi szolgáltatásokról és a 97/7/EK, a 2002/65/EK, a 2005/60/EK és a 2006/48/EK irányelv módosításáról és a 97/5/EK irányelv hatályon kívül helyezéséről* szóló irányelvét (továbbiakban: PSD). [2] A fő célja az volt, hogy szabályozza az Európai Unió (továbbiakban: EU) és az Európai Gazdasági Térség (továbbiakban: EGT) területén a pénzforgalmi szolgáltatókat és szolgáltatásokat. Ezen belül az egyenlő piaci feltételek megteremtése volt a középpontban. A PSD biztosítja a jogi hátteret az Európai Fizetési Tanács (European Payments Council) – az európai bankszektor fizetési műveletekkel foglalkozó döntéshozó és koordinációs feladatokat ellátó testülete – által kidolgozott pénzfizetési megoldásokra, infrastruktúrákra és műszaki szabványokra vonatkozó harmonizációs törekvésére. A 2007. december 25-én elfogadott irányelveket 2009. november 1-jéig kellett harmonizálni az EU és az EGT tagállamainak a saját országuk jogrendjébe.

Az elmúlt közel 10 évben a korábban létező elektronikus fizetési módszerek mindegyike nagy fejlődésen ment keresztül, így különösen a fizetési célú mobilalkalmazások területe [3], valamint a korábban a dedikált adatkapcsolat helyett az internetet, illetve nyílt protokollokat használó fizetési megoldások. [4] A korábban elterjedt típusok mellé új megoldások, felületek kerültek piacra. Szükségessé vált tehát a PSD irányelv felülvizsgálata. A vizsgálat az Európai Bizottság javaslatára *Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változatának* 114. – a jogharmonizációról szóló – cikke tekintetében, az Európai Központi Bank és az Európai Gazdasági és Szociális Bizottság véleményezésével rendes jogalkotási eljárás keretében zajlott le. Az eljárás végén egy új irányelvet alkottak meg: *Az Európai Parlament és a Tanács (EU) 2015/2366 Irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről* (továbbiakban: PSD2). Ezt a tagállamok 2018. január 13-ától át kell ültetniük a saját jogi környezetükbe és alkalmazniuk kell az abban foglaltakat. [5; Preamb. 115.]

Az irányelv kapcsán több kérdés is felmerült. Valószínűleg csak a harmonizációs törekvések folyamán, illetve a bevezetést követően fog jobban kitisztulni a néhol talán túlszabályozott, néhol nagyon általános direktíva céljának megvalósíthatósága. Jelen tanulmány leginkább a Magyarország viszonylatában próbálja meg értelmezni a kérdéskört.

A VÁLTOZÁS SZÜKSÉGESSÉGÉNEK KÖRÜLMÉNYEI

A PSD2 létrejövetelének indokaként az irányelv sok okot sorol fel a preambulumban. Ezek közül kiemelendő az (1) bekezdés, mely szerint az EU-n belül „jelentős előrelépést sikerült elérni a lakossági pénzforgalom integrációja terén" [5; Preamb. 1]. A (3) bekezdés megfogalmazza, hogy szükség van az új irányelvre, mivel az 2007-ben elfogadott PSD hatálybalépése óta „jelentős technikai innováció zajlott le a lakossági pénzforgalmi piacon, gyorsan nőtt az elektronikus és mobilfizetések száma és a pénzforgalmi szolgáltatások új típusai jelentek meg". [5; Preamb. 3] Az európai egységes kártyás, internetes és mobilfizetés megteremtése, a nemzeti határok feloldása [5; Preamb. 4] nélkül nem valósítható meg, így célkitűzésként ez ismét belekerült az első pontok közé az irányelv létrejöttének okai között. Az irányelv számos célt határoz meg. Ezek közül technikai szempontból a következő bekezdésekben tárgyaltak fontosak.

Kiemelendő, hogy mind a jelenleg piacon lévő, mind a jövőben oda csatlakozni kívánó szereplők számára a folytonosság biztosítva legyen, illetve, hogy mindenki számára egy egyértelmű és harmonizált keretet nyújthasson, elkerülve bármilyen negatív megkülönböztetést a résztvevők között. [5; Preamb. 33] Fontos az, hogy nem csak a technológiák fejlődtek az elmúlt évtizedben, hanem a piacra új szereplők kerültek, akik nem voltak korábban integrálva a PSD által létrehozott rendszerbe. Az új változatban célként került meghatározásra, hogy minél szélesebb piacot érhessenek el az új fizetési megoldások. [5; Preamb. 6 és 27] Különösen igaz ez az internet alapú, hídként funkcionáló átutalásos jellegű banki platformokra, amelyek jellemzően fintech szolgáltatások.

A tagállamok a 2007/64/EK irányelv kivételekre vonatkozó részeit nagyon különbözőképpen értelmezték. Ez a fogyasztók kockázatának növelésén kívül a pénzforgalmi piacon történő verseny torzításához is vezetett. Az új irányelv tehát meghatározza, hogy a hatály alóli kivétel csak abban az esetben alkalmazható, ha az ügyfelek pénzeszközei nem kerülnek a pénzforgalmi közvetítőhöz és azok felett semmilyen befolyással sem rendelkeznek. [5; Preamb. 11] Erre a kitételre példák „az áruházi kártyák, az üzemanyagkártyák, a tagsági kártyák, a közlekedési kártyák, a parkolási kártyák, az étkezési jegyek illetve meghatározott szolgáltatási utalványok". [5; Preamb. 14] Kivételként határozza meg továbbá a kizárólag bankjegyek és pénzérmék fizikai szállításával foglalkozó pénzszállító és készpénzkezelő vállalkozásokat. [5; Preamb. 12]

Tisztázandónak tartja a jogszabály a különböző távközlési vagy más információtechnológiai eszközökkel történő fizetéseket, mivel ezek a legtöbb esetben hozzáadott értékkel is rendelkeznek. Szabályozandóak tehát a különböző mikrofizetési kategóriák közül többek között „a csevegésre, a letöltésekre, például videofilmek, zene és játékok letöltésére, a tájékoztatásra, például időjárás-jelentésre, hírekre, sporthírekre, tőzsdei hírekre és tudakozó szolgáltatásokra, valamint a részvételi televíziózásra, és rádiózásra, például szavazásra, vetélkedőkön való részvételre, élő visszajelzésekre vonatkozó szolgáltatások", illetve a különböző elektronikus jegyek és adományozáshoz kapcsolódó fizetési műveletek is. [5; Preamb. 15 és 16]

A kivételekkel történő visszaéléseket elősegítette az, hogy az eredeti irányelv nem kötötte hatósági bejelentéshez, ha egy vállalkozás ilyen szolgáltatásokat nyújtott. A PSD2 már kitér arra, hogy a releváns tevékenységekről az illetékes hatóságok meghatározzák, hogy valóban zártkörű hálózatok keretében működnek-e, mert csak ebben az esetben képeznek kivételt. [5; Preamb. 19]

A PSD2 GYAKORLATI ÁTTEKINTÉSE

Az Európai Unió egységes piacot célzó törekvései a PSD2 segítségével amellett, hogy a pénzmozgásokat azonnalivá szeretnék alakítani, többek között arra irányulnak, hogy a

bankkártya-társaságok egyeduralmából egy sokkal jobban megosztott piac jöjjön létre. Ez gazdasági szemszögből több ponton lehet érdekes. Sallai György rávilágít, hogy miért is alakulhat ki majd tisztább verseny a bankszektor ezen területén, ha más szereplők is jelen lesznek. [6]

Gazdasági szempontok

Eddig a bankkártyával történő fizetéskor nem közvetlenül a felhasználó bankjához kerültek a tranzakciók adatai, hanem a kártyatársaságok azonosítottak bennünket és a tranzakciót mind a két irányban. Ezért a szolgáltatásért a kereskedők voltak anyagilag terhelve, amely bevételből a bankok részesedést kaptak. Ezt az EU 2015/751 rendelete szabályozta, azonban ez nem volt elég. [7] A PSD2 segítségével a szolgáltatási piac megnyitása azonban eredményezheti a tisztább versenyt, melynek a végső nyertesei a felhasználók lehetnek.

Sallai rávilágít arra, hogy üzembiztonsági előnyökkel is jár a piac megnyitása. Példaként az Oroszország elleni szankciók bevezetését hozta, ahol a Visa és a MasterCard felfüggesztette a tranzakciós szolgáltatást, így gyakorlatilag súlyosan korlátozta a hétköznapok normális folyását. Ha csak néhány szolgáltató van a piacon és abból valamilyen okból néhány kiesik, könnyű belátni, hogy a tranzakciók nem fognak végbemenni. Azonban tekintsük meg az általános nyílt piaci viszonyokat. Ha több szolgáltatónak van lehetősége jelen lenni és abból néhány működésképtelen lesz valamilyen okból, akkor a többi még el tudja látni a feladatot. A szolgáltatás kiesés lehet egy fent említett szankció vagy akár egy rosszindulatú kód – például a napjainkban nagy figyelmet kapó ransomwarek egyike – aktivizálódása is.

A PSD2 oly módon nyitja majd ki, ezáltal feltehetően meg is változtatja az elektronikus fizetési piacot, hogy nem a megszokott kártyaadatokat megadási felülettel találja majd szemben a felhasználó magát. A majdani szolgáltató lesz az, akit meg kell adnunk egy fizetés során. Mindezek a műveletek egy teljesen egységes alapú webes felületen kellenek majd, hogy véghez menjenek.

Az elemzésből is kiderül, amit a téma kapcsán alapcélként tekinthetünk, hogy a fizetési lánc ily módon történő megváltoztatása elősegíti majd a résztvevők versengését a felhasználókért. Ezáltal egyre lejjebb szorítva a díjakat, egyúttal átláthatóbbá téve a piacon működő folyamatokat. Az áttekinthetőség az előírás szerinti, minden bankra kötelezően vonatkozó 20 elemű jegyzés elkészítésével válik teljesebbé. Egy összehasonlító oldalra kell a szabályozott pénzintézeteknek feltölteni a legjellemzőbb, díjköteles, fizetési számlához köthető szolgáltatásokat.

A direktíva meg fogja könnyíteni a bankváltás eddigi időbeni nehézségeit. Más kérdés, hogy Magyarországon az emberek többsége inkább aszerint választ bankot, hogy a lakhelyéhez melyiknek van közelebb bankfiókja, ATM-je. A könnyű váltás persze, mivel EU-s direktíváról beszélünk nem csak egy országon belüli bankváltást könnyíti meg. A rendelet célja, hogy feloldja azokat a korlátokat, melyeket a különböző tagállamok állítottak országhatáraikon belül. Így az adott szolgáltatók előtt nemzetközi lehetőségek nyílnak.

Ahhoz azonban, hogy a PSD2 keretrendszere a legjobban optimalizálható legyen, a társadalomnak fel kell ismernie a lehetőségeket az elektronikus fizetések kapcsán. Vannak olyan országok, mint például Japán, ahol az emberek többsége nem használ kézpénzt. Nem okoz tehát sem a fiatalkorúnak, sem az idős generációnak a kártyás fizetés. Itthon ez már kevésbé a valóság. Sokan ragaszkodnak a kézzel fogható fizetőeszközhöz. Ez itthon feltehetően az ország fejlődéséhez és a szocializációhoz vezethető vissza. Az EU törekvései a szürke-fekete gazdaság felszámolásával, az átláthatósággal pedig nyílván úgy valósítható meg, ha minél több pénzmozgásnak van látható nyoma.

Technikai megvalósítás

A 2018. elejében induló új fizetési lánc majdani résztvevői, feltehetően már elkezdtek készülődni, hogy a piac robbanásakor be tudják vezetni a saját megoldásaikat. A piaci nyitás törekvésének technikai oldalról vett alapja az úgynevezett banki API-k megnyitása [8]. Az API gyakorlatilag egy olyan modul, ami segítségével egy rendszer bizonyos részeit mások felhasználhatják saját felületükre. A legegyszerűbb példa, amikor a Google Maps API-ját használta, a Nintendo nagy sikerű Pokemon Go elnevezésű, a valóságot virtuális térré átalakító játéka. Itt a játék fejlesztői a megfelelő API-t használták, hogy rá tudják illeszteni a valós térképre a saját „világukat".

Valami hasonlót kell majd elképzelni a bankok kapcsán is. A pénzintézet köteles lesz biztosítani egy API-t, amihez a piacra lépő szolgáltatók (adott esetben maguk a bankok) a megfelelő engedélyekkel rendelkezve hozzáférhetnek az ügyfelek számlaadataihoz. Ehhez azonban az előírt engedélyekre van szükség, mind a kezdeti piacra jutási engedélyezési eljárás során megszerzett hatósági engedélyre, mind a felhasználó hozzájárulására az adott szolgáltatás igénybevételekor.

Szabályozás

Többek között Németh Monika is felveti a finteczone.hu-n [9] a túlszabályozottság kérdéskörét. A már korábban említett szolgáltatók rendszerbe történő beintegrálódásához szükséges előírások sok esetben nem kockázatarányosak. Emellett sok kritika éri az erős autentikációt szabályozni kívánó RTS (Regulatory Technical Standards on Strong Customer Authentication) előírást. Ahogy Németh is említi, a fő probléma az egyensúly megtalálása. Ez persze minden biztonsági rendszerben egy fontos alapkérdés. Feltehetően a kétfaktoros hitelesítés a kivételek megadásával manapság már nem annyira kényelmetlen. Így a félelmek talán csak a régebbi rossz gyakorlatból fakadnak.

Az tény, hogy az átlag felhasználó biztonságtudatosságának hiánya miatt plusz energiának tűnik egy második faktor beillesztése. Jelen technológia mellett, ahol a telekommunikációs cégek rendelkezésre állása, a hálózatok magyarországi lefedettsége egyre jobb, az SMS alapú második faktor beiktatása már nem lehet kényelmi hátrány. A biometrikus eszközök, tokenek is egyre szélesebb körben elterjedtek. Természetesen ezek plusz másodpercek, azonban optimista feltételezésünk szerint, egy ilyen mindenki által használt rendszer elindítása jó alkalom lesz a tudatosabb felhasználói szokások kialakítására.

Természetesen ez az intézkedés miatt az online fizetési felületek elveszíthetik a „one-click" típusú műveleteiket. De ne legyen kétségünk afelől, hogy azok a technológiai cégek, akik egy ilyen jövedelmező, új területből profitot szeretnének realizálni, azon lesznek, hogy a felhasználók minél egyszerűbben, kényelmesen tudják a szolgáltatásaikat igénybe venni. A sikerüknek ez lesz az egyik, hanem legfontosabb része, a megfelelő biztonsági előírások betartása mellet.

AZ ELEKTRONIKUS PÉNZFORGALMI SZOLGÁLTATÁSOK ELLENI HUMÁN ALAPÚ TÁMADÁSI LEHETŐSÉGEK

A social engineering, azaz az emberek céljaink érdekében történő irányítása, sok esetben összeforrt a hackelés fogalmával. [10] A támadás nem csak informatikai rendszerek ellen irányulhat. A banki, pénzügyi szektort fókuszba véve a támadás elsősorban adatok megszerzésére, illetve anyagi haszonszerzésre irányul. Megtörténhet, hogy valaki identitását használják saját célra a támadók, de az is előfordulhat, hogy olyan szolgáltatásokat hoznak létre, melyeknek a célja, hogy a gyanútlan áldozat pénzéhez jusson hozzá ellenszolgáltatás nélkül. Ebbe a kategóriába tartozik az olyan kecsegtető megoldás (pl.: mobil alkalmazás) nyújtása, mely elvégzi ugyan azt a funkciót, amiért az áldozat igénybe veszi (ingyen vagy fizetségért

cserébe), azonban a háttérben olyan is történik, melyet nem szeretne a szolgáltatást igénybevevő.

Mivel a nem szakmabeli emberek nem ismerik a lehetőségeiket, technikai tudásuk nem elegendő arra, hogy felismerjék a veszélyeket, így könnyen megvezethetőek. Ez különösen igaz a mobil eszközökkel kapcsolatos, illetve a közösségi médiában megjelent új készpénzkímélő megoldásokkal kapcsolatban. Az alkalmazáson belüli vásárlások, a hamis e-bank oldalak, a különböző online bankkártyák mind lehetőséget adnak a gyanútlan személyek kihasználására a különböző social engineering módszerekkel.

A magyar büntetőjog a készpénz-helyettesítő fizetési eszköz hamisítását és az azzal való visszaélést bünteti. Szerencsére az ilyen típusú bűncselekmények csökkenő tendenciát mutatnak. [11]

A VÉDELMI SZINT NÖVELÉSE A PSD2 SEGÍTSÉGÉVEL

A PSD2-ben leírt szabályozások alapvetően a pénzforgalmi szolgáltatást nyújtókra vonatkoztatott keretet határoz meg, mely mégis olyan következményekkel jár, ami a fogyasztók számára a biztonsági szint növelését segíti elő. Ezáltal közvetve hozzájárul a humán alapú támadások megakadályozásához, melynek alanya lehet a fogyasztó és a szolgáltatást nyújtó is. A legtágabb körű védelmi szint az, hogy az elektronikus pénzforgalmi szolgáltatást nyújtók csak engedélyhez kötötten végezhetnek ilyen jellegű tevékenységet, így ha nem felelnek meg a velük szemben támasztott követelményeknek, normál esetben nem is nyújthatnak ilyen szolgáltatásokat. Ahhoz, hogy egy pénzforgalmi intézmény működni tudjon, a székhely szerinti tagállam illetékes hatóságához kell fordulnia engedélyért.

Az ellen, hogy a szolgáltató lehetővé tegye a vevőtől történő pénz beszedését, de ellenszolgáltatást cserébe ne nyújtson az irányelv 7. cikke nyújt védelmet. Ez meghatározza, hogy a pénzforgalmi intézmények tőkéje – a szolgáltatások milyenségétől függően – nem csökkenhet 20 000, 50 000 vagy 125 000 EUR alá.

Az irányelv a személyes adatok védelmével, a különböző erre vonatkozó felelősség-meghatározásra irányuló jogi problémák megoldására is próbál megoldást találni. [5; Preamb. 29 és 30] A fogyasztó és a vállalkozó oldal különbsége miatt fontos megállapítani, hogy különböző szintű védelemre van szükségük, azonban jogállástól függetlenül az irányelvnek mindenkor alkalmazhatónak kell lennie. [5; Preamb. 53]

BANKKÁRTYÁS FIZETÉSI BIZTONSÁG A PCI DSS-SZEL

A PSD2 megnyitja a lehetőséget az alternatív készpénz-kímélő fizetési módok előtt, viszont ezek kevésbé szabályozott szolgáltatások, – ha nem is jogilag, mindinkább műszaki szempontból – mint a klasszikus bank- és hitelkártyás fizetési tranzakciók.

A szigorúbban szabályozott pénzügyi szolgáltatások előnye az, hogy pontosabban meghatározott biztonsági követelményeket írnak elő velük szemben. Jó példa erre a bankkártyás fizetési piac. Öt nagy bankkártya márka (American Express, Discover, JCB International, MasterCard és Visa Inc.) együttműködéséből született szervezet és bankkártyás fizetési biztonsági szabvány (Payment Card Industry Data Security Standard, PCI DSS) szabvány részletesen meghatározza a követendő biztonsági szabályokat. Így konkrétan előírja, hogy a bankkártyát elfogadó kereskedők illetve a bankkártyás fizetésben érintett szolgáltatók informatikai rendszereit hogyan kell kialakítani. A 139 oldalas szabvány – melynek legújabb 3.2.1 verziója 2018 májusában jelent meg – részletekbe menően meghatározza még azt is, hogy a tűzfal szabályok módosításairól milyen bizonyítékokkal kell rendelkeznie a szervezetnek. [12] A PCI DSS az informatikai biztonsági szabványok közül messze a legrészletesebb és lehető legpontosabban meghatározza a betartandó szabályokat. Ez persze nem teszi lehetetlenné

a visszaéléseket, – ahogy azokról a napi sajtóban is értesülhetünk – viszont jelentősen csökkenti az incidensek bekövetkezésének valószínűségét.

A PCI DSS minden olyan informatikai rendszerre és szervezetre vonatkozik, ahol bankkártya adatokat kezelnek, vagy pedig bankkártya adatok biztonság a múlik az adott szolgáltatáson. A szabványok vonatkoznak a rendszer infrastrukturális elemeire, az üzemeltető személyzetre, és a dokumentációkra is.

A szabvány első fejezete az informatikai hálózatok biztonsági követelményeit határozza meg. A biztonság legfontosabb meghatározó elemei a tűzfal és az útvonalválasztó (router). Az első fejezet nagy része ezek biztonságos konfigurációjáról, a konfiguráció központi tárolásáról. menedzsmentjéről és az új eszközökön az automatikus beállításáról szól.

A második fejezet az informatikai rendszerek és a hálózati infrastruktúra biztonságos konfigurációjával foglalkozik. Ezen belül az alapértelmezett jelszavak megváltoztatása, a hálózati konfiguráció védelme és a biztonságos alapbeállítások létrehozása a cél. Minden szervernek csak egy elsődleges funkciója lehet és csak a feltétlenül szükséges szolgáltatások futhatnak rajtuk. Minden, nem a konzol előtt végzett rendszergazdai műveletet csak titkosított csatornán lehet végezni.

A harmadik fejezet célja a tárolt hitelkártya adatok védelme. A legjobb az, hogyha elkerüljük az adatok tárolását, de ha erre nincsen lehetőség, akkor csak a legszükségesebb adatkört szabad kezelni, annyi ideig, ami elengedhetetlen az üzleti, vagy technikai cél eléréséhez és a titkos azonosító adatok (úgymint pinkód és a három számjegyből álló CVC2/CVV2 kód) kizárólag a kártyakibocsátók által tárolhatók. Azt, hogy ez minden esetben teljesül, kötelező a rendszerben vizsgálni. Véletlen tárolás lehet például a webszerver hibanaplójában. Alapvetően a bankkártyaszám megjelenítésénél maszkolásra kell törekedni, amikor csak az első hat és az utolsó négy számjegy jeleníthető meg legfeljebb. A tárolt adatokat titkosítani kell, ami történhet a táblázat, az állomány, vagy a teljes lemez titkosításával. A kulcsok kezelésének szabályait részletesen meg kell határozni, így például a szabadszöveges kulcsokat szét kell osztani.

A negyedik fejezetben a bankkártya adatok nyilvános hálózatban történő átküldése kerül szabályozásra. Alapvető követelmény itt, hogy csak megfelelő titkosítású protokoll használható. Az átlagosnál szigorúbb követelmény, hogy az SSL és korai TLS protokollokat a szabvány nem tekinti biztonságosnak. Ezek használata csak 2018 júliusáig lehetséges és akkor is csak megfelelő migrációs és kockázatcsökkentési terv mellett. [13]

Az ötödik fejezet a kártékony kódok elleni védelemről és az antivírus program naprakészen tartásáról szól. Előírás, hogy minden olyan rendszeren, ami ki van téve vírustámadás veszélyének, kötelező a vírusvédelmet biztosítani. A rendszeresen frissített és ütemezett teljes keresést végrehajtó víruskereső beállításaihoz csak az arra felhatalmazott felhasználói kör férhet hozzá.

A hatodik fejezet a biztonságos rendszerek fejlesztéséről és üzemben tartásáról szól. A különböző sérülékenységeket azonosítani és magas kockázat esetén három hónapon belül javítani szükséges. Ezzel előírva a rendszeres operációs rendszer és alkalmazás frissítések kötelezettségét. Szoftverfejlesztéskor külön feladat megfelelően biztonságos kód fejlesztése. Ezen belül a megfelelően kialakított változáskövetési rendszer, a szokásos programozási hibák és sérülékenységek kiküszöbölése, így különösen az OWASP TOP10 sérülékenységi lista kiküszöbölése.

A hetedik fejezet a bankkártya adatokhoz való hozzáférés korlátozásáról szól, amelynek meg kell felelnie az üzleti igényben meghatározott legkisebb tudás elvének. Elvárás, hogy erre külön hozzáférésvezérlési rendszer legyen létrehozva.

A nyolcadik fejezet a rendszerkomponensekhez való hozzáférések vezérléséről és azonosításáról szól. Szükséges a hozzáférések megadásának és menedzsmentjének a formalizálása. Ez történhet egy federált identitás menedzsment rendszer bevezetésével is akár, de alapvetően lokális gépen megfelelően szabályozott fiókok és hozzáférési engedélyek is

elégségesek. Ugyanígy külön foglalkozni kell a harmadik felek által a rendszerhez való hozzáférés korlátozásával. Szükséges a legalább hét karakteres komplex jelszó alkalmazása, amely legfeljebb három hónapig érvényes és nem egyezhet meg az előző négy jelszóval. A hat téves próbálkozást legalább harminc perces kizárás kell, hogy kövesse. A megnyitott kapcsolatokat tevékenység hiányában tizenöt perc után le kell zárni. A rendszergazdai hozzáférések esetében többfaktoros azonosítást kell alkalmazni. A csoportos, több felhasználó között megosztott, vagy az általános felhasználói fiókok használata tilos.

A kilencedik fejezet a bankkártya adatok fizikai hozzáférés-védelmével foglalkozik. Ennek keretében a szervertermet vagy az irodát kamerával meg kell figyelni, vagy kártyás beléptetőrendszerrel kell szabályozni a belépést. A hozzáférési adatokat vagy kamerafelvételt egy évig kell tárolni, ezen belül a legutóbbi három hónap adatainak azonnal visszakereshetőnek kell lenni. Ezzel kapcsolatban problémát jelent a személyi és vagyonvédelmi tevékenységet szabályozó törvényben meghatározott adattárolási idő. Amennyiben a PCI DSS által meghatározott követelmény valamely nemzeti jogi előírás miatt nem teljesíthető, akkor azt külön rögzíteni szükséges, de ilyenkor mindig a nemzeti jognak van elsőbbsége. A védett területen azonosítani kell és meg kell különböztetni a munkatársakat és a vendégeket. Ide tartozik a biztonsági mentések és minden más adathordozó fizikai védelme, a tárolás, a szállítás és a megsemmisítés kapcsán.

A következő fejezet a biztonsági naplózás előírásait határozza meg, így különösen a naplók tartalmát, a napi (sic!) logelemzés szükségességét és a naplók egy éves megőrzését egy dedikált naplószerveren vagy mentésekben. Itt foglalkozik a szabványalkotó az időszinkron beállításaival is, ugyanis ez is kiemelten fontos a naplók felhasználhatósága, valamint az azonosítás (authentikáció) esetében is.

A tizenegyedik fejezet a biztonsági tesztelés kérdéskörét tárgyalja, így az engedély nélküli vezeték nélküli hálózatok negyedévenként végzendő keresését, a külső és belső sérülékenység-vizsgálatokat szintén negyedévenként, az éves behatolási tesztelést (penetration test) és ugyanezt félévenként a hálózati szegmentációra vonatkozóan. A külső sérülékenység-vizsgálatokat csak a szintén PCI Council által meghatározott PCI Approved Scanning Vendor (ASV) programban részt vevő szervezetek végezhetnek.

Az utolsó fejezet a belső szabályzatokkal, adminisztratív kontrollokkal foglalkozik. Ezen belül az információbiztonsági politika és annak felülvizsgálata, munkavállalók biztonsági átvilágítása, képzések, beszállítók kiválasztása, felelősségek, hatáskörök tisztázása a szabályozott kérdések.

A fentiek alapján látható, hogy a PCI DSS meglehetősen részletesen szabályozza a bankkártyás fizetési biztonság területét, de alkalmazása viszont csak azokban az esetekben kötelező, ahol a fenti cégek bankkártyáival történik a fizetés. Így tehát minden olyan fizetési eljárás, ami kikerüli a legismertebb bankkártyákat mindennemű ellenőrzés nélkül működhet. Hasonlóképpen igaz ez az állami pénzmozgásokra. [15] Ezzel a kérdéssel viszont jelen cikkünkben nem foglalkozunk. A szerzők részéről talán nem alaptalanul merül fel az aggodalom, hogy a PSD2 bevezetésével az Európai Uniós pénzkímélő fizetési eszközök piacán hirtelen szabályozatlanul sokféle új fizetési mód jelenik meg. Ez nem jelenti azt, hogy ezek a fizetési módok rosszak lennének, viszont azok megfelelőségét nem kötelező vizsgálni és nincsenek is meg rá a megfelelő szabványok illetve a helyes iparági gyakorlat. Tehát az a szabályozás, ami a piacra lépést megkönnyíti könnyen sodorhatja veszélybe az állampolgárok anyagi biztonságát és egyben pénzügyi rendszerbe befektetett bizalmát. Ez utóbbi kiépítése több évtizedes komoly fejlesztés eredménye, beleértve azt is, amikor a bankok még az elvárhatónál is jobban igyekeznek kielégíteni az ügyfél biztonsági igényeit. Erre példa volt Magyarországon, hogy a MALÉV csődje esetében több bank visszatérítette a bankkártyával vásárolt repülőjegyet, amire pedig semmiféle kötelezettsége nem volt, kizárólag a bizalom erősítését szolgálta.

A fentiekkel szemben egy új típusú mobil fizetési eljárás sok esetben ismeretlen terület. A gyártó nyilván végez kockázat csökkentési lépéseket, de azoknak a pontos módjára nincsen jól bevált ipari gyakorlat, ami egyben azt is jelenti, hogy könnyen megeshet, hogy ezek a jónak tűnő védelmi intézkedések valójában nem megfelelően hatásosak és ezért incidensek történnek és a már kiadott szoftvert többször módosítani, rosszabb esetben visszavonni kell. A vevői bizalom másik kulcsfontosságú terület a hatékonyság és felhasználó barátság mellett, amely jellemző kihívása minden digitális szolgáltatásnak. Elég erre egy analóg példaként az elektronikus aláírást említeni, ahol húsz éve nem sikerült kialakítani azt a felhasználói bizalmat, ami a tömeges elterjedéshez szükséges. Így gyakorlatilag két évtized után is csak egyes részterületeken, különleges eljárásokban használják a digitális aláírást, pedig az az elektronikus hitelesség egyetlen valódi eszköze. Ennek legfőbb oka az, hogy a felhasználók nem értik a rendszer működését és így mint egy átláthatatlan matematikai eljárásra nem bízzák a szerződések hitelességét. Másrészről valószínűleg a használók nagy többsége a bankkártyás fizetési eszközök működését sem ismeri, de ott a praktikum és a széleskörű alkalmazhatóság, valamint az incidensek relatíve alacsony száma meggyőzte a használókat ennek a szükségességéről. Ez a bizalom az, amit egy rossz döntéssel, rossz termékkel, vagy egy szélesebb körű incidenssel nagyon gyorsan le lehet rombolni és elérjük vele, hogy a felhasználó visszatérjenek a készpénz alkalmazásához.

ÖSSZEGZÉS

A mindennapjainkat nagyban meghatározó különböző elektronikus tranzakciók védelme szerencsére egyre nagyobb figyelmet kap. Ez azért is fontos, mert a sűrűn használt bankkártyás fizetések mellett a piacon egyre jobban elterjednek a mobileszközökön történő mikrofizetések. Ennek a biztonságosabbá tételére a PSD2 jó védelmi megoldást nyújt mind az elektronikus fizetési megoldásokat szolgáltató, mind az ezeket igénybevevők számára. Az Nem szabad azonban a szakembereknek csupán azzal foglalkozniuk, hogy a jogharmonizáció után elérjék azt a szintet, hogy a PSD2-nek megfeleljenek. Törekedniük kell arra, hogy a lakosság figyelmét felhívják a saját naivitásukból, ismereteik hiányából fakadó olyan veszélyekre, melyek anyagi és erkölcsi károkat okozhatnak számukra. Ez, a védelmi megoldások beiktatása mellett, csak a megfelelő neveléssel, oktatással lehetséges.

FELHASZNÁLT IRODALOM

[1] KECSKÉS A.: *Európai jogi szabályozás és annak magyarországi implementációja a pénzügyi intézményeket érintő új kihívások területén*. In: TILK Péter (szerk.): Az uniós jog és a magyar jogrendszer viszonya. PTE, Pécs, 2016. Pp. 333-356.

[2] *Az Európai Parlament és a Tanács 2007/64/EK irányelve (2007. november 13.) a belső piaci pénzforgalmi szolgáltatásokról és a 97/7/EK, a 2002/65/EK, a 2005/60/EK és a 2006/48/EK irányelv módosításáról és a 97/5/EK irányelv hatályon kívül helyezéséről szóló irányelvét* (Payment Services Directive, PSD)

[3] Z. JORGENSEN, J. CHEN, C. S. GATES, N. Li, ROBERT W Proctor, TING Yu: Dimension of Risk in Mobile Applications; San Antonio, Texas, USA; 2015; ISBN: 978-1-4503-3191-3

[4] K. SUNG, J. KYU LEE: *Preference of Internet-based Debit Payment Protocols*; Liverpool, United Kingdom; 2011; ISBN: 978-1-4503-1428-2

[5] Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről, OJ L 337, 23.12.2015, p. 35–127 http://data.europa.eu/eli/dir/2015/2366/oj

[6] SALLAI Gy.: *Olyan változás jön, ami minden magyar bankkártyát érint;* http://www.portfolio.hu/vallalatok/it/olyan_valtozas_jon_ami_minden_magyar_bankkartyajat_erinti.229610.html (letöltve: 2018. 06. 01.)

[7] *Az Európai Parlament és a Tanács (EU) 2015/751 rendelete (2015. április 29.) a kártyaalapú fizetési műveletek bankközi jutalékairól, HL L 123.,* 2015.5.19., 1—15. o. http://data.europa.eu/eli/reg/2015/751/oj

[8] NYÁRY M.: *A banki adatok kötelező megnyitása: robbanás előtt a pénzügyi informatika* http://hirlevel.egov.hu/2016/11/21/a-banki-adatok-kotelezo-megnyitasa-robbanas-elott-a-penzugyi-informatika/; (letöltve: 2017. 03. 12.)

[9] NÉMETH M.: *Egy évvel a PSD2 után*; http://fintechzone.hu/egy-evvel-a-psd2-elfogadasa-utan/; (letöltve: 2017. 03. 12.)

[10] KOVÁCS L.: *Az információs terrorizmus eszköztára*, Hadmérnök, I. évf. 2006. különszám

[11] TÓTH D.: *A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények büntetőjogi szabályozása*. In: KECSKÉS Gábor (szerk.): Doktori műhelytanulmányok, Széchenyi István Egyetem, Győr, 2015. ISSN 2064-1788

[12] *Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures. Version 3.2.1* May 2018. PCI Security Standards Council, LLC.

[13] SZÁDECZKY Tamás: Kriptográfiai protokollok megfelelősége, Hadmérnök XI. évf. 4. sz. 2016. december. ISSN 1788-1919 pp. 178-183.

[14] SZÁDECZKY T.: *Information Security Law and Strategy in Hungar*y, Academic and Applied Research in Military and Public Management Science (ISSN: 2064-0021) 14: (4) pp. 281-289. (2015)

[15] SZABÓ ZS. M.: *A nyugdíjfolyósítás információbiztonsági és informatikai biztonsági kérdései,* In: Bitay Enikő (szerk.): A XXII. Fiatal Műszakiak Tudományos Ülésszak előadásai. Kolozsvár: Erdélyi Múzeum Egyesület (EME); Óbudai Egyetem, 2017. 4 p. (ISBN 978-963-449-018-0) pp. 363-366. (Műszaki Tudományos Közlemények - Papers on Technical Science)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

AZ IT BIZTONSÁGTUDATOSSÁG SZEREPE AZ E-LEARNING HALLGATÓI HASZNÁLATI HAJLANDÓSÁGÁNAK TAM MODELLJÉBEN MAGYAR OKTATÁSI KÖRNYEZETBEN - A STRUKTURÁLIS EGYENLET MODELLEZÉS

THE ROLE OF IT SECURITY AWARENESS IN THE TAM MODEL OF STUDENTS' MOTIVATION AND BEHAVIOURAL INTENTION TO USE AN E-LEARNING ENVIRONMENT IN HUNGARY - A STRUCTURAL EQUATION MODELING APPROACH

TICK Andrea

(ORCID: 0000-0002-3139-6509)

Tick.Andrea@uni-bge.hu

Absztrakt

A digitalizáció nagymértékű elterjedése mind az iparban, mind az üzleti világban a XXI. század második évtizedében, valamint a felsőoktatásban, a tanulási folyamatokban végbemenő digitalizáció az (online) e-learning kurzusok esetén, amely a felsőoktatásban megjelenő oktatási módszertani megújulás része Magyarországon, maga után vonta az e-learning (rendszerek) elfogadás és használat vizsgálatának szükségességét a korai Z generációhoz tartozó magyar diákok között. A cikkben kiterjesztem a TAM modellt olyan külső faktorokkal mint a digitális tanulás, az okos eszközök, az IT biztonságtudatosság, és elemzem, hogy ezen faktorok jelentősen befolyásolják-e a TAM modell endogén változóit a magyar környezetben. A kutatás adatai a SEM modell használatával kerültek feldolgozásra az AMOS programban. Az elemzésem alátámasztja a legtöbb hipotézist, azaz a modell alkalmazható a magyar környezetben. A felsőoktatás stratégiai döntéshozóinak és e-learning fejlesztőinek figyelembe kell venniük a fenti faktorokat az e-learning-es fejlesztések során a magyar felsőoktatásban.

Kulcsszavak: *Kiterjesztett TAM, SEM, e-learning, IT biztonságtudatosság*

Abstract

The massive proliferation of digitilisation in the fields of industry and business in the second decade of the 21st century, the need of the digitalisation of the learning processes using (online) e-learning course in higher education as part of the renewal of education methodologies in Hungary brought along the need for the analysis of the adoption and use of e-learning (systems) among Hungarian students of the early Z generation. This paper aims to extend the TAM model with external factors such as digital learning, smart tools, IT security awareness to see whether these factors have a significant impact on the endogenous factors of the TAM model in the Hungarian environment. The data gathered in the survey was analysed using the SEM with the AMOS software. The analysis supported most of the hypotheses meaning that the model is applicable in the Hungarian context. Strategic decision makers and e-learning developers in higher education should consider the above mentioned factors when developing e-learning in higher education in Hungary.

Keywords: *Extended TAM, SEM, e-learning, IT security awareness*

A kézirat benyújtásának dátuma (Date of the submission): 2018.04.22.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.05.02.

BEVEZETÉS

A digitalizáció minél erősebb előretörésével, az internet technológiák és a kommunikáció technológiák aggregálásával, az okos eszközök és a digitális tanulás összefonódása miatt egyre nagyobb hangsúlyt kap a felsőoktatásban is a digitális és e-learning tanulási formák megerősödése és intenzív integrálása az oktatási, tanulási folyamatban.

A Z generáció sajátosságaiból fakadóan olyan integrált blended learning stratégia kidolgozására, fejlesztésére és alkalmazására van szükség, amely pozitívan, és hatékonyan szolgálja az egyetemi hallgatók tanulását, s később a munkaerő piacon való sikerességét. Ennek szerves részét képezi a digitális, e-learning kurzusok fejlesztése, és integrálása az egyetemi oktatásba. Az elmúlt évtizedben a magyar felsőoktatásban az egyetemek stratégiák kidolgozásával, jó gyakorlatok alkalmazásával és fejlesztésekkel igyekeztek ezen célkitűzéseket elérni. Az egyetemek erőfeszítésének sikeressége azonban nem csak az egyetemen bevezetett e-learning rendszerek és kurzusok számától, mennyiségétől, színvonalától és azok oktatásba való integráltságától függ, hanem attól is, hogy a hallgatók mennyire fogadják el az e-learning alapú oktatást, mennyire tartják könnyűnek, hasznosnak a rendszert és a kurzusokat, illetve mennyire hajlandóak ezeket a rendszereket használni. A hallgatói igények felmérése központi szerepet kap. Ezzel párhuzamosan nem csak a hallgatók viselkedése befolyásolhatja az e-learning típusú tanulás sikerességét, ahol a tanár és a diák időben és fizikailag, vagy akár mindkét szempont szerint is távol van egymástól, a diák részben önállóan, saját tempójában halad a tananyag elsajátításában, hanem a használt eszközök típusa, az IT biztonság kérdése, és a tanulási preferenciák is.

A Z generáció azon tagjai, akik már beléptek a felsőoktatásba, a generáció elsőszülöttjei, így a digitális migránsok és a bennszülöttek között egy átmeneti generációt alkotnak, amely még magán hordozza a hagyományos tanulás preferenciáit, de a digitális eszközök, okos eszközös elterjedésének, az internet és a hiperlinkek a mindennapi életünkbe való beszivárgásának köszönhetően már igénylik az akár tisztán e-learning alapú tanulás, a digitális tanulás eszköztárát is [1].

Magyar környezetben kevés olyan kutatással találkozunk, amely a Technológia Elfogadásai Modellt (TAM)[1] [2] alkalmazza strukturális egyenlet modellezéssel (SEM)[2] konfirmatív faktoranalízisre az SPSS AMOS programmal. A SEM Strukturális Egyenlet Modellezés egy olyan regresszió alapú többváltozós technika, amely útelemzést alkalmaz (path analysis) [3]. A különböző látens változók között ok-okozati összefüggéseket feltételezünk, amely alapján regressziós egyenleteket ír fel a szoftver. A modell grafikus megjelenítése egy irányított gráf, amelyben a csúcsok a változók és az irányított élek lesznek a regressziós együtthatók. Általában konfirmatív faktoranalízisre használjuk. A TAM szerint meghatározott faktorokat az AMOS program segítségével a SEM használatával ellenőrizzük és határozzuk meg a modell helyességét és elfogadhatóságát. Magyar viszonylatban ilyen típusú kutatást találunk például média elfogadásról [4], marketing kommunikáció alkalmazásáról [5] turizmusban a technológia elfogadásról [6], az innováció elfogadásról [7], maguknak a modelleknek az összehasonlításáról [8], valamint egy romániai magyar nyelvű, a mobilapplikációk fogyasztói elfogadásának kutatására vonatkozólag [9], azonban az e-learning oktatási forma elfogadásának, használatának ilyen szempontú vizsgálatára nem találunk példát.

---

[1] A „Technology Acceptance Model” rövidítése, mely a számítógép használatát, annak használati hajlandóságát vizsgálta az érzékelt használati hasznosság és az érzékelt könnyű használat függvényében. A modellt a szerző többször is továbbfejlesztette.

[2] A strukturális egyenlet modellezés kifejezés az SPSS terminológiája.
http://clementine.hu/amos/uncategorised/amos

A TAM (Technológia Elfogadási Modell) használhatóságát, melyet Davis [2] vezetett be munkahelyi környezetre, annak magyarázó erejét webes, online és e-learning környezetben többször számos kutató alátámasztotta [10]. Ezen kutatások alapoztak az internet használat globális mivoltára, azonban nem terjednek ki a lokális különbségekre, beleértve a kulturális, helyi intranet, extranet, internet és okos eszköz használati különbségeket is. Számos eredmény született [10,11,12,13], mely alátámasztja, hogy az eredeti modellben külső változóknak definiált faktor körét kibővítsük, egyrészt kulturális szempontokkal, másrészt olyan, a digitalizációval kapcsolatos szempontokkal, melyek ma meghatározóak az internet, a közösségi média vagy az e-learning rendszerek használatánál. Ilyen szempontok az okos eszközök használata, a digitális tanulás jellemvonásai és az IT biztonságtudatosság.

Mindezek fényében a TAM modellt ezen faktorokkal bővítettem ki, s vizsgáltam meg, hogyan befolyásolják az e-learning rendszerek használati hajlandóságát, az érzékelt könnyű használatát és az érzékelt hasznosságát a magyar diákok körében.

KUTATÁS MÓDSZERTANA

A kutatás két budapesti egyetem hallgatói felmérésével történt, a Budapest Gazdasági Egyetem és az Óbudai Egyetem nagyrészt elsőéves hallgatói között, de a válaszadók között 5. és 6. szemeszterben tanuló válaszadót is találunk, illetve néhány mesterképzéses hallgatót is. A kérdőív módszertana, az adatgyűjtés és adatmenedzsment, valamint az általános rész részletes bemutatására és kiértékelésére egy korábbi cikkben [1] került sor. A hallgatók számítógép/IT és internet kompetenciáinak, digitális írástudásának elemzése, valamint e-learning rendszerek és kurzusok elérésének módja szintén egy korábbi cikkben bemutatásra került [14], azonban az IT biztonságtudatosság és a digitalizáció szerepe további vizsgálatokat kíván. A cikk további fejezeteiben ezen vizsgálatok kerülnek bemutatásra, valamint a modellben létrejött endogén és exogén változók kapcsolatrendszerének feltárása.

AZ IT BIZTONSÁGTUDATOSSÁG ÉS A DIGITALIZÁCIÓ

Az IT biztonságtudatosság és a digitalizáció kérdéskörében a kérdőív összesen hét kérdést tartalmazott, melyek a faktorelemzés során egy exogén változót, faktort (IT) alkottak. Ezen faktornak a további, a kiterjesztett modellben használt exogén változókra gyakorolt hatását [14] elemezte.

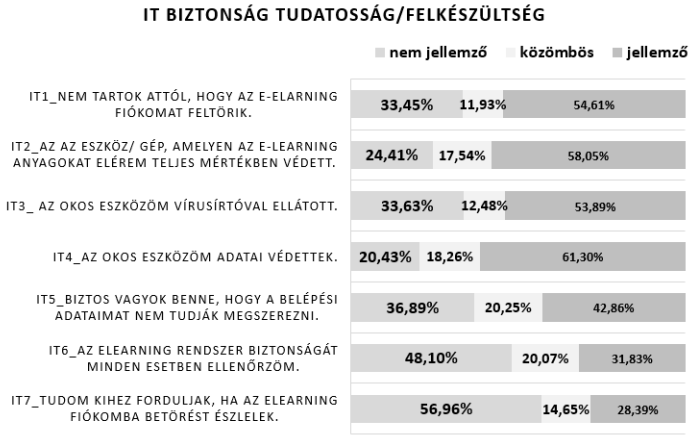
Az e-learning használatával kapcsolatos IT biztonságra vonatkozó kérdések esetén az 1. táblázat mutatja, hogy a hallgatók biztosak abban, hogy az okos eszközeiken lévő adatok, és egyben az okos eszközeik is, amelyeken az e-learning anyagokat, kurzusokat elérik védettek, azonban tartanak attól, hogy adataikat feltörhetik, de mégsem ellenőrzik, hogy az e-learning rendszer védett-e. A vizsgálatból egyértelműen kiderült, hogy a hallgatók nincsenek tisztában azzal, hogy kihez forduljanak, ha IT biztonsági problémával találkoznak. Itt kaptuk a hetes skálán mért válaszokból a legalacsonyabb átlagot, és a legnagyobb pozitív ferdeséget, mely a nem jellemző válaszok többségét igazolja. Ezen a területen mindenféleképpen szükséges az egyetemeken a részletesebb tájékoztatás, és a hallgatók felkészítése.

IT biztonság tudatosságra vonatkozó kérdések

	Átlag	Ferdeség
IT1 [Nem tartok attól, hogy az e-elarning fiókomat feltörik.]	4,56	-,378
IT2 [Az az eszköz/ gép, amelyen az e-elarning anyagokat elérem teljes mértékben védett.]	4,69	-,431
IT3 [Az okos eszközöm vírusirtóval ellátott.]	4,56	-,358
IT4 [Az okos eszközöm adatai védettek.]	5,01	-,566
IT5 [Biztos vagyok benne, hogy a belépési adataimat nem tudják megszerezni.]	4,12	-,084
IT6 [Az elearning rendszer biztonságát minden esetben ellenőrzöm.]	3,64	,232
IT7 [Tudom kihez forduljak, ha az elearning fiókomba betörést észlelek.]	3,29	,487

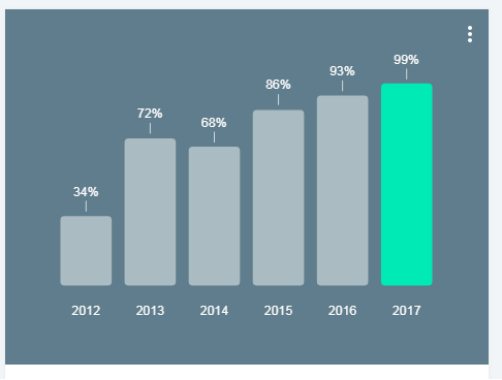
1. táblázat IT biztonságtudatosságra vonatkozó válaszok átlaga és ferdesége (saját szerkesztés)

Az 1. ábra mutatja részletesen a hallgatói válaszokat. A vizsgálat során a hallgatók IT biztonságtudatosságra vonatkozó válaszait 3 csoportba osztottam, „jellemző", „közömbös" és „nem jellemző" kategóriákba. A 1-7-es Likert skálán adott válaszok esetén azon hallgatók, akik 1-3-ig válaszoltak, a „nem jellemző" kategóriába, az 5-7-ig adott válaszok esetén a „jellemző", a 4-es választ adók pedig a „közömbös" kategóriába kerültek. Ezzel a kategorizálással a válaszok egyértelműbben értelmezhetők.



1. ábra IT biztonságtudatosság (saját szerkesztés)

A válaszok alapján a hallgatók számára nem közömbös, hogy a személyes adataik védettek-e, illetve fontos számukra, hogy vírusirtó programot telepítsenek az okos eszközeikre. A felmért hallgatók kétharmada (68%) nem ellenőrzi, illetve közömbös aziránt, hogy az e-learning rendszer biztonságos-e, van-e tanúsítványa, és a hallgatók csak 28,39%-a tudja, hogy kihez forduljon, ha betörést észlel az e-learning fiókjába. Pozitívan értékelendő, hogy a hallgatók körülbelül fele fontosnak tartja az IT biztonsági problémákat, mint pl. adatvédelem, okos eszköz védelme, vagy vírusirtó telepítése azon az eszközön, amelyen az e-learning rendszert használja. A vizsgált hallgatók kb. 70%-a okos eszközön éri el az általa használt e-learning rendszert [1], míg a Google Fogyasztói Barométere szerint [15] 2017-ben a magyar 25 év alatti lakosság 99%-a rendelkezett okos telefonnal (2. ábra).



2. ábra Magyarországon a 25 év alatti lakosság okos telefon ellátottsága [15]

A hallgatók további biztonságtudatossággal kapcsolatos elemzéséhez klaszteranalízist hajtottam végre. A vizsgált változók esetén a „Nem tartok attól, hogy az e-learning fiókomat feltörik" változó esetén a többi változóval szükséges korreláció nem érte el a kívánt 0,3-as szintet, így ezt a változót kivettem a klaszterelemzésből. A klaszterek elkészítéséhez így már a változók megfelelő módon korreláltak egymással, nem volt túl erős a korreláció sem, azonban több kiugró értékem maradt a Mahalanobis távolsággal számolva, így a kiugró és extrém

értékeket is kizártam, amely kb. 50 eset kizárását eredményezte, így 503 fős lett a klaszter alapjául szolgáló minta. A 7. kérdés (IT7) esetén a korreláció nem mindenhol érte el a kívánt értéket, viszont az IT biztonságtudatosság fontossága szempontjából a kérdést a vizsgálatban hagytam [16]. A 2. táblázat mutatja a kérdések közötti korrelációt.

Korreláció az IT biztonságtudatosság kérdései között						
	IT2	**IT3**	**IT4**	**IT5**	**IT6**	**IT7**
IT2	1					
IT3	0,379	1				
IT4	0,48	0,695	1			
IT5	0,426	0,41	0,608	1		
IT6	0,351	0,395	0,491	0,675	1	
IT7	0,281	0,232	0,279	0,376	0,478	1

2. táblázat Az IT biztonságtudatosság kérdései közötti korreláció (saját szerkesztés)

A klaszterelemzés során a Ward és a Centroid módszert is lefuttatva, illetve diszkriminancia elemzéssel visszaellenőrizve 3 csoport kialakítása tűnt megfelelőnek. Mindkét módszer hasonló klaszтereket határozott meg, a klaszterek sorrendjében volt eltérés. A kérdések közötti lineáris kapcsolat szignifikánsnak bizonyult (F-test p=0,000). A K közép módszerrel kapott első csoportba (ők voltak a második csoport a Ward módszerrel) azok a hallgatók tartoznak, akik egyáltalán nem biztonságtudatosak, nevezzük őket „Nem törődöm" csoportnak, azaz nem foglalkoznak azzal, hogy biztonságban vannak-e az adataik, védett-e az eszköz, amelyen az e-learning rendszert elérik, nem ellenőrzik a rendszer biztonságát, illetve nem is tudják, kihez forduljanak, ha biztonsági problémával találkoznak. Az Ő esetükben szükséges a legrészletesebb tájékoztatás, az informatika biztonságra, annak fontosságára való figyelem felhívás, és tréning tartása, melyen biztonsági kérdésekkel kapcsolatos gyakorlati képzést kaphatnak. Az elemzés során ez a csoport lett a legkisebb létszámú. A másik két csoport közötti legmarkánsabb különbség a biztonsági probléma riportálása esetén van. A harmadik csoport a „Biztonságtudatos" csoport, hiszen minden kérdésre adott válaszuk esetén az átlag 6 körül van, bár itt is a legalacsonyabb átlagot az IT7-es kérdés esetén látjuk. Ők úgy gondolják, ha megtettek minden lépést az adatvédelem, gépvédelem stb. kapcsán, akkor biztonságban tudhatják elektronikus adataikat. A második csoport esetén (Ward módszer szerint az első) nem kapunk ilyen homogén átlagértékeket, ők több biztonsági kérdéssel tisztában vannak, az alapvető biztonsági lépéseket megteszik, de „Kételkedők", hiszen annak ellenére nem biztosak abban, hogy adataik védettek, hogy telepítenek vírusirtót, illetve védik okos eszközeiket. Ők vannak a legnagyobb létszámban.

Az 1. csoport ugyan létszámában a legkisebb, azonban viselkedésében a legnagyobb IT biztonsági kockázatot jelenti, hiszen a legjobb táptalaja a fertőzésnek, illetve a rendszer továbbfertőződésének. A 3. csoport a második legveszélyesebb IT biztonság szempontjából, mert ugyan bizonyos mértékig védekeznek, de a védelem nem koherens, ezért rendszerük sérülékenységének valószínűsége reális veszély és nagy számuk jelentős kockázat forrása lehet.

A klasztercsoportok ellenőrzése során a normális eloszlás és a homoszkedaszticitás feltételek nem teljesülése miatt logisztikus regresszió futtatására volt szükség, azonban ebben az esetben is hasonló eredményt kaptunk, így a diszkriminancia szerinti eredményeket mutatom be (3.-5. táblázat, 3. ábra). A három klaszter meghatározó dimenzióit el tudjuk nevezni „személyes érintettség" (vízszintes dimenzió) és a „technikai védelem" (függőleges dimenzió) néven.

Eigenvalues

Function	Eigenvalue	% of Variance	Cumulative %	Canonical Correlation
1	3,141[a]	91,8	91,8	,871
2	,280[a]	8,2	100,0	,468

a. First 2 canonical discriminant functions were used in the analysis.

Wilks' Lambda

Test of Function(s)	Wilks' Lambda	Chi-square	df	Sig.
1 through 2	,189	829,874	12	,000
2	,781	122,933	5	,000

3. táblázat Ward módszer szerinti klaszterek elválasztó dimenzióinak sajátértéke és jelentősége[3]

Struktúra mátrix

	Függvények	
	1	2
IT5 [Biztos vagyok benne, hogy a belépési adataimat nem tudják megszerezni.]	,513*	,056
IT6 [Az elearning rendszer biztonságát minden esetben ellenőrzöm.]	,496*	,186
IT2 [Az az eszköz/ gép, amelyen az e-elarning anyagokat elérem teljes mértékben védett.]	,300*	-,189
IT7 [Tudom kihez forduljak, ha az elearning fiókomba betörést észlelek.]	,467	,721*
IT3 [Az okos eszközöm vírusírtóval ellátott.]	,498	-,637*
IT4 [Az okos eszközöm adatai védettek.]	,537	-,628*

Pooled within-groups correlations between discriminating variables and standardized canonical discriminant functions
Variables ordered by absolute size of correlation within function.

*. Largest absolute correlation between each variable and any discriminant function

4. táblázat Ward módszer szerinti klaszterek elválasztó dimenzióihoz tartozás

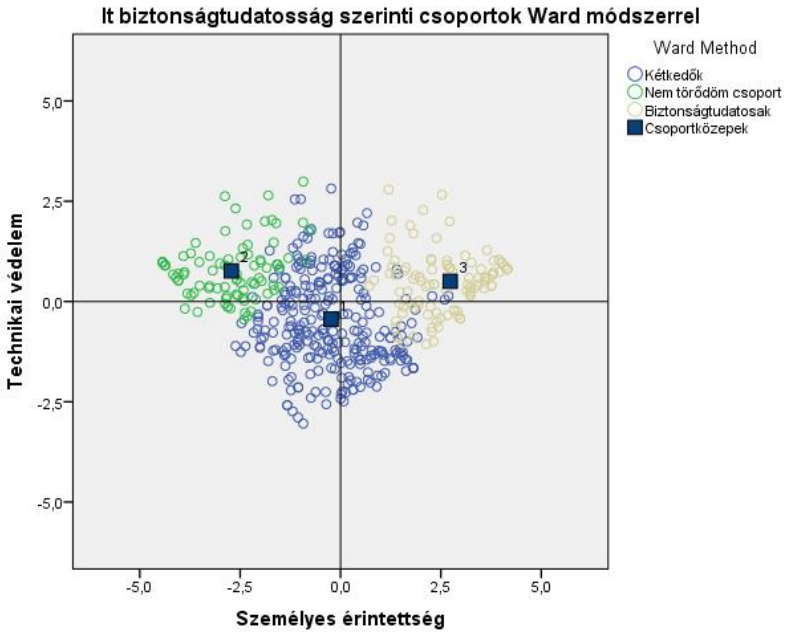
Functions at Group Centroids

Ward Method	Function	
	1	2
1	-,236	-,439
2	-2,721	,764
3	2,732	,503

Unstandardized canonical discriminant functions evaluated at group means

5. táblázat Csoportközepek koordinátái 2 elválasztó függvény esetén

[3] A Wilks' Lambda értéke alapján annál jobb a függvény, minél alacsonyabb a Wilks' lambda értéke, mert ekkor nagyobb a csoportok közötti különbség.



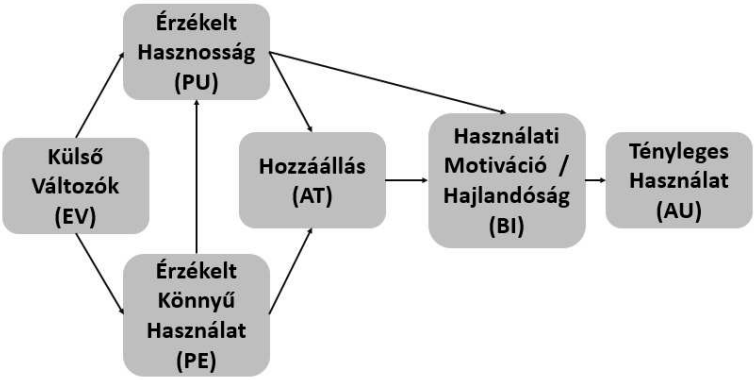
3. ábra IT biztonságtudatos csoportok elhelyezkedése a két dimenzió szerint

A személyes érintettség dimenzió mellett egyértelműen sokkal jobban elkülönülnek a csoportok, mint a technikai védelem dimenzió mentén. Feltételezhetően több hallgató úgy gondolja, ha megtette a technikai lépéseket, biztonságban tudhatja az adatait és nem kell tovább törődnie a védelemmel. A nemtörődömség nem jelenti feltétlen, hogy a hallgató által használt okos eszközök, gépek nem védettek, inkább a biztonságtudatosság hiányát feltételezi a hallgatók körében.

A KITERJESZTETT TAM MODELL

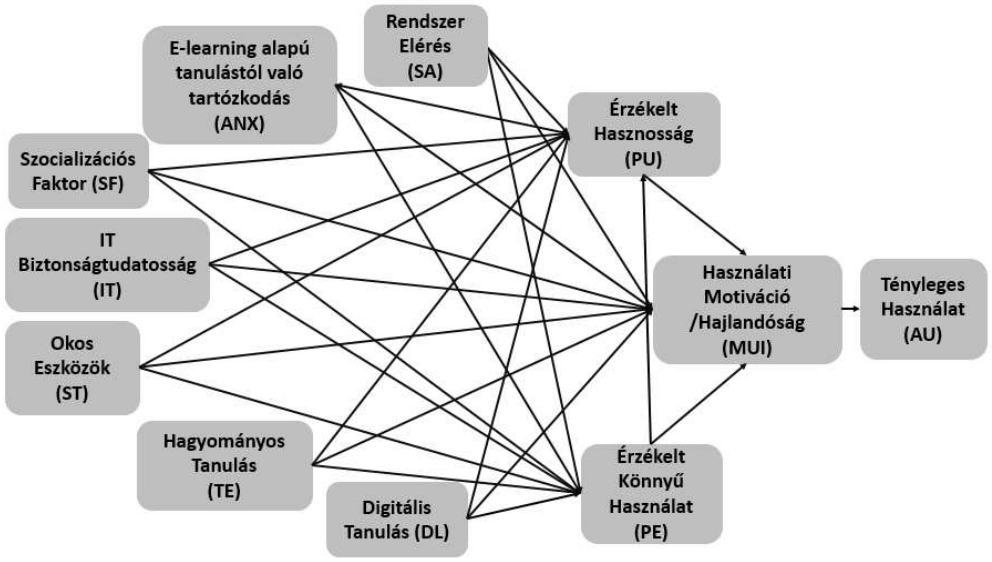
A Technológia Elfogadási Modell kidolgozása Davis [2] nevéhez fűződik, melyet több ízben átdolgoztak és további szempontokat is figyelembe vettek, melyek helyi kontextusban megjelenítik a különbségeket. A kutatás harmadik lépéseként [1,14] ezen modell alkalmazásával vizsgáltam, hogy a különböző exogén változók milyen hatással vannak az endogén változókra, melyek szignifikánsak, és melyeket érdemes illetve nem érdemes a modellben hagyni.

Az eredeti Davis által megadott faktorokat részben elfogadottnak tekintettem (4. ábra), összevontam az attitűd és a használati motivációt és endogén változóként használtam a Strukturális Egyenlet Modell (SEM) elemzéséhez.



4. ábra TAM Modell Davis alapján (szerző szerkesztése [2] alapján)

A kérdőív összeállításánál alapul vettem az eredeti [2] kérdőívet, e-learning rendszerek használatára adaptáltam, illetve kiegészítettem a kérdéseket a kiterjesztéshez szükséges faktorokhoz. Az eredeti, illetve a módosított modellhez tartozó kérdések alapját a már korábban használt kérdések alkották, amelyeket módosítottam e-learning környezetre [2, 17, 18, 19, 20]. Az új faktorokhoz (IT, DL, ST, TE) új kérdések készültek (5. ábra).



5. ábra Kiterjesztett TAM modell DAVIS modelljéből indulva (saját szerkesztés)

A közös külső tényezőket végül hét különböző bemeneti faktorra bontottam, ahol minden faktorhoz 4-6 kérdés tartozott:

1. Rendszer elérés (SA) – az egyetemen illetve online e-learning rendszerek elérhetősége
2. Szocializációs faktor (SF) – pl. önálló vagy közös/csoportos tanulás, személyes kontaktus stb.
3. IT biztonságtudatossági kérdések (IT) – adatvédelemmel, rendszervédelemmel kapcsolatos kérdések
4. Digitális jellemzők (DL) – a Z generációra jellemző, digitális tanulási stratégiákra vonatkozó kérdések
5. Okos eszközök (ST) – a digitális boom eredményeként a Z generáció tagjai, mint digitális bennszülöttek az okos eszközöket egyre nagyobb mértékben használják tanulásra is
6. E-learningtől való tartózkodás (ANX) – a nem magabiztos digitális írástudás, a nem megfelelő internet használati magabiztosság hatással lehet ezen rendszerek használatára
7. Hagyományos tanulás (TE) – a korai Z generáció tagjai részben még preferálják a hagyományos tanulási formát, abban szocializálódtak

A faktorok létrehozása a kérdések alapján főtengelyelemzéssel, 10 faktor kiválasztásával és Promax rotációval történt. A 10 faktorba beletartoznak az endogén változók is, azaz az Érzékelt Hasznosság (PU), az Érzékelt Könnyű használat (PE) és a Használati Motiváció/Hajlandóság is (MUI). A tényleges használatra vonatkozó kérdések itt nem kerültek elemzésre.

A kérdések erre a 10 faktorra illeszkedtek, az eredeti változók információtartalmának 56,635%-át tartották meg, így elfogadtam a faktorokat, azonban konfirmatív elemzéssel SEM modellt alkalmazva ellenőriztem, hogy a modell illeszkedik-e az eredeti adataimra, és elfogadható, alkalmazható-e. A faktorsúlyok átlagai 0,6 felett voltak, illetve egy faktornál sem

volt 0,3-nál alacsonyabb faktorsúly. Ezek az értékek még elfogadhatóak. A korrelációs mátrixban nem volt 0,7 feletti érték, ez szintén megfelelő a faktorok elfogadásához. A faktorok létrehozásánál ügyeltem arra, hogy egy-egy kérdés több faktorhoz ne tartozzon túl nagy súllyal, ne legyen keresztfaktor kapcsolat. Ennek érdekében inkább kizártam egy-egy kérdést, mely nagyon elhúzta volna a modellt. Az így kialakított 10 faktoros modellre állítottam fel a hipotéziseket, és vizsgáltam meg az AMOS programmal.

A hipotézisek

A vizsgálat során a következő hipotéziseket állítottam fel az endogén változókra:

H_1: A használati motiváció/ hajlandóságot (MUI) befolyásolja az érzékelt hasznosság (PU) (H_{11}), az érzékelt könnyű használat (PE) (H_{12}), a szocializációs faktor (SF) (H_{13}), az IT biztonságtudatosság (IT) (H_{14}), a digitális jellemzők (DL) (H_{15}), a hagyományos tanulás tényezők (TE) (H_{16}), a rendszer elérés (SA) (H_{17}), az e-learning tanulási formától való tartózkodás (ANX) (H_{18}), és az okos eszközök használata (ST) (H_{19}) a magyar hallgatók esetében.

H_2: A magyar egyetemista hallgatók esetén az érzékelt hasznosságot (PU) befolyásolja, a szocializációs faktor (SF) (H_{21}), az IT biztonságtudatosság (IT) (H_{22}), a digitális jellemzők (DL) (H_{23}), a hagyományos tanulás tényezők (TE) (H_{24}), a rendszer elérés (SA) (H_{25}), az e-learning tanulási formától való tartózkodás (ANX) (H_{26}), az okos eszközök használata (ST) (H_{27}), és az érzékelt könnyű használat (PE) (H_{28}).

H_3: Az érzékelt könnyű használatot (PE) a magyar hallgatók esetén befolyásolja a szocializációs faktor (SF) (H_{31}), az IT biztonságtudatosság (IT) (H_{32}), a digitális jellemzők (DL) (H_{33}), a hagyományos tanulás tényezők (TE) (H_{34}), a rendszer elérés (SA) (H_{35}), az e-learning-től való tartózkodás (ANX) (H_{36}), és az okos eszközök használata (ST) (H_{37}).

Az elemzés megkívánta, hogy az exogén változók közötti kapcsolatokat is vegyük fel a kapcsolatok vizsgálatánál. Ezek bejelölésre kerültek, azonban jelen cikkben az endogén változókra vonatkozó hatásokat vizsgálom.

EREDMÉNYEK

Általános eredmények

Az eredmények értékeléséhez a modell érvényességét, valamint illeszkedését is meg kellett vizsgálni, hiszen a futtatás során előfordulhat, hogy olyan faktorok maradnak a modellben, amelyek nem megbízhatóak, illetve rontják a modell illeszkedését, jóságát.

Modell megbízhatóság és érvényesség

A modell és a faktorok megbízhatóságát a Cornbach alpha illetve a CR (Composite Reliability)[4] értékekkel vizsgáltam meg. A Cronbach's alpha értéke összességében 0,638-as értéket adott ezekkel a faktorokkal, ami megkérdőjelezheti a megbízhatóságot, de pl. [21] elfogadja a 0,6 és 0,7 közötti értéket is, és mérsékelten megbízhatónak nevezi az ilyen modelleket. Azonban az ANX faktor kivételével a megbízhatóság 0,702-re nő, ami elgondolkodtató, hiszen a Z generáció esetén a részben digitális bennszülötti lét maga után vonja, hogy a számítógépektől, digitális eszközöktől való tartózkodás a minimálisra csökken. Azonban mivel a korai Z

[4] A „Composite Reliability" (összetett, kompozit megbízhatóság) egy átfogó megbízhatósági mutató heterogén, de hasonló faktorok halmaza esetén

generáció átmeneti generációnak tekinthető [1], így a vizsgálatban benne hagytam az ANX faktort, annak ellenére, hogy így a modell megbízhatósága 0,7 alá esett.

A faktorok megbízhatóságának vizsgálatára a Cronbach alpha mellett a CR érték kiszámítása is megtörtént. Amennyiben mind a Cronbach alpha értéket, mind a CR-t figyelembe vesszük, a hagyományos tanulás (TE) faktor nem illik modellünkbe, nem megbízható. Ezt a faktort a modellből kivettem, mivel a vizsgálat során nem bizonyult semmi esetben sem szignifikánsnak, így nincs hatása sem pozitívan sem negatívan az endogén változókra (6. táblázat). A SEM feldolgozása során egyértelműen kiderült, hogy a hagyományos tanulásra (TE) vonatkozó faktort ki kell venni, mert egy újabb másodlagos látens változó meghatározását kívánta volna meg a modell. Azonban a faktor kivétele nem rontotta el a faktorelemezés jóságát: KMO =0,911, Bartlett teszt szignifikáns, 56,52%-ot magyaráz a modell, Cronbach's alpha: 0,691, tehát még javult is a megbízhatóság. A TE faktor elhagyása után a faktorok megbízhatósága kismértékben változott, de így is minden esetben 0,7 feletti értéket kaptunk.

		Eredeti TE faktorral		**TE faktor nélkül**	
Faktorok		**CR**	**Cronbach's α**	**CR**	**Cronbach's α**
PE	Érzékelt könnyű használat	0,902	0,925	0,899	0,925
ST	Okos eszközök	0,847	0,859	0,846	0,859
ANX	E-learningtől való tartózkodás	0,823	0,831	0,825	0,831
PU	Érzékelt hasznosság	0,875	0,895	0,872	0,895
MUI	Használati motiváció/hajlandóság	0,836	0,881	0,834	0,881
IT	IT biztonságtudatosság	0,784	0,775	0,784	0,775
DL	Digitális tanulás	0,783	0,760	0,740	0,760
SF	Szocializációs faktor	0,803	0,801	0,818	0,801
SA	Rendszer elérés	0,821	0,806	0,820	0,806
TE	Hagyományos tanulás	*0,626*	*0,573*	-	-

6. táblázat A faktorok megbízhatósága (saját szerkesztés)

A 9 faktorral történő elemzés során a DL faktorhoz tartozó 4. kérdés kiesett a pattern mátrixban, de a struktúra mátrixban benne maradt, ezért meghagytam a SEM modell alkalmazásakor.

Pattern Matrix										
	Factor				**Factor**				**Factor**	
	1	**2**	**3**		**4**	**5**	**6**		**7**	**8**	**9**
PE3	,804			**MUI2**	,938			**IT4**	,802		
PE6	,800			**MUI3**	,864			**IT5**	,687		
PE4	,798			**MUI1**	,842			**IT6**	,648		
PE5	,760			**MUI5**	,455			**IT3**	,623		
PE1	,739			**MUI6**	,448			**IT2**	,544		
PE2	,737			**MUI7**	,396			**IT7**	,321		
ST2		,879		**MUI4**	,395			**SF2**		,880	
ST3		,871		**PU3**		,993		**SF3**		,832	
ST1		,794		**PU4**		,854		**SF1**		,653	
ST5		,635		**PU1**		,745		**SF4**		,515	
ST4		,483		**PU2**		,539		**SA2**			,905
ST6		,419		**DL3**			,821	**SA3**			,898
ANX3			,861	**DL5**			,818	**SA1**			,482
ANX4			,794	**DL2**			,705				
ANX2			,792	**DL1**			,520				
ANX1			,632								
ANX6			,441								
ANX7			,399								

7. táblázat Faktorsúlyok 9 faktor esetén

Konfirmatív faktorelemzés AMOS programmal

Az elemzés során több ízben változtatni kellett a modell kapcsolati ábráján. Az illeszkedés vizsgálat első lépésében a kovariancia mátrix azt mutatta, hogy az exogén változók is kapcsolatban állnak egymással, így felvettem ezeket a kapcsolatokat is. Ezek a kapcsolatok újabb hipotézisek felállítását tették lehetővé, mely kapcsolatok elemzését mutatja be [14]. A kapcsolatok felvétele javította az illeszkedési mutatókat (a szf.[5] 15-tel nőtt, és a CHI^2 3118 -ról 2788-ra csökkent, a különbség 330, ami jóval több, mint a 15 kétszerese (a 2 szf. közötti különbség)), érdemes volt az exogén változók közötti kapcsolatokat felvenni, azonban a vizsgálat során további javítást jelzett a modell. A faktorsúlyok több helyen alacsonyabbak, mint az elvárt 0,7, azonban az eredeti faktoranalízisben is benne hagytuk a 0,6 alattiakat és a 0,3 felettieket, de annál jobb faktorelemzést nem tudtunk elérni[6].

A modell még mindig javítást igényel, ezért a javasolt modifikációk közül addig végeztem módosítást, amíg már jól illeszkedő modellt kaptam. Az egyedi hozzájárulások között kellett néhányat összekapcsolnom. Mivel fennálltak további olyan kapcsolatok, melyek a modell jóságát növelik, így a hibatagok esetén is felvettem kapcsolatokat. Ezek mind egy faktoron belüli egyedi varianciák közötti kapcsolatok, nincsenek keresztkapcsolatok. Ez a modell már megfelelt több kritériumnak is, a CHI^2 még mindig szignifikáns (CHI^2=2346,408, a szf. még kilenccel csökkent), de a többi mutató már jól illeszkedő modellt mutatott.

SEM modell elemzés és hipotézisek kiértékelése

Az 6. ábra bemutatja a teljes alkalmazott SEM modellt, amely mind a 9 faktort tartalmazza, és amelynek azon része kerül most kiértékelésre, mely az endogén változókra való hatást mutatja.

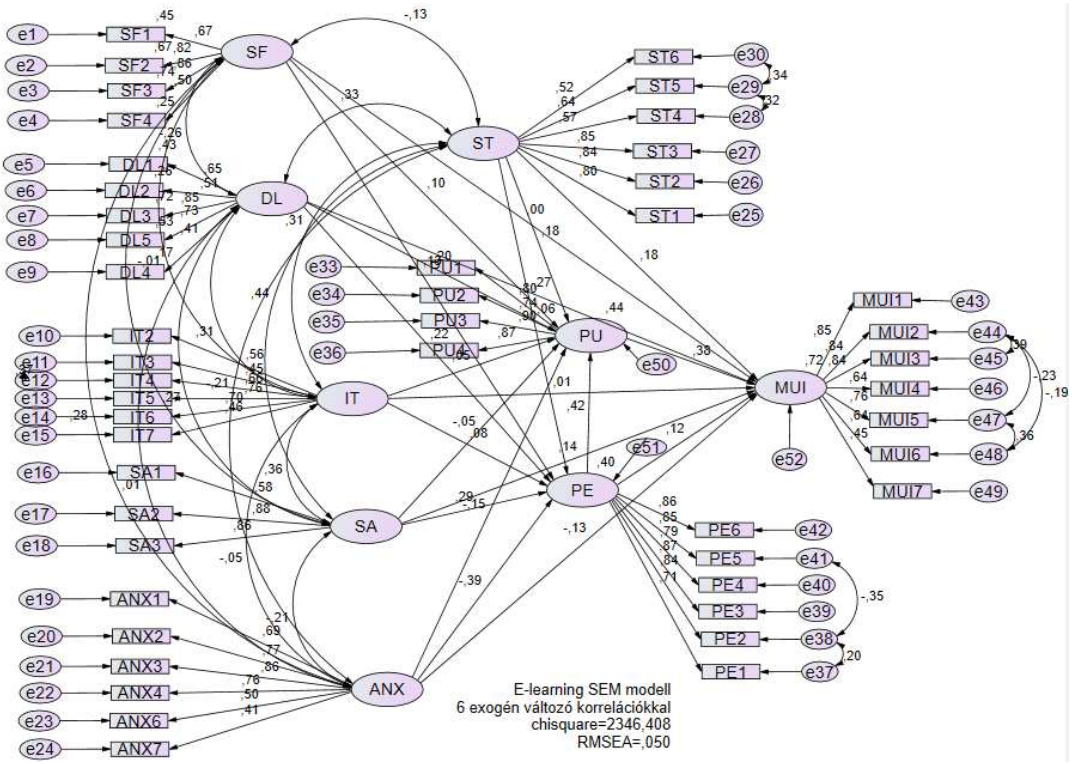
A modell jóságát a CHI^2, RMSA, CFI és IFI mértékkel mértem, ezek a mutatók jó illeszkedést mutatnak a kritériumok szerint (8. táblázat).

Illeszkedési mutató	***Érték***	***Ajánlott érték***
CHI^2	2346,408 (p=0,000)	p>0,05
RMSEA	0,05	<0,10
CFI	0,905	>0,9
IFI	0,906	>0,9

8. táblázat Modell jóságának, illeszkedésének mutatói (saját szerkesztés)

[5] szabadságfok

[6] Minél magasabb a faktorsúlyok értéke, annál jobban meghatározza a modellt, azonban a részletesebb kiértékelés miatt tartottam fontosnak, hogy az alacsonyabb faktorsúlyok is benne maradjanak a modellben.



6. ábra SEM modell kiértékelése AMOS programmal

A strukturális egyenlet modell magyarázó erejét a központi illeszkedés vizsgálat R^2 értéke adja meg. A 9 faktor a Használati Motivációt/Hajlandóságot (MUI) 71,7%-ban magyarázza, amely meghatározó magyarázó erőnek nevezhető. Az érzékelt hasznosságot és az érzékelt könnyű használatot a faktorok együttesen 43,8% illetve 40,4%-ban magyarázzák, amely közepesen erős magyarázó tényezőnek nevezhető. A MUI esetén viszonylag erős az együttes magyarázó erő, a másik két faktor esetén léteznek még más befolyásoló tényezők is. Ezek alapján a három endogén változó esetén jó magyarázó erővel rendelkező modellt kaptunk (9. táblázat).

Faktor	R^2
PU	0,438
PE	0,404
MUI	0,717

9. táblázat A változók/faktorok együttes magyarázó ereje az endogén változókra (saját szerkesztés)

A modellben mind a 8 faktor mérte a MUI faktort, ezek közül az érzékelt hasznosság (0,324) bizonyult a legerősebbnek, majd a digitális tanulás (0,247) és az okos eszközök (0,172) (10. táblázat). Mindhárom esetben szignifikáns a befolyásolás. A faktorok közül az e-learning rendszerektől való tartózkodásnak van negatív befolyásolási hatása, amely szintén magyarázható, hiszen, amennyiben frusztrációt okoz az e-learning rendszer használata a hallgató számára, nem lesz motivált, és nem fogja használni.

Az érzékelt könnyű használat esetén, a legerősebb pozitív befolyást a rendszerelérés jelenti (0,254), a digitális tanulási formák a második legerősebb (0,189) ebben az esetben is az e-learning tanulási formától való tartózkodás közepesen erősen negatívan hat a könnyű használatra (-0,424).

Az érzékelt hasznosság esetén a könnyű használat hatott a legpozitívabban (0,515), a digitális tanulási forma és az okos eszközök használata kevésbé befolyásolja az érzékelt könnyű

használatot (0,211 és 0,204), bár mindkettő szignifikáns. Ebben az esetben is az e-learning tanulási formától való tartózkodás enyhén negatívan hatott az érzékelt hasznosságra (-0,197).

Összességében elmondható, hogy a kiterjesztett modellbe felvett 2 faktor, a digitális tanulási forma (DL), és az okos eszközök (ST), mindhárom endogén változót pozitívan befolyásolja, azaz minél jobban használják a diákok a digitális tanulási formát és az okos eszközöket, annál inkább motiváltak e-learning rendszerek és kurzusok használatára, azokat hasznosnak és könnyen használhatónak tartják.

Kapcsolatok szignifikanciája és erőssége						
Faktor 1 ← Faktor 2	**együttható**	**S.E.**	**z próba**	**P**	**béta érték[7]**	**hipotézis kiértékelése**
MUI ← PU	0,324	0,036	8,878	***	0,38	✓
MUI ← DL	0,247	0,037	6,704	***	0,275	✓
MUI ← ST	0,172	0,035	4,882	***	0,183	✓
MUI ← SA	0,13	0,035	3,674	***	0,143	✓
MUI ← PE	0,122	0,045	2,706	0,007	0,117	✓
MUI ← ANX	-0,146	0,044	-3,318	***	-0,128	✓
PE ← SA	0,254	0,042	6,015	***	0,291	✓
PE ← DL	0,189	0,041	4,571	***	0,22	✓
PE ← SF	0,114	0,038	2,963	0,003	0,13	✓
PE ← ANX	-0,424	0,051	-8,321	***	-0,388	✓
PU ← PE	0,515	0,064	8,073	***	0,42	✓
PU ← DL	0,211	0,051	4,117	***	0,201	✓
PU ← ST	0,204	0,051	4,037	***	0,185	✓
PU ← SF	0,107	0,047	2,281	0,023	0,1	✓
PU ← ANX	-0,197	0,064	-3,071	0,002	-0,147	✓
MUI ← IT	0,007	0,042	0,166	0,868	0,006	nem igazolódott be
MUI ← SF	0,005	0,032	0,143	0,887	0,005	nem igazolódott be
PE ← IT	0,084	0,051	1,638	0,102	0,077	nem igazolódott be
PE ← ST	0,057	0,042	1,357	0,175	0,063	nem igazolódott be
PU ← IT	0,062	0,062	0,997	0,319	0,046	nem igazolódott be
PU ← SA	-0,05	0,052	-0,962	0,336	-0,047	nem igazolódott be

10. táblázat MUI, PE és PU faktorokra ható változók viselkedése (saját szerkesztés)

Az eredeti hipotéziseinkből nem igazolódott be, hogy az IT biztonságtudatosság közvetlenül szignifikánsan befolyásolná az érzékelt hasznosságot, az érzékelt könnyű használatot vagy a motivációt és használati hajlandóságot. Valamint a rendszerelérés (SA) és az okos eszközök (ST) használata sem befolyásolja szignifikánsan az érzékelt hasznosságot, az okos eszközök használata (ST) nem áll szignifikáns kapcsolatban a könnyű használattal. Ez utóbbi meglepő is lehet, hiszen azt várnánk, hogy az okos eszközökre fejlesztett alkalmazások a könnyű használatot erősítik. Valószínűleg a mobil felület még nem teljesen megfelelő, ezért az egyetemeknek stratégiai szempontnak kell tekinteni, hogy az e-learning oktatási formája okos eszközökön könnyen elérhető és használható legyen.

A szocializációs faktor (SF) és a használati motiváció/hajlandóság (MUI) közötti befolyásolás sem igazolódott be, ez a blended learning létjogosultságát erősíti, hiszen a személyes konzultáció, a face-to-face oktatás kedvelése nem erősíti vagy gyengíti az e-learning rendszerek használati hajlandóságát, és ne feledjük, hogy a vizsgálat a Z generáció elsőszülöttjei között történt, akik még átmenetet képeznek a digitális bennszülöttek és a digitális migránsok között.

A legerősebb negatív befolyásolás az e-learningtől való tartózkodás (ANX) és az érzékelt könnyű használat (PE), a legerősebb pozitív befolyásolás pedig az érzékelt könnyű használat (PE) és az érzékelt hasznosság (PU) között van. A digitális tanulás kedvelése erősíti mind a

[7] standardizált regressziós együttható

hasznosságot, mind a könnyű használatot és motivációt. Ez a generáció, mely már szinte digitális bennszülött, szívesen használja az e-learning rendszereket. A szocializációs faktor - a személyes konzultáció, face-to-face oktatás – szintén pozitívan járul hozzá az e-learning rendszerek hasznosságához, érzékelt könnyű használatához és a használati hajlandósághoz, ez megint csak a blended learning erősségét támasztja alá. Ebben az esetben az oktató személyes meggyőző képessége járul hozzá pozitívan az e-learning rendszerek és kurzusok erőteljesebb használatához. A rendszerelérés, a hasznosság és a használati hajlandóság közötti pozitív befolyásolás várható volt, ezt egy korábbi modell is igazolja [17].

A hatás mértékét[8] vizsgálva, amely megmutatja, hogy milyen a prediktív képessége a modellünknek a használati motiváció/halandóság faktorra, azt látjuk, hogy amennyiben [22] által meghatározott értékeket vesszük alapul, mely szerint a 0,02-es érték kicsi, a 0,15-ös közepes és a 0,35-ös határ mértékek erős hatást jelentenek az endogén változóra, hogy majdnem minden esetben közepes vagy erős a hatás. Így a szignifikáns hatásokat figyelembe véve a direkt hatások esetén pozitív erős hatása van a DL és a PU faktoroknak, negatív erős hatása van az ANX faktornak, az összes többi faktornak közepesen erős pozitív hatása van az endogén változókra (11. táblázat).

	ST	**ANX**	**SA**	**DL**	**SF**	**PE**	**PU**
PE		-0,388	0,291	0,22	0,13		
PU	0,211	-0,31		0,293	0,154	0,42	
MUI	0,27	-0,291	0,206	0,412		0,277	0,38

11. táblázat A hatás mértéke az exogén és az endogén változók között[9].

A bemeneti (exogén) faktorok kapcsolatának vizsgálatakor azt tapasztaltam, hogy az IT biztonságtudatosság a digitális tanulással (DL), az okos eszközökkel (ST) és a szocializációs faktorral áll szignifikáns kapcsolatban (12. táblázat), ami a Z generáció esetén nagyon jó visszajelzés, hiszen úgy gondolják azok, akik kedvelik a digitális tanulást, hogy oda kell figyelniük a rendszer biztonságára, az eszköz védettségére. Az IT biztonságtudatosság szintén szignifikáns kapcsolatban áll az okos eszközök (ST) használatára vonatkozó faktorral, ami szintén a Z generáció tudatos rendszerhasználati szokásait erősíti. A kölcsönös kapcsolat jelenti, hogy az IT biztonságtudatosság erősíti a digitális tanulást és az okos eszközök használatát, azaz, minél IT biztonságtudatosabb a hallgató, annál inkább fogja magabiztosan használni az okos eszközöket. Az IT faktor és a rendszerelérés (SA) közötti viszonylag erős pozitív, szignifikáns kapcsolat feltételezhető volt.

[8] „effect size” az AMOS programban
[9] Az üres cellák gyenge, kicsi hatást mutattak, nem szignifikáns a hatás mértéke.

Bemeneti faktorok kapcsolatvizsgálata						
Faktor 1 ↔ Faktor2	**C**	**S.E.**	**z próba**	**P**	**Korreláció**	**hipotézis kiértékelése**
DL ↔ SA	0,623	0,118	5,293	***	0,275	✓
DL ↔ IT	0,563	0,102	5,499	***	0,312	✓
DL ↔ ST	0,726	0,115	6,298	***	0,331	✓
IT ↔ ST	0,529	0,095	5,564	***	0,308	✓
IT ↔ SA	0,642	0,102	6,308	***	0,36	✓
SA ↔ ANX	-0,374	0,09	-4,17	***	-0,209	✓
SA ↔ ST	0,948	0,117	8,135	***	0,438	✓
SF ↔ DL	-0,593	0,119	-4,996	***	-0,262	✓
SF ↔ ST	-0,281	0,106	-2,644	0,008	-0,131	✓
SF ↔ SA	-0,223	0,11	-2,02	0,043	-0,1	✓
SF ↔ ANX	0,504	0,093	5,414	***	0,283	✓
ANX ↔ ST	-0,355	0,086	-4,136	***	-0,206	✓
DL ↔ ANX	0,025	0,09	0,277	0,782	0,014	nem szignifikáns
IT ↔ ANX	-0,068	0,073	-0,935	0,35	-0,048	nem szignifikáns
SF ↔ IT	-0,023	0,092	-0,248	0,804	-0,013	nem szignifikáns

12. táblázat Bemeneti faktorok kapcsolatvizsgálata (saját szerkesztés)

Itt a legerősebb kapcsolat a rendszerelérés (SA) és az okos eszközök (ST) között van (0,948), ami alátámasztja, hogy a Z generáció már kb. 70%-ban okos eszközökön szereti elérni az e-learning rendszereket [1]. Ide tartozik és ezt a Z generációs tulajdonságot erősíti a digitális tanulás és az okos eszközökre vonatkozó faktor közötti szintén erős kapcsolat (0,726). Az e-learning rendszertől való tartózkodás mind az okos eszközök faktorral, mind a rendszereléréssel, mind pedig a szocializációs faktorral negatív kapcsolatban áll.

KÖVETKEZTETÉSEK

A felsőoktatásban tanuló hallgatók egy kb. 600 fős csoportjának e-learning rendszerek, kurzusok használatához való hozzáállását, azaz motivációját, használati hajlandóságát, annak számukra érzékelt hasznosságát és könnyű használatát vizsgáltam a Technológia Elfogadási Modellel és a Strukturális Egyenlet Modellezéssel. A TAM modellt kiterjesztettem olyan külső változókkal, melyek a digitalizáció és az okos boom miatt hatással lehetnek ezen tényezőkre.

Ezen külső változók egyike az IT biztonságtudatosság kérdése különös fontossággal bír a 21. század második évtizedében, ahol az online közösségeknek, a közösségi hálóknak és magának az internetnek az elterjedése, az online lét a Z generáció, mint az első digitális bennszülöttek számára mindennapos, az online lét elkerülhetetlen a számukra. Mindez megnöveli a biztonság szerepének fontosságát, s ebből kifolyólag az IT biztonságtudatosság meglétének fontosságát, ezért ezen kérdéskört részletesebben elemeztem.

A korai Z generáció magyar felsőoktatásban lévő hallgatói körében végzett vizsgálat szerint a hallgatók három csoportra oszthatók IT biztonságtudatossági szempont szerint, vannak a „nem törődöm” hallgatók, akik nem foglalkoznak adatvédelemmel, vírusvédelemmel, elfogadják, hogy az eszközeik védettek, és nem is ellenőrzik a rendszer biztonságát. Az ő számukra a legfontosabb a tájékoztatás, a tréning, mely növeli az IT biztonságtudatosságukat, mely egyre nagyobb jelentőséggel bír a digitális világban. Ők alkotják a felmérés szerint a legkisebb csoportot, azonban ők jelentik a legkockázatosabb csoportot is sérülékenység és vírusfertőzés szempontjából. A „biztonságtudatos” csoport viselkedik a legtudatosabban, ők tesznek meg mindent az adat-, vírus-, és rendszervédelemért, illetve ők a legtájékozottabbak. A „kételkedők” esetén kifejezetten az IT biztonságtudatod kell erősíteni, hiszen ők tájékozottak, védik az adataikat, a rendszerüket, de nem bíznak a rendszerben. Számuk nagy a felmérés szerint és ezen csoport esetében kérdőjelezhető meg a koherens védelem megléte, így az általuk használt rendszerek sérülékenységének valószínűsége is reális.

A általam kidolgozott újszerűen 5 változóval kiterjesztett TAM modell jól mutatja a hallgatók körében a megadott exogén változók hatását az endogén változókra. A modell alkalmazása az e-learning használatával kapcsolatos vizsgálatnak jól megfelelt, megfelelően mérhetővé vált a kiterjesztett modell exogén változóinak hatása az endogén változókra a magyar környezetben.

Az e-learning használati motivációját/hajlandóságát, hasznosságát és könnyű használatát feltáró TAM modell kiértékelése során a felállított hipotézisek közül szignifikánsnak bizonyult a digitális tanulás (DL) befolyása az endogén változókra (H_{15}, H_{23}, H_{33},), az okos eszközök (ST) használatának befolyása az érzékelt hasznosságra és a használati hajlandóságra (H_{19}, H_{27},). Továbbá beigazolódott a három endogén változó esetén a PU és PE hatása a MUI változóra (H_{11}, H_{12}, H_{28}), a rendszer elérés (SA) hatása a MUI és PE változókra, (H_{17}, H_{35}), az ANX azaz az e-learning rendszertől való tartózkodás negatív befolyásolása mindhárom endogén változóra (H_{18}, H_{26}, H_{36}), valamint a szocializációs faktor hatása (H_{21}, H_{31}). Azonban nem igazolódtak be a hagyományos tanulással kapcsolatos hipotézisek (H_{16}, H_{24}, H_{34}), az IT biztonságtudatosság kapcsolatos hipotézisek (H_{14}, H_{22}, H_{32}) valamint a H_{13} (SF → MUI), a H_{25} (SA → PU) és a H_{37} (ST → PE).

Mindemellett a modell szerint az IT biztonságtudatosság szignifikáns kapcsolatban áll a kiterjesztett modell exogén változóival, úgymint a digitális tanulás (DL), az okos eszközök (ST), a rendszer elérés (SA), de nem áll kapcsolatban a személyes érintettséggel, azaz az e-learning rendszertől való tartózkodás (ANX) illetve a szocializációs faktor (SF) változókkal. Az endogén változókra az IT biztonságtudatosság nincs szignifikáns befolyásolással, csak közvetve hat rájuk, azaz közvetve gyakorol hatást az e-learning érzékelt hasznosságára, a könnyű használatára és az e-learning használati motivációjára, hajlandóságára. Az e-learning rendszerek érzékelt hasznosságát, könnyű használatát és használati hajlandóságát határozottan negatívan befolyásolja a rendszertől való tartózkodás, azaz, ha nem magabiztos a hallgató, akkor inkább nem használja a rendszert. A magyar hallgatókat vizsgálva is erős befolyásolás áll fenn az érzékelt könnyű használat, az érzékelt hasznosság és a használati hajlandóság között, mely alátámasztja az eddigi TAM és SEM modellek használatát és magyarázó erejét. A digitális tanulási forma előretörése és egyre nagyobb népszerűsége erős befolyással van az e-learning rendszerek használati hajlandóságára, és méréskelten járulnak hozzá az érzékelt hasznossághoz és az érzékelt könnyű használathoz. A könnyű használatot inkább a rendszerelérés milyensége határozza meg.

A vizsgálat eredményeként elmondhatjuk, hogy a Z generáció jelenleg a felsőoktatásban lévő hallgatói számára az egyetemeken figyelmet kell szentelni az IT biztonságtudatosság fejlesztésére, az e-learning stratégia kialakításánál figyelembe kell venni, hogy ezen hallgatók egyre inkább a digitális tanulás felé fordulnak, amelyet az okos eszközeiken szeretnének elérni, azonban az e-learning oktatási forma esetén is szükségük van a személyes kontakt lehetőségére.

A modell alapján elmondható, hogy a digitalizáció, az okos eszközök segítenek a hallgatóknak, hogy az e-learning rendszerek, kurzusok használatára motiváltabbak legyenek, ezen rendszerek elérése is könnyebb, ha a megfelelő fejlesztések végbemennek.

FELHASZNÁLT IRODALOM

[1] TICK, A.: *Research on the Digital Learning and E-learning Behaviour and Habits of the Early Z Generation*, 22nd IEEE International Conference on Intelligent Engineering Systems, (2018) (megjelenés alatt)

[2] DAVIS, F. D.: *Perceived usefulness, perceived ease of use, and user acceptance of information technology*, MIS Quarterly, Abi/Inform Global, 13 (3), (1989) 319-339. o.

[3] TÁNCZOS, E.: *Látens változós modellezés,* diplomadolgozat, ELTE, 2009

[4] NYÍRŐ, N.: *Médiatechnológiai innovációk elfogadása és terjedése*, Budapesti Corvinus Egyetem, PhD., 2011

[5] BERNSCHÜTZ, M.: Az integrált marketingkommunikáció alkalmazásának strukturális modellje, PhD., 2011

[6] RÁTHONYI, G.: *Innovatív információtechnológiák alkalmazása a turizmus menedzsmentben,* DE, 2016

[7] GERDERICS, V., PAVLUSKA, V.: Irodalomkutatás az innováció elfogadás-elméletekről, PTE, 2013

[8] KESZEI, T, ZSUKK, J.: *Az új technológiák fogyasztói elfogadása, A magyar és nemzetközi szakirodalom áttekintése és kritikai értékelése,* Vezetéstudomány, XLVIII. 10. (2017)

[9] HÉGEN-SZÉNÁS E.A., SEER, L.: *Mobilalkalmazások elfogadását befolyásoló tényezők romániai középiskolások és egyetemi hallgatók körében*, Közgazdász Fórum. 19 (126), (2016/1) 55-80. o

[10] TARHINI, A. et.al.: Extending the TAM model to empirically investigate the students' behavioural intention to use e-learning in developing countries, Science and Information Conference, (2013), London (UK) DOI: http://dx.doi.org/10.5539/ijbm.v11n2p299

[11] LI N., KIRKUP G.: *Gender and cultural differences in Internet use: A study of China and the UK,* "Computers & Education", 48. (2007), DOI:10.1016/j.compedu.2005.01.007

[12] AKOUR, I.A., DWAIRI, M. A.: *Testing Technology Acceptance Model in Developing Countries: the Case of Jordan*, International Journal of Business and Social Science 2 (14), 2011, 278-284.o.

[13] STRAUB, D., KEILE, M., BRENNER, W.: *Testing the technology acceptance model across cultures: A three country study,* Information & Management, 33 (1), (1997), 1-11.o. DOI: https://doi.org/10.1016/S0378-7206(97)00026-8

[14] TICK, A.: *IT Security as a Special Awareness at the Analysis of the Digital/E-learning Acceptance Strategies of the Early Z Generation*, 22nd IEEE International Conference on Intelligent Engineering Systems, (2018) (megjelenés alatt)

[15] Google, Consumer Barometer with Google, (2018), https://www.consumerbarometer.com/en/trending/?countryCode=HU&category=TRN-AGE-UNDER-25, (letöltve: 2018. április 20.)

[16] JAKUS, A., TICK, A.: *IT biztonsági kockázatok és kockázatkezelés*, Hadmérnök, XII. 1. (2017), 182-202. o.

[17] PARK, S. Y.: *An analysis of the Technology Acceptance Model in understanding university students' behavioural intention to use e-learning,* Educational Technology & Society, 12 (3), (2009), 150-162.o. DOI: https://www.learntechlib.org/p/75428/.

[18] OLIVIER, J.: *Blended learning in a first-year language class: Evaluating the acceptance of an interactive learning environment*, Literator-Journal of Literary Criticism, Comparative Linguistics and Literary Studies 37(2), (2016) 1-12.O. DOI: a1288. http://dx.doi.org/10.4102/lit.v37i2.1288

[19] TARHINI, A. et.al.: *Factors affecting students' acceptance of e-learning environments in developing countries: A structural equation modeling approach*, International Journal of Information and Educational Technology, 3(1), (2013), 54-59. o. DOI: 10.7763/IJIET.2013.V3.233

[20] MALHOTRA, Y., GALETTA, D.: *Extending the Technology Acceptance Model to Account for Social Influence: Theoretical Bases and Empirical Validation*, Computers in Human. 23 (10), 1999, DOI: 10.1109/HICSS.1999.772658

[21] HINTON, P.R. et.al.: *SPSS Explained*, Routledge, London and New York, 2004

[22] CHIN, W.W. MARCOLUN, B., NEWSTED, P.R.: *A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic mail Emotion/Adoption Study*, Information Systems Research. 14. (2003).

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

A HIBATŰRŐ KÉPESSÉG NÖVELÉSE KRITIKUS INFRASTRUKTÚRÁKBAN

INCREESING THE FAULT TOLERANCE OF CRITICAL INFRASTRUCTURES

ZENTAI Dániel

(ORCID: 0000-0002-3321-2013)

zentai.daniel@bgk.uni-obuda.hu

Absztrakt

A kritikus infrastruktúrák hálózatokat alkotnak, legyen szó akár vasúthálózatról, úthálózatról, elektromos hálózatról, vagy informatikai hálózatról. Ezen hálózatok matematikai elemzése gráfelméleti módszerek segítségével történhet. Kritikus infrastruktúrákkal szemben természetes elvárás lehet, hogy egy (vagy esetleg néhány) infrastruktúra elem meghibásodása esetén az infrastruktúra összefüggő maradjon, azaz lehetőség szerint ne jöjjenek létre egymástól elválasztott komponensek a hálózatban. Ezen hibatűrő képesség gráfelméleti megfelelője a többszörös összefüggőség, melynek kiszámítására ismertek hatékony algoritmusok. Fontos kérdés, hogy ha egy kritikus infrastruktúra nem teljesít bizonyos gráfelméleti megbízhatósággal kapcsolatos követelményeket, akkor hogyan lehet a lehető legkisebb költséggel kibővíteni az infrastruktúrát oly módon, hogy ezen követelményeknek eleget tegyen.

A cikk kutatásaihoz az Új Széchenyi Terv keretein belül az EFOP-3.6.2-16-2017-00016 számú projekt biztosított forrást. A kutatás az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósult meg.

Kulcsszavak: *kritikus infrastruktúrák, gráfelmélet*

Abstract

Critical infrastructures form networks, including railway networks, road networks, electronic networks, or computer networks. Mathematical analysis of these networks is often done with graph theory. We can set up a natural requirement regarding to critical infrastructures, namely, even if some failures occur in the infrastructure, and some component become unreachable for a while, the infrastructure itself has to remain connected, i.e. we have to avoid separated components in the infrastructure. This fault tolerance capability is called multiple connectivity in graph theory. Given a critical infrastructure, we can ask the following important question. If the infrastructure does not satisfy some robustness requirements, then what is the minimal cost of the completion of the infrastructure, such that it becomes robust enough to satisfy these requirements.

The research presented in this paper was carried out as part of the EFOP-3.6.2-16-2017-00016 project in the framework of the New Széchenyi Plan. The completion of this project is funded by the European Union and co-financed by the European Social Fund.

Keywords: *critical infrastructures, graph theory*

A kézirat benyújtásának dátuma (Date of the submission): 2018.06.03.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.24.

BEVEZETÉS

Kritikus infrastruktúrák [4,5,7] matematikai modellezésének természetes eszköze a gráfelmélet. Gráfnak nevezzük csomópontoknak élek által összekötött (általában véges) halmazát. Tekinthetünk gráfként egy úthálózatra, ahol a kereszteződések a csomópontok, és az ezeket összekötő útszakaszok az élek, vagy egy infokommunikációs hálózatra, ahol a csomópontok a kommunikáló eszközök, az élek pedig az ezeket összekötő kommunikációs csatorna. A gráfok megbízhatóságának, támadásokkal szembeni állóképességének egy lehetséges mérőszáma a többszörös összefüggőség. Ez a gráfparaméter mutatja meg, hogy hány élt, vagy csomópontot törölhetünk ki a gráfból oly módon, hogy a megmaradt élek és csomópontok továbbra is egy összefüggő gráfot alkossanak. A [6] cikkben gráfok többszörös összefüggőségét vizsgáltuk, itt arra térünk ki, hogy ha egy gráf, illetve a megfelelő kritikus infrastruktúra nem felel meg a követelményeinknek, hogyan lehet a lehető legkevesebb él hozzávételével javítani a megbízhatóságát, azaz növelni az összefüggőségi számát.

GRÁFELMÉLET

Ebben a fejezetben alapvető gráfelméleti fogalmakat ismertetünk, melyek szükségesek lesznek a továbbiak megértéséhez. A gráfelméleti háttér alaposabb megértéséhez javaslom a [2,3] könyveket.

Legyen $V = \{v_1, v_2, \ldots, v_n\}$ véges halmaz, és legyen E a V halmaz bizonyos kételemű részhalmazainak egy halmaza, azaz $E \subseteq \binom{V}{2}$. Az ebből a két halmazból álló $G = (V,E)$ rendezett párt véges egyszerű gráfnak nevezzük.

A $V = V(G)$ halmaz elemeit a G gráf csúcsainak, vagy pontjainak, az $E = E(G)$ halmaz elemeit pedig a G gráf éleinek nevezzük. A $G = (V,E)$ gráfban a $v, w \in V$ csúcsokat szomszédosnak nevezzük, ha őket él köti össze, azaz ha $\{v,w\} \in E$. A $G = (V,E)$ gráf irányított gráf abban az esetben, ha minden élének van egy iránya is, azaz megkülönböztetjük a $(v,w) \in E$ élt a $(w,v) \in E$ éltől. Ebben az esetben $E \subseteq \binom{V}{2}$ helyett $E \subseteq V \times V$. A gráfok szokásos geometriai reprezentációjában az éleket irányítatlan esetben szakaszokkal, vagy görbékkel, irányított esetben pedig nyilakkal ábrázoljuk.

A $G = (V,E)$ gráf $v \in V$ csúcsának fokszáma a v szomszédjainak számával egyenlő. A v csúcs fokszámát d(v) jelöli. Irányított gráf esetében megkülönböztetjük a v csúcs befokát és kifokát. A v csúcs befoka azon éleknek a száma, melyeknek végpontja v, a v csúcs kifoka pedig azon élek száma, melyeknek a kezdőpontja v.

A séta a gráfban csúcsok és élek váltakozó $v_0e_1v_1 \ldots e_kv_k$ sorozata, ahol mindegyik él a sorozatban őt megelőző és őt követő csúcsokat köti össze, azaz $e_i = \{v_{i-1},v_i\}$. A vonal olyan séta, amelyben egy él legfeljebb egyszer szerepelhet, az út pedig olyan vonal, amelyben minden csúcs is maximum egyszer szerepel. A séta, vonal vagy út hosszának az ezek során érintett élek számát nevezzük.

A $G = (V,E)$ gráfot összefüggőnek nevezzük, ha bármely $u \in V$ pontjából bármely $v \in V$ pontjába vezet u kezdőpontú és v végpontú út. Legyen $G = (V,E)$ nem feltétlenül összefüggő gráf. G ponthalmazának egy $C \subseteq V(G)$ részhalmazát akkor nevezzük összefüggőségi komponensnek, ha teljesül rá, hogy bármely $u \in C$ pontból bármely $v \in C$ pontba vezet út, de semelyik C-beli pontból nem vezet út a $V \setminus C$ halmaz semelyik pontjába sem. A G gráf összefüggőségi komponenseinek számát c(G) jelöli. Egy G gráf tehát pontosan akkor összefüggő, ha $c(G) = 1$.

Többszörös összefüggőség

Hálózatok, és így kritikus infrastruktúrák topologikus értelemben vett hibatűrésének egy természetes mérőszáma a hálózatot, vagy infrastruktúrát modellező gráf többszörös összefüggősége.

Definíció: Azt mondjuk, hogy a G = (V,E) gráf k-szorosan él-összefüggő, vagy röviden k-él-összefüggő, ha G-nek legalább k+1 pontja van (azaz $|V(G)| \geq k+1$), és bárhogyan hagyunk el G-ből legfeljebb k darab élt, a kapott G' gráf összefüggő marad. A legnagyobb olyan k értéket, ami a fenti feltételeket teljesíti, a gráf él-összefüggőségi számának nevezzük, és $\lambda(G)$-vel jelöljük.

Definíció: Azt mondjuk, hogy a G = (V,E) k-szorosan összefüggő, vagy röviden k-összefüggő, ha G-nek legalább k+1 pontja van (azaz $|V(G)| \geq k+1$), és bárhogyan hagyunk el G-ből legfeljebb k darab csúcsot, a kapott G' gráf összefüggő marad. A legnagyobb olyan k értéket, ami a fenti feltételeket teljesíti, a gráf összefüggőségi számának nevezzük, és $\kappa(G)$-vel jelöljük.

A fentiek közül a k-él-összefüggőség modellezi az összeköttetések, a k-összefüggőség pedig a csomópontok támadásával szemben támasztott megbízhatósági követelményt.

A TÖBBSZÖRÖS ÖSSZEFÜGGŐSÉG NÖVELÉSE

Algoritmikusan könnyedén kiszámolható egy gráf él-összefüggőségi, illetve összefüggőségi száma. Erre szolgálnak a folyamalgoritmusok [1]. Közvetlenül a definíció alapján nem tudnánk hatékonyan kiszámolni egy gráf összefüggőségi számát, így a folyamalgoritmusok sem ezt a módszert követik, hanem a definíció egy ekvivalens átfogalmazását használják. A következő két tétel Menger tételének közvetlen következményei. Menger tételeit az olvasó megtalálhatja [2]-ben.

Tétel: Az alábbiak ekvivalensek:

- A G = (V,E) gráf k-szorosan él-összefüggő.
- Tetszőleges $u,v \in V(G)$ esetén van k darab éldiszjunkt u-v út, azaz k darab olyan u-v út, melyekre teljesül, hogy semelyik kettőnek nincs közös éle.

Tétel: Az alábbiak ekvivalensek:

- A G = (V,E) gráf k-szorosan összefüggő.
- Tetszőleges $u,v \in V(G)$ esetén van k darab belsőleg pontdiszjunkt u-v út, azaz k darab olyan u-v út, melyekre teljesül, hogy semelyik kettőnek nincs közös pontja a kezdőponttól és a végponttól eltekintve.

Alább definiáljuk gráfok lokális él-összefüggőségét, illetve lokális összefüggőségét.

Definíció: Legyen G = (V,E) gráf, és $u,v \in V(G)$ tetszőleges csúcsok. Az u és v csúcsok közötti lokális él-összefüggőség az u és v közötti éldiszjunkt utak maximális száma, melyet $\lambda(u,v)$ jelöl.

Definíció: Legyen G = (V,E) gráf, és $u,v \in V(G)$ tetszőleges csúcsok. Az u és v csúcsok közötti lokális összefüggőség az u és v közötti belsőleg pontdiszjunkt utak maximális száma, melyet $\kappa(u,v)$ jelöl.

Könnyen ellenőrizhető, hogy egy gráf globális él-összefüggőségi száma a lokális él-összefüggőségi számok minimuma, formálisan $\lambda(G) = \min\{\lambda(u,v) \mid u,v \in V(G)\}$. Hasonlóan, egy gráf globális összefüggőségi száma megegyezik a lokális összefüggőségi számok minimumával, azaz $\kappa(G) = \min\{\kappa(u,v) \mid u,v \in V(G)\}$.

Az alábbiakban arra a kérdésre keressük a választ, hogy ha az általunk vizsgált infrastruktúra (pontosabban az azt modellező gráf) nem teljesíti az általunk támasztott összefüggőségi

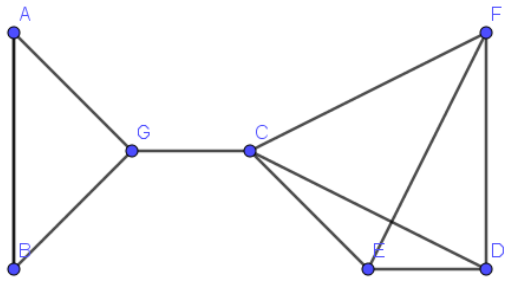
követelményeket, akkor hogyan tudjuk ezt új összeköttetések létesítésével kibővíteni úgy, hogy eleget tegyen ezen követelményeknek.

Él-összefüggőség

Teljes általánosságban a feladat a következő. Legyen $r : V \times V \rightarrow \mathbb{Z}+$ egy csúcspárokat pozitív egész számokra képező függvény, és tegyük fel, hogy $\lambda(u,v) < r(u,v)$ legalább egy csúcspárra. Célunk egy olyan G'=(V,E') gráfot konstruálni, melyre teljesül, hogy $\lambda(u,v) \geq r(u,v)$ minden G'-beli csúcspárra, és G'-t minimális összköltségű élek hozzáadásával kaptuk G-ből. A feladatra ebben az általános formában nem várhatunk hatékony algoritmust, ugyanis a probléma NP-teljes.

Jelen esetben mi azzal a speciális esettel fogunk foglalkozni, melyben minden hozzáadott él költsége azonos (azaz a hozzáadott élek darabszámát szeretnénk minimalizálni), illetve r(u,v) = 2 minden (u,v) csúcspárra. A továbbiakban tehát azt az esetet részletezzük, amikor a G=(V,E) gráfot minimális darabszámú él hozzáadásával szeretnénk kiegészíteni 2-él-összefüggővé. Erre a speciális esetre ismerünk hatékony algoritmust [1]. Kritikus infrastruktúrák esetében az, hogy csak a 2-él-összefüggőség esetét vizsgáljuk, egy észszerű megszorítást jelent, ugyanis csupán annyit feltételezünk, hogy a támadónak nem áll módjában az infrastruktúra egynél több összeköttetését támadni egyidejűleg.

Az algoritmus részletezése előtt szükségünk lesz a következő fogalmakra. A G gráf egy e éle elvágó él, ha a G''=(V,E \ {e}) gráf már nem összefüggő, azaz ha az e él törlésével a gráf több komponensre esik szét.



1. ábra Nem 2-él-összefüggő gráf

A fenti ábrán láthatunk egy példát olyan gráfra, amely nem 2-él-összefüggő, ugyanis {C,G} egy elvágó él. Könnyen látható azonban, hogy az {A,F} és hozzáadásával már 2-él-összefüggő gráfot kapunk. Blokkoknak hívjuk a G gráf elvágó élt nem tartalmazó maximális részgráfjait. Egy olyan blokkot, amire mindössze egy darab elvágó él illeszkedik, levélblokknak hívunk. Két blokk távolságán az őket összekötő legrövidebb utat értjük. Ezek után rátérhetünk a fent említett algoritmusra:

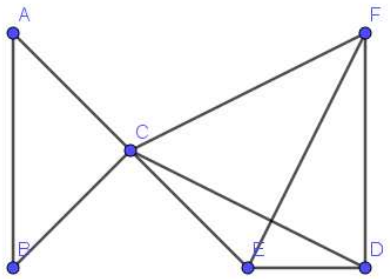
Algoritmus: Legyen kezdetben G'=G. Amíg a G'=(V,E') gráf nem 2-él-összefüggő, válasszunk 2 olyan levélblokkot, amelyek távolsága maximális. Adjunk hozzá G'-höz egy olyan f élt, ami ezen levelek egy-egy tetszőleges pontját köti össze, azaz legyen $G'=(V,E' \cup \{f\})$.

Látható, hogy minden egyes él hozzáadása 2-vel csökkenti a levélblokkok számát, azt az esetet kivéve, amikor összesen 3 levélblokk van. (Ez utóbbi esetben csak 1-gyel csökken a levélblokkok száma.) Ebből következik, hogy G kiegészítése 2-él-összefüggővé legkevesebb $\lceil L(G)/2 \rceil$ él hozzáadásával történhet, ahol L(G) jelöli G levélblokkjainak a számát.

Csúcs-összefüggőség

Az előbbiekhez hasonlóan az általános feladatban legyen $r : V \times V \rightarrow \mathbb{Z}+$ egy csúcspárokat pozitív egész számokra képező függvény, és tegyük fel, hogy $\kappa(u,v) < r(u,v)$ legalább egy

csúcspárra. Célunk egy olyan G'=(V,E') gráfot konstruálni, melyre teljesül, hogy $\kappa(u,v) \geq r(u,v)$ minden G'-beli csúcspárra, és G'-t minimális összköltségű élek hozzáadásával kaptuk G-ből. Az él-összefüggőségi esethez hasonlóan erre a feladatra sem várhatunk az általános esetben hatékony algoritmust, azonban most is elegendő lesz azzal a speciális esettel fogunk foglalkozni, melyben minden hozzáadott él költsége azonos, illetve $r(u,v) = 2$ minden (u,v) csúcspárra. Továbbra is élünk ugyanis azzal a feltevéssel, hogy a támadó egyidejűleg csak egy csomópontját támadja az infrastruktúrának. Most is szükségünk lesz az él-összefüggőségi esettel analóg fogalmakra. A G gráf egy v csúcsa elvágó csúcs, ha a G''=(V \ {v},E \ F) gráf már nem összefüggő, ahol F a v csúcsra illeszkedő élek halmaza, azaz ha a v csúcs törlésével a gráf több komponensre esik szét.



2. ábra

A fenti ábrán láthatunk egy példát olyan gráfra, amely nem 2-összefüggő, ugyanis C egy elvágó csúcs. Könnyen látható azonban, hogy az {A,F} és hozzáadásával már 2-összefüggő gráfot kapunk. Blokkoknak hívjuk a G gráf elvágó csúcsot nem tartalmazó maximális részgráfjait. Egy olyan blokkot, amire mindössze egy darab elvágó csúcs illeszkedik, most is levélblokknak hívunk. Két blokk távolságán az őket összekötő legrövidebb utat értjük. Legyen továbbá $b(G) = \max\{c(G - v) : v \in V\}$, ahol G – v jelöli a G''=(V \ {v},E \ F) gráfot. Tehát b(G) az a maximális érték, ahány komponens keletkezik a legtöbb komponenst létrehozó v csúcs törlésével. Ezek után az algoritmus a következő:

Algoritmus: Legyen kezdetben G'=G. Amíg a G'=(V,E') gráf nem 2-összefüggő, válasszunk 2 olyan levélblokkot, amelyek távolsága maximális. Adjunk hozzá G'-höz egy olyan f élt, ami ezen levelek egy-egy tetszőleges pontját köti össze, azaz legyen G'=(V,E'∪{f}).

Az algoritmus tehát megegyezik az él-összefüggőségi esetben említett algoritmussal, a hozzáadandó élek száma azonban változni fog ebben az esetben. Belátható ugyanis, hogy G kiegészítése 2-összefüggővé legkevesebb $\max\{\lceil L(G)/2 \rceil, b(G)-1\}$ él hozzáadásával történhet, ahol L(G) jelöli G levélblokkjainak a számát.

FELHASZNÁLT IRODALOM

[1] JORDÁN T., RECSKI A., SZESZLÉR D.: Rendszeroptimalizálás, Typotex kiadó, Budapest, 2004

[2] KATONA Y. Gy, RECSKI A., SZABÓ Cs.: A számítástudomány alapjai, Typotex kiadó, Budapest, 2002

[3] LOVÁSZ L., PELIKÁN J., VESZTERGOMBI K.: Diszkrét matematika. Typotex kiadó, Budapest, 2010

[4] Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 12. számú ajánlása – BODALKI Á., CSERNAY A., MÁTYÁS P., MUHA l., PAPP Gy., VADÁSZ D.: Informatikai Rendszerek Biztonsági Követelményei – Budapest, 1996.

[5] BABOS T.: The First Critical Infrastructure Protection Research Project in Hungary, Springer Publishing Company, 2016, 1-22. old.

[6] ZENTAI D.: Gráfelméleti módszerek a kritikus infrastruktúra védelemben, Hadmérnök, XII. Évfolyam 2. pp. 341-347.

[7] http://uni-nke.hu/downloads/konyvtar/kovasz/kritikus_infrastrukturak.pdf (letöltve: 2017.11.20.)

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

VEZETÉSI MÓDSZEREK GYAKORLATI ALKALMAZÁSA A TÖMEGES VIHARKÁROK FELSZÁMOLÁSA SORÁN

MANAGEMENT METHODS IN PRACTICE BY ELIMINATION OF STORM DAMAGES

GYŐZŐ-MOLNÁR Árpád

(ORCID ID 0000-0003-2046-8658)

arpad.gyozo@katved.gov.hu

Absztrakt

A XXI. század jelentős károkat okozó természeti katasztrófa típusa a rendkívüli időjárás, amely tömeges viharkárral jár. A viharkárok közös jellemzője, hogy a kiváltó ok előrejelzése és következmények megelőzése még napjaink technikai fejlettségével is komoly nehézségekbe ütközik, továbbá a bekövetkezés nagy károkat okoz a közlekedési és áramhálózati infrastruktúrában, illetve a civil szektorban egyaránt.
Mindezekből kiindulva célszerű megvizsgálni a bekövetkezést követő kárfelszámolás során alkalmazott irányítási és vezetési módszereket, továbbá ezek hatékonyságát. A megfelelő vezetési módszer alkalmazásával a károk felszámolása sokkal eredményesebb, jelentősen lecsökken a beavatkozások időtartama, illetve a másodlagos károk kialakulásának esélye, ugyanakkor növelhető a lakosság biztonságérzete.

Kulcsszavak: *viharkár, vezetési módszer, kárfelszámolás*

Abstract

Extraordinary storms are those type of natural disasters which causing massive considerable damages in the 21st Century. Common features of these injuries are multiple, because the prediction of causes (storms) and the prevention of consequences face serious difficulties despite the technical development of today's. Nevertheless, this kind of incidents cause major damage to both transport and electricity infrastructure, even in the civil sector as well.
Based on these considerations, it is practical to examine the management and leadership methods and their effectiveness related to the damage elimination. Applying the proper management method, the elimination of damages can be much more effective, the duration of operations and the likelihood of secondary damage may significantly reduce, and the sense of security felt by the population can be increased at the same time.

Keywords: *storm damage, management method, elimination of damages*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.28.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.20.

BEVEZETÉS

Kutatásom legfőbb célja, hogy a katasztrófavédelmi rendszer 2012-ben végrehajtott transzformációját követően Magyarországon bekövetkezett természeti katasztrófák során alkalmazott vezetési és irányítási módszereket, továbbá azok hatékonyságát vizsgáljam, majd a kutatás eredményét figyelembe véve a katasztrófavédelmi törvényhez és az ehhez kapcsolódó ágazati szabályzói rendszerhez módosító javaslatokat dolgozzak ki. [1] A módosítások szükségességét indokolja, egy olyan szabályzói rendszer létrejöttének igénye, amely konkretizálja elsősorban a veszélyhelyzet[1] kihirdetésének szintjét el nem érő természeti katasztrófák során a kárfelszámolás vezetési-irányítási és a kapcsolódó jelentési, valamint adatszolgáltatási rendjét, illetve egyértelműsíti, megnevezi azt a szervezetet, amely a kárfelszámolás irányításában prioritást élvez. [2] Részcélként fogalmazom meg egy eljárásrend kidolgozását és a belső szabályzórendszer ezirányú módosítását elsődlegesen a hivatásos katasztrófavédelmi szervezet és az általa felügyelt önkéntes beavatkozó szervezetek számára, mely kapcsolódik a módosított jogszabályokhoz. További célom, hogy a megújított szabályzók figyelembevételével a rendvédelmi (katasztrófavédelmi) felsőoktatásban tananyag, jegyzet kerüljön kidolgozásra.

Jelen cikk a tervezett kutatásnak egy kis részét fedi le, azonban a témaválasztás aktualitását jól jelzi, hogy az elmúlt 5 éves időszakot vizsgálva jelentősen megnövekedett a nehezen prognosztizálható rendkívüli időjárási jelenségekből – elsősorban a tömeges viharkárokból – fakadó káresemények száma, melyek jelentős károkat okoznak a gazdasági élet, a közigazgatás és a lakosságnak, továbbá jellegükből fakadóan komoly igénybevételnek teszik ki mind a beavatkozásokat irányító, mind a beavatkozó állományt. [3] A tömeges viharkárok előrejelzésének eredményessége még napjainkban is csak meglehetősen korlátozott, [4] a megfelelő megelőzés lehetőségének hiányában a kárfelszámolás irányítási és vezetési rendszerében tapasztalható hiányosságok javítása lehet az egyik tényező, amellyel hatékonyabban állíthatók helyre a keletkezett károk, illetve meggátolható a másodlagos káresemények kialakulása.

Fő célom a jelen írással, hogy a tömeges viharkárok felszámolása során a katasztrófavédelem szervezetrendszerén belül alkalmazott vezetési módszer elemzése, továbbá a jellemző irányítási módszer, valamint az alkalmazott döntéstámogatási eszközök és tevékenységek bemutatása. Ennek érdekében egy megtörtént tömeges káreseményen keresztül vizsgálom, azokat a vezetési és irányítási módszereket, amelyeket a katasztrófavédelem hivatásos állománya ilyen jellegű káresetek felszámolása során alkalmaz.

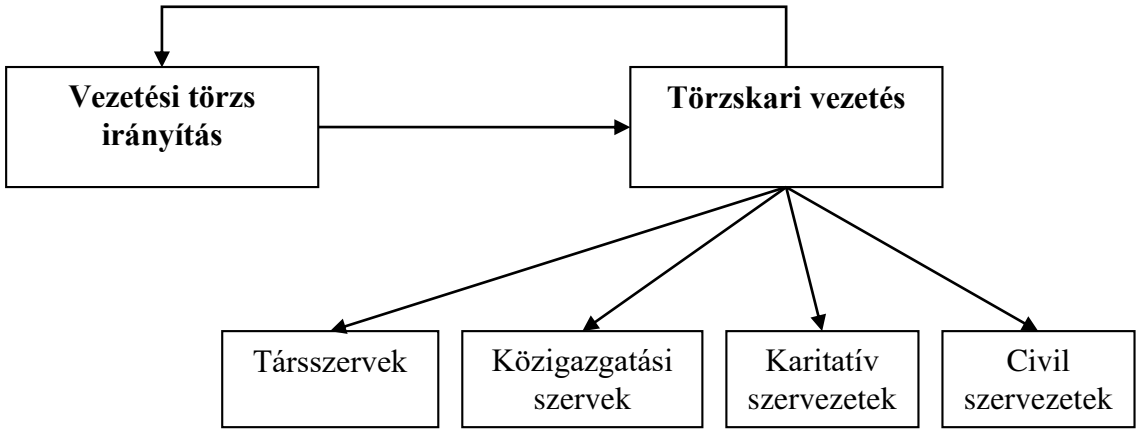
A tömeges viharkárok következményeinek tűzoltói felszámolásának belső szabályzórendszere kiforrott, a kárfelszámolásban a hivatásos katasztrófavédelmi szervezet nagy tapasztalatokkal rendelkezik a vezetési-irányítási módszerek alkalmazását tekintve és a kialakult gyakorlat biztosítja az eredményes beavatkozások biztosítását.

A cikk elején le kell szögezni, hogy a vizsgálatban szereplő vezetési-irányítási módok, önmagukban egy kárfelszámolás során nehezen értelmezhetők, ezért legtöbb esetben ezek kevert módon, sok esetben egymással párhuzamosan – a káresemény jellegének megfelelően – kerülnek alkalmazásra.

[1] A Kormány az élet- és vagyonbiztonságot veszélyeztető elemi csapás vagy ipari szerencsétlenség esetén, valamint ezek következményeinek az elhárítása érdekében veszélyhelyzetet hirdet ki, és sarkalatos törvényben meghatározott rendkívüli intézkedéseket vezethet be. A vezetés vonatkozásában ilyen rendkívüli intézkedés lehet kormánybiztos kinevezése, vagy a településen a helyi katasztrófavédelmi tevékenység irányítását - helyszínre érkezésétől - a polgármestertől átvevő a hivatásos katasztrófavédelmi szerv területi szerve vezetője által kijelölt személy.

AZ ALKALMAZOTT VEZETÉSI ÉS IRÁNYÍTÁSI MÓDSZEREK

A vezetési módszerek vizsgálata során meg kell különböztetnünk, illetve el kell határolnunk a katasztrófavédelem beavatkozó egységei által közvetlenül az egyes kárhelyszíneken alkalmazott irányítási módokat,[2] valamint azokat a vezetési módszereket, melyek átfogóan értelmezik a kiterjedt kárhelyszíneken történő tömeges káresetek felszámolását és amely a katasztrófavédelmi szervezet gyakorlatában kizárólag törzskari vezetéssel valósítható meg. [5] Törzskari vezetés alkalmazása szükséges *„azon káresemények esetén, amelyek elhárítása a katasztrófavédelem rendelkezésre álló hivatásos erőivel nem hajtható végre és az esemény Magyarország lakosságának személyi és anyagi biztonságát jelentős mértékben érinti, továbbá nagysága, időbeli lefolyása, bonyolultsága, a helyszín tagoltsága, a beavatkozó erők létszáma vagy egyéb körülmények a végrehajtandó feladatok szélesebb körű megosztását, speciális képességek igénybevételét, illetve jelentős számú civil szervezetek bevonását teszik szükségessé, valamint katasztrófaveszély nem áll fenn és veszélyhelyzet nem került kihirdetésre”*. [5: 1. mell. 10]



1. ábra. *A törzskari vezetés elvi megvalósulása a katasztrófavédelmi alkalmazásban.* [5: 1. mell. 11]

A vizsgált természeti katasztrófa típusnál a tömeges jellegből és a kiterjedésből fakadóan, valamint mivel a kárfelszámoláshoz a hivatásos katasztrófavédelmi erőkön kívül más szervezetek beavatkozása is szükséges, kizárólag törzskari vezetéssel valósítható meg az eredményes vezetés, melynek érdekében helyszíni operatív törzs kerül felállításra.

Jelen tanulmánynak – terjedelmi okokból – nem célja, hogy elemezze a közvetlen kárhelyszíneken alkalmazott irányítási módokat és azok eredményességét, ezért pusztán az alapirányítás[3] bemutatására szorítkozik, mellyel a viharkárok okozta káresemények felszámolásra kerültek.

A kiterjedt viharkárok felszámolásának nemzetközi tapasztalatai és a kialakult gyakorlat, az irányítási rendszerek, az eltérő szervezeti struktúra és az alkalmazott informatikai és kommunikációs eszközök miatt az itthoni alkalmazástól némileg eltérnek, azonban jellemző módon törzskari vezetéssel valósulnak meg. [6]

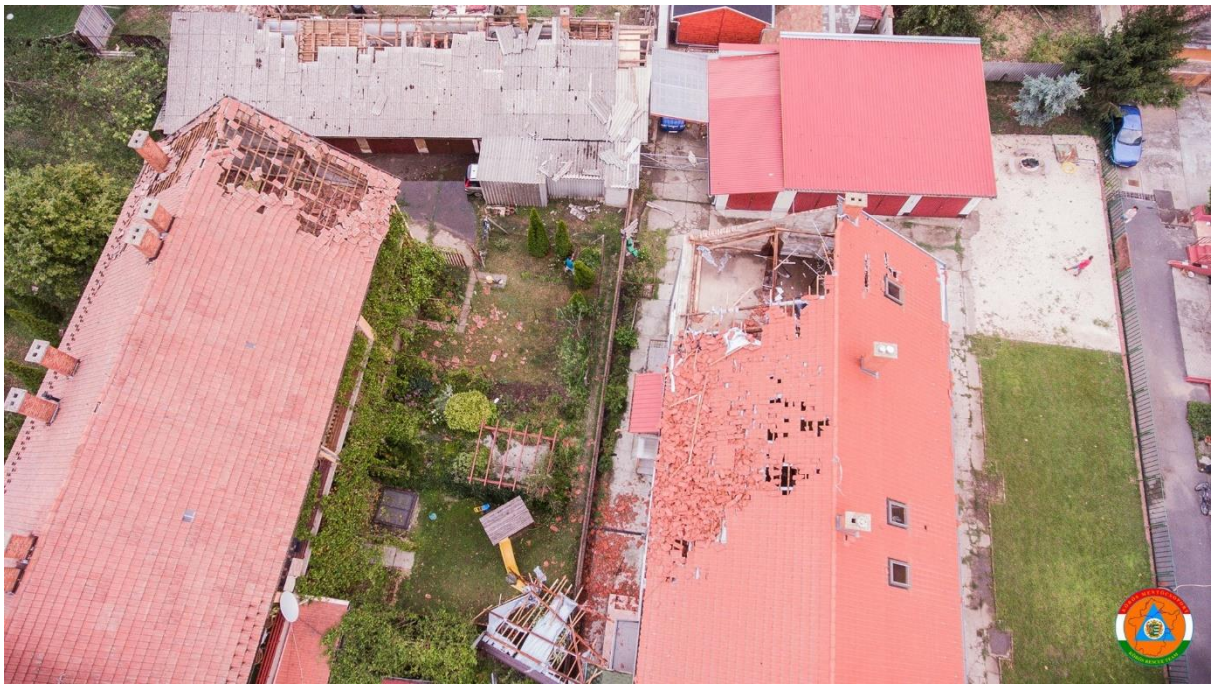
[2] A tűzoltásban és műszaki mentésben résztvevők közvetlen vezetésére, irányítására alkalmazott módok, melyek az események bonyolultságát, kiterjedését figyelembe véve lehetnek: alapirányítás, csoportirányítás és vezetési törzsirányítás.

[3] Alapirányítás: amennyiben a beavatkozó tűzoltó erőket a kárhelyparancsnok egyedül irányítja.

A törzskari vezetés megvalósulása, a helyszíni operatív törzs működése

A törzskari vezetés a gyakorlatban történő megvalósulását, illetve a helyszíni operatív törzs alkalmazásának lépéseit egy megtörtént káresemény feldolgozásán keresztül célszerű leginkább szemléltetni. Az esemény kiválasztása során a szerző törekedett, hogy egy tipikusnak ítélhető, azaz jelentős széllel, valamint jégesővel együtt járó esemény kerüljön elemzésre, ezzel is bemutatandó azokat a nehézségeket, amelyek a vezetés valamennyi szintjén jelentkeznek a tömeges viharkárok felszámolása során. [3]

2017. augusztus 06-án a késő délutáni órákban, a Békés megyében található Orosháza város közigazgatási területét orkán erejű széllökésekkel[4] és jégesővel járó vihar érte el, mely jelentős épület- és infrastrukturális károkkal járt. Közvetlenül a vihar bekövetkezése után 45 lakossági bejelentés érkezett, melyek száma a lakosság és a hatóságok észlelései miatt folyamatosan nőtt.[5] A bejelentések nagy többsége súlyosan megrongálódott lakóingatlanokról (elsődlegesen a tetőszerkezet vonatkozásában), a belterületi közutakat, valamint a 47-es számú főközlekedési útvonalat és a Szeged-Békéscsaba közötti 135-ös jelzésű vasútvonalat elzáró fakidőlésekről tett említést. Mindezek mellett a város belterületén a villamoshálózat nagyarányú rongálódásából fakadóan, négyszáz fogyasztási helyen okozott áramkimaradást. Kiemelten jelentős károkat szenvedett el az Orosházi Kórház, ahol a viharkárokra tekintettel ideiglenesen szünetelt a betegellátás, illetve a sürgősségi esetek átirányításra kerültek a környező településeik egészségügyi intézményeibe.



***2. ábra**. A jellemző viharkárok.*
(Fotó: Melega Krisztián Körös Mentőcsoport, 2017. augusztus 06.)

A jelzések mennyiségéből és tartalmából arra lehetett következtetni, hogy az Orosházi Hivatásos Tűzoltóparancsnokságon (továbbiakban: Orosházi HTP) rendelkezésre álló tűzoltó

[4] A Beaufort-skála értelmében orkánról beszélünk, ha a szél sebessége legalább 118 km/h.
[5] A Katasztrófavédelmi Adatszolgáltatási Program nyilvántartása alapján 282 db káresemény került felszámolásra a katasztrófavédelem erői által az orosházi viharkár következtében. A fenti adat nem tartalmazza a lakosság és a társszervek önálló, a katasztrófavédelem egységei nélkül végrehajtott beavatkozásait. (A szerző saját gyűjtése. Letöltve: 2017. 11. 10.)

erők[6] a kárfelszámolás elvégzésére nem lesznek elegendők, ezért a Békés Megyei Katasztrófavédelmi Igazgatóság (továbbiakban: Békés MKI) Megyei Műveletirányítási Ügyelete intézkedett a Békés- és Csongrád megyében működő hivatásos tűzoltóparancsnokságok helyszínre irányítására, az Orosháza településre vonatkozó műveleti terv alapján. [7]

A hivatásos erők átcsoportosításán kívül az elérhető és beavatkozási jogosultsággal, minősítéssel rendelkező önkéntes szervezetek, elsősorban három önkéntes tűzoltó egyesület (továbbiakban: ÖTE), az illetékes járási mentőcsoport, továbbá a megyei mentőcsoport riasztására és alkalmazására is sor került. [8] [9]

Ssz.	Megnevezés (EDR hívónév)	Létszám (fő)	Eszköz	Megjegyzés
1.	Orosháza/1	5	gépjárműfecskendő	beavatkozó
2.	Orosháza/2	4	gépjárműfecskendő	beavatkozó
3.	Szarvas/1	5	gépjárműfecskendő	beavatkozó
4.	Vásár/1	5	gépjárműfecskendő	beavatkozó
5.	Csaba/1	5	gépjárműfecskendő	beavatkozó
6.	Gyula/2	4	gépjárműfecskendő	beavatkozó
7.	Kovács/2	4	gépjárműfecskendő	beavatkozó
8.	Csaba/Létra	2	magasból mentő	beavatkozó
9.	Szentes/Létra	2	magasból mentő	beavatkozó
10.	Orosháza/Pálya	2	gyorsbeavatkozó	beavatkozó
11.	Békés/KMSZ	1	KMSZ jármű	beavatkozó
12.	Békés/KSE	2	KSE jármű	az egység az operatív törzs tevékenységét támogatta
13.	Helyszíni operatív törzs	10	3 ügyintéző gépjármű 1 tűzoltásvezető gépjármű	
	HIVATÁSOS ÖSSZESEN	**51**	**17**	
1.	Körös Mentőcsoport	2	drón	beavatkozó
2.	Dél-Békés Mentőcsoport	6	csapatszállító	beavatkozó
3.	Battonya ÖTE	5	gépjárműfecskendő	beavatkozó
4.	Nagyszénás ÖTE	3	magasból mentő	beavatkozó
5.	Tótkomlós ÖTE	5	gyorsbeavatkozó	beavatkozó
	ÖNKÉNTES ÖSSZESEN	**21**	**5**	
	MINDÖSSZESEN	**72**	**22**	

***1. táblázat**. Kimutatás a 2017. augusztus 6-án beavatkozó erőkről.*
(Összeállította: Győző-Molnár Árpád tűzoltó alezredes)

Fentiekre tekintettel, a káresemények kezelésére – figyelembe véve a nagyszámú beavatkozó állományt, az esemény kiterjedését, az esetszámokat, továbbá a közlekedési- és áramhálózat jelentős rongálódását – a Békés MKI igazgatója a törzskari irányítás megvalósítása érdekében, helyszíni operatív törzset hozott létre. [10] Az operatív törzs a megfelelő elhelyezési, áramellátási és informatikai lehetőségek biztosítása érdekében az Orosházi Katasztrófavédelmi Kirendeltség (továbbiakban: KvK) épületében látta el feladatait, melyet az áram- és internetszolgáltatás kimaradása nem érintett. A megalakított helyszíni operatív törzsbe a Békés MKI állományából (megyei igazgatóhelyettes, megyei polgári védelmi főfelügyelő, megyei iparbiztonsági főfelügyelő, informatikai osztályvezető, sajtószóvivő, Katasztrófavédelmi

[6] A káresemény bekövetkezésekor: két gépjárműfecskendő, egy vízszállító jármű, valamint egy gyorsbeavatkozó jármű és 13 fő készenléti szolgálatot ellátó tűzoltó.

Sugárfelderítő Egység állománya), valamint az illetékes helyi szervek – az Orosházi KvK és HTP vezetői állománya (kirendeltség-vezető, tűzoltósági felügyelő, polgári védelmi felügyelő, hatósági osztályvezető és tűzoltóparancsnok) – került bevonásra.

A létrehozott törzsben a társszervek vonatkozásában az önkormányzat szervezeteit a városüzemeltetés és a mezőőrség képviselték. A rendőrség, valamint az áramszolgáltató a megalakított törzsbe nem delegált összekötőt, mely az egységes szabályzórendszer hiányára vezethető vissza. Így ezen szervezetek a saját ágazati és belső szabályzóiknak megfelelően végezték a tevékenységüket. Az összekötők távolmaradása, több esetben jelentősen hátráltatta a beavatkozások eredményességét, illetve megnövelte a beavatkozások idejét, mivel lassította a szervezetek közötti közvetlen információáramlást, amely így a megyei, illetve az áramszolgáltató vonatkozásában, a területi ügyeleti szolgálatokon keresztül valósult meg.

Az operatív törzset a Békés MKI megyei igazgatóhelyettes vezette, helyetteseként az Orosházi KvK kirendeltség-vezetője került kijelölésre. A társszervekkel a kapcsolatot a megyei ügyeletek vonatkozásában, a megyei polgári védelmi- és az iparbiztonsági főfelügyelők tartották. A törzs EDR-en[7] történő rádióforgalmazásáért és a műveleti napló[8] vezetéséért – 2 fő beosztott tiszttel – a megyei informatikai osztály vezetője felelt. A sajtószóvivő folyamatosan kapcsolatot tartott a helyi és megyei média képviselőivel, mely lehetővé tette a folyamatos és hiteles tájékoztatást. Az operatív törzs a fentiekben nem nevesített állománya, a jelentkező egyéb feladatok végrehajtásában, illetve a felderítő csoportok munkájában működött közre.

A helyszíni operatív törzs működésével kapcsolatban be kell mutatni, a közvetlen alárendeltségében működő, négy, alkalmi jelleggel felállított felderítő csoportot, amelyek állománya vegyesen állt a katasztrófavédelem és a társszervek állományából. A felderítő csoportok a Békés MKI Megyei Műveletirányítási Ügyelet által átadott és folyamatosan frissített káresemények listája alapján végezték a tevékenységüket. A káresemények listája alapján a csoportok még a kiérkező beavatkozó állomány előtt osztályozták az események súlyosságát, melyek alapján három kategóriát határoztak meg. Az elsőbe azok az események tartoztak, melyek közvetlen élet- vagy balesetveszélyt jelentettek, illetve veszélyeztették a közúti vagy vasúti közlekedést, illetve az áramhálózatot. A második osztályba kerültek besorolásra azok a káresemények, ahol az azonnali tűzoltói vagy egyéb társszervek általi beavatkozás nem volt indokolt, de a kapacitások rendelkezésre állása után szükséges a beavatkozás, mint pl. a tetőszerkezetek nem kritikus rongálódása. A harmadik kategóriát képezték azok a káresemények, amelyeknél a haladéktalan tűzoltói beavatkozás nem volt indokolt, nem veszélyeztetett közvetlenül sem közlekedési útvonalat, sem épületet, pl. olyan járdára dőlt fák esetében, ahol a gyalogosközlekedés biztosított volt. [7] A felderítő csoportok a tapasztaltakról közvetlenül jelentettek az operatív törzsnek, amely állománya egyeztetve a Békés MKI Megyei Műveletirányítási Ügyeletével intézkedett a megfelelő saját- vagy a társszervek erőinek a helyszínre irányítására. A felderítő csoportok ezáltal nagyban segítették az operatív törzs működését abban, hogy pontos információkkal rendelkezzenek a károk mértékéről, továbbá a helyszínen folyó munkálatokról. A káresetek hozzávetőleg 23%-a során volt szükség az azonnali beavatkozásra, 51% tartozott a második osztályozási kategóriába, továbbá 26% volt azon káresemények aránya,[9] ahol a tűzoltói beavatkozás nem volt haladéktalanul indokolt és amelyek során a felszámolást jellemzően a városüzemeltetés

[7] Egységes Digitális Rádiórendszer.

[8] A törzskar tevékenységéről műveleti naplót kell vezetni, melyben napi szinten rögzíteni kell a törzskarba beosztottak adatait (név, képviselt szervezet, beosztás), káresemény felszámolásában résztvevők létszámát, szervezeti hovatartozását, a bevetett technikai eszközök, anyagok megnevezését, mennyiségét, a káresemény felszámolása érdekében végrehajtott tevékenység rövid leírását, a meghozott döntéseket, valamint a kárfelszámolás szempontjából lényeges egyéb információkat.

[9] A Katasztrófavédelmi Adatszolgáltatási Program nyilvántartása alapján végzett kimutatás. (A szerző saját gyűjtése. Letöltve: 2017. 11. 10.)

szakemberei hajtották végre. A felderítő csoportok alkalmazása hatékonyan segítette a helyszíni operatív törzs munkáját, továbbá a megfelelő beavatkozási rend kialakítását.

Az EDR működése az esemény során folyamatosan biztosította az összeköttetést a beavatkozó erők, az operatív törzs és Békés MKI Megyei Műveletirányítási Ügyelete között.

Az operatív törzs és a beavatkozó állomány munkáját egyaránt segítette a Békés megyében működő Körös Mentőcsoport drónos komponense, amely valósidejű légi felderítési adatokkal, elsősorban képekkel és videókkal támogatta a tevékenységet, egészen a sötétedésig.

A helyszíni operatív törzs fentiekben bemutatott működését 2017. augusztus 7-én 5 óráig folytatta, a továbbiakban csökkentett létszámmal – csak koordináló szerepkörben – egészen 2017. augusztus 10-én 12 óráig folytatta a tevékenységét.

A kárhelyszíneken közvetlenül alkalmazott jellemző irányítási módszer

A viharkárok felszámolásának közös jellemzője, hogy változó számú „kisebb" káreseményből tevődnek össze, melyek felszámolásához a tűzoltói erők vonatkozásában elegendő egy félraj[10] illetve raj alkalmazása.[11]

Az alkalmazott erők és eszközök mennyiségéből is érzékelhető, hogy egy viharkárral összefüggő káresemény felszámolásának irányítását a félrajt, vagy rajt irányító kárhelyparancsnok egyedül, önállóan is hatékonyan el tudja látni, ezért elegendő az alapirányítás alkalmazása. Az alapirányítás alkalmazása nem zárja ki a helyszínen jelen lévő más szerv képviselőjével történő konzultáció lehetőségét, illetve más szerv állományának vagy eszközének használatát. Különösen igaz ez abban az esetben, ha a beavatkozást végrehajtó egység olyan bonyolult és a beavatkozók biztonságát veszélyeztető eseménynél avatkozik be, mint amilyenek az áramhálózat elemeinek rongálódása.

Az alapirányítás megköveteli az alkalmazójától a nagyfokú önállóságot, a kárhelyszín felderítésének önálló elvégzését, a megfelelő beavatkozási mód megválasztását, illetve a lehetőség szerinti gyors döntések meghozatalát.

[10] Félraj: a tűzoltás és műszaki mentés szervezetének olyan taktikai része, amely a rendelkezésre álló eszközeivel önálló beavatkozásra képes, létszáma 1+3 fő;

[11] Raj: a tűzoltás és műszaki mentés szervezetének taktikai része, amely a rendelkezésre álló eszközeivel önálló beavatkozásra képes, létszáma 1+5 fő.

***3. ábra**. A 47-es főutat teljes szélességében elzáró fakidőlések felszámolása alapirányítás alkalmazásával, továbbá a légi felderítés jelentősége.*
(Fotó: Melega Krisztián Körös Mentőcsoport, 2017. augusztus 06.)

KÖVETKEZTETÉSEK

A cikkben bemutatott törzskari vezetési módszer, azaz a helyszíni operatív törzs alkalmazása, valamint a kárhelyszíneken az alapirányítás alkalmazása alapvetően hatékonyan segítik elő a tömeges káresemények kezelését és felszámolását. Az operatív törzs alkalmazása a kárfelszámolás során jól kezelhetővé teszi a beérkező információk feldolgozását, továbbá eredményesen támogatja a vezetői döntések meghozatalát. A katasztrófavédelem hivatásos, továbbá a szakmai felügyelet alatt működő önkéntes erői a meglévő szabályzórendszerre támaszkodva eredményesen avatkozhatnak be. Lényeges szempont egy helyszíni operatív törzs alkalmazása során, hogy mindenképpen kerüljön bevonásra a helyismerettel rendelkező állomány, amely a bemutatott káresemény során megvalósult.

Külön érdemes kiemelni a felderítő csoportok és a drónos légi felderítés alkalmazását és jó színvonalú működését. A drónos felderítés nagy szerepet játszott a károk azonosításában, valamint lehetővé tette a törzs állományának a kárhelyszínek beazonosítását, hátránya, hogy csak jó látási viszonyok között volt alkalmazható, ezért az esti órákban szerepét átvették a felderítő csoportok.

Hiányosságként a bemutatott törzs működése során is jelentkezett azonban az a tapasztalat, hogy a megfelelő jogszabályi háttér hiányában, egyes beavatkozó szervezetek nem vettek részt a megalakított helyszíni operatív törzs tevékenységében. Ennek következtében a beavatkozást végrehajtó szervezetek között az információátadás időben elhúzódott, ezáltal több esetben hátráltatva az eredményes kárfelszámolást, mivel szétaprózta azokat a beavatkozó erőket, amelyek egymás mellett, közös vezetéssel történő alkalmazása meggyorsíthatta volna a kárfelszámolás menetét.

Az eddig lefolytatott vizsgálat eredményei alapján, a későbbiekben elemzem a társszervek rendelkezésre álló belső szabályzóiban foglaltakat, illetve a hasonló események során a katasztrófavédelem vezetési tevékenységben résztvevőinek tapasztalatait.

FELHASZNÁLT IRODALOM

[1] ENDRŐDI I.: *A katasztrófavédelem feladat- és szervezetrendszere - egyetemi szakanyag* Budapest: Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, 2013. http://real.mtak.hu/17528/1/A%20katasztr%C3%B3fav%C3%A9delem%20feladat-%C3%A9s%20szervezetrendszere%20PDF.pdf (A letöltés dátuma: 2017. 11. 15.)

[2] 2011. évi CXXVIII. törvény *a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról.*

[3] *Trends in extreme weather events in Europe: implications for national and European Union adaptation strategies.* Halle: Deutsche Akademie der Naturforscher Leopoldina, 2013. www.easac.eu/fileadmin/PDF_s/reports_statements/Easac_Report_Extreme_Weather_Events.pdfhttp://www.easac.eu/fileadmin/PDF_s/reports_statements/Easac_Report_Extreme_Weather_Events.pdf (A letöltés dátuma: 2017. 11. 19.)

[4] ANTAL R.: Az utóbbi idők szélsőséges időjárásának következményei, avagy a katasztrófavédelem feladatainak elemzése az új kihívások tükrében Magyarországon. *Pécsi Határőr Tudományos Közlemények,* XIV (2013), 223–230.

[5] *6/2016. (VI. 24.) BM OKF utasítás a Tűzoltás-taktikai Szabályzat és a Műszaki Mentési Szabályzat kiadásáról.*

[6] KOLINSKA, M.: Potentials, abilities, structures in Hungarian and Polish management systems in the cases of natural disasters – a comparison. *AARMS,* 11 1 (2012) 107–119. http://www.zmne.hu/aarms/docs/Volume11/Issue1/pdf/09.pdf (A letöltés dátuma: 2017. 11. 20.)

[7] *16/2016. (IV. 29.) BM OKF intézkedés a hivatásos katasztrófavédelmi szervek műveletirányításának rendjéről és a riasztás szakmai szabályairó.l*

[8] *13/2013. (X. 14.) BM OKF utasítás a Nemzeti Minősítő Rendszer alapkövetelményeiről*

[9] *2/2014. (I. 17.) BM OKF utasítás az önkéntes tűzoltó egyesület önálló beavatkozásának feltételeiről és a beavatkozó önkéntes tűzoltó egyesület (önkéntes tűzoltóság) tevékenységéről*

[10] *9/2016. (III. 16.) Békés MKI intézkedés a hivatásos katasztrófavédelmi szervek működési rendjének szabályozására katasztrófaveszély, veszélyhelyzet, helyreállítás és újjáépítés idején, valamint katasztrófavédelmi operatív munkaszervek létrehozásáról, működési feltételek biztosításáról, szervezeti felépítéséről, valamint feladatairól*

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

EXAMINATION OF THE NEED FOR A DIRECTIVE TO STRENGTHEN THE CONTROL OVER POSSESSION OF FIREARMS ENVISAGED BY THE EUROPEAN COMMISSION IN THE CONTEXT OF NEW TYPES OF SECURITY CHALLENGES AFFECTING THE EUROPEAN UNION

AZ EURÓPAI BIZOTTSÁG ÁLTAL ELŐIRÁNYZOTT SZIGORÚBB LŐFEGYVERTARTÁSRÓL SZÓLÓ IRÁNYELV SZÜKSÉGESSÉGÉNEK VIZSGÁLATA AZ EURÓPAI UNIÓT ÉRINTŐ ÚJ TÍPUSÚ BIZTONSÁGI KIHÍVÁSOK SZEMPONTJÁBÓL

SZABÓ Csaba

(ORCID: 0000-0001-9573-2332)

szabo.csaba@uni-nke.hu

Abstract

The research described in this paper, through reviewing issues of the weapons policy domain of the European Union, analyses the questions formulated by the European Council in relation to such new security challenges as the suppression of illegal acquisition of firearms, the increasing of security risks relating to the transport, import and export of civilian firearms in the European Union, the improvement of traceability of legally held firearms (hunting, sports, self-defense) and ensuring that deactivated firearms are rendered inoperable. Giving the professional analysis of the background of the directive on stricter firearms possession foreseen by the European Commission in 2015, the study seeks to high-light the need for EU action to tackle the new security challenges in the weapons possession policy.
The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in the Győző Concha Doctoral Program

Keywords: *weapons policy, security policy, Weapons Act, new security challenges, police.*

Absztrakt

Jelen tanulmányban szereplő kutatás az Európai Unió fegyverrendészeti szakterületének problémáit elemezve vizsgál olyan az Európai Tanács által megfogalmazott új típusú biztonsági kihívásokra vonatkozó kérdéseket, mint az illegális lőfegyverek beszerzésének a korlátozása, a polgári célú tűzfegyverek szállítására, importjára és exportjára vonatkozó biztonsági kockázatok erősödése az Európai Unió területén, a jogszerűen (vadászat, sport, önvédelem) tartott lőfegyverek nyomon követésének a szigorítása, valamint a hatástalanított lőfegyverek működésképtelenségének a biztosításával kapcsolatos kihívások. A tanulmány az Európai Bizottság által 2015-ben előirányzott szigorúbb lőfegyvertartásról szóló irányelv hátterének a szakmai elemzésével kívánja megvilágítani a fegyvertartás rendészetére vonatkozó új biztonsági kihívások kezelése érdekében tett uniós lépések szükségességét.

Kulcsszavak: *fegyverigazgatás, biztonságpolitika, fegyvertörvény, új biztonsági kihívások, rendőrség.*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.26.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.23.

INTRODUCTION

On 13 November 2015, terrorist acts were carried out at several locations in Paris, where in several waves around two hundred people were killed by concerted attacks. To address the new security challenges (with focus on the illicit acquisition and trade of firearms) affecting the European Union, the European Commission has launched the negotiating phase on the preliminary control of legal norms of the draft envisaging stricter firearms regulation. Following terrorist acts, the Member States of the European Union have decided to introduce minimum rules to prevent the illegal acquisition of firearms. The purpose of the measure was to tighten up the legal framework for restricting the acquisition of firearms used in terrorist acts. Subsequently, the European Commission presented its professional concepts and guidelines for tightening the existing Firearms Directive (in force since 1991) to be the basis of a security protocol that shall be elaborated in future (where armament interests will be a secondary priority). The result of this restructuring was that civilian semi-automatic firearms similar in their operation system to fully automatic military weapons were intended to be reclassified from the 'B' weapons category (subject to authorisation) into the 'A' weapons category (banned). The changes, intended to be introduced, have given rise to a great indignation in the European Union's Member States having traditions with some civilian firearms. Many criticisms have been made in respect of the creation of rules for the introduction of measures to re-regulate civilian possession of firearms. The European Commission reasoned the need for stricter firearms regulation to address the new types of security challenges. The firearms concepts formulated in the draft directive deal with more stringent controls on hunting clubs and shooting clubs, the reclassification of firearms categories, the ban on semi-automatic weapons, the development of a technical standard system for deac-tivated weapons, and the transformation of the systems of rules on museum weapons.[1] [1]

The present study intends to carry out a background analysis (and also a legal analysis) in the context of the stricter firearms control strategy of the European Commission, seeking the answer to whether the recent arms control proposals provide for the European Union appropriate responding measures to the new security challenges posed by terrorist acts.

In the course of my investigations, I sought answers for three issues:[2]

- Is it justified on the part of the European Commission to tighten up the existing firearms control principles to address the new security challenges facing the European Union?
- To what extent does stricter firearms regulation affecting the Member States of the European Union influences the development of professional areas of sport hunting and shooting sports and the market situation of the European firearms manufacturers and distributors sector?
- Are the future revision of the European Commission's Firearms Directive and the formulation of proposals for its amending justified and necessary?

To answer the questions I used the method of literature research and analysis of legal regulations.[3]

---

[1] The author of the study explains his professional point of view that the EU draft on firearms would totally prohibit the use of semi-automatic weapons, as they can easily be converted into automatic firearms. In their view, changing the regulation would mean, from a professional point of view, that semi-automatic firearm types such as AR, AK, SKS, G3, or SL08 would be banned.

[2] These competences have been highlighted during the investigation, as these questions can answer (1) in what direction is it necessary to move towards a more uniform European firearms control, (2) whether the security challenges facing the European Union justify stricter firearms control in respect of civilian firearms.

[3] The primary tool of the research was the PubMed search engine and the online search in Scopus pubications database. The PubMed allows you to search the MedLine database of publications based on search queries. The

THE SYSTEM OF RULES RELATING TO THE AMENDMENT OF THE REGULATION AND CONTROL OF FIREARMS BY THE EUROPEAN COMMISSION

The European Union's Member States are primarily themselves responsible for maintaining and effectively securing the internal order and public security of the Member States, but the new cross-border security challenges require coordination of independent capacities to act of individual Member States and the efficient use of the EU funds to build trust and cooperation, and to facilitate information exchange and joint action. In order to strengthen cooperation on security issues in the European Union, Jean-Claude Juncker, the president of the European Commission, in his statement explained that according to the policy guidelines the European Union's security program should be addressed as a matter of priority, in connection with which the European Commission (in line with the 2015 Commission work programme) is committed to restrictions relating to safe transportation of firearms in order to enhance the implementation of the European Union's security policy concept. [2] On 28 April 2015, the European Commission set out a European Agenda on Security for the period 2015-2020 to support cooperation between Member States and to identify and address security threats. In the Agenda on Security, the European Commission has defined tackling of security challenges such as fight against terrorism, organised crime, and cybercrime. The European Commission has laid down the concrete tools and measures that can be taken by the Member States in their mutual work to improve public order and public security to address the three most serious threats more effectively. In the 2016 schedule and work programme, the European Commission envisaged to revise existing firearms legislation in 2016 to improve information sharing, strengthen traceability, standardise firearms marking and establish common standards for the firearms deactivation. [3] To prevent terrorist attacks and persistent threats affecting the Member States of the European Union, the European Commission has decided to speed up work processes in connection with civilian firearms significantly. The European Commission has taken significant steps to implement the elements of the Agenda. Measures and initiatives taken to strengthen security complement on-going work to combat the illegal trafficking of firearms, including, including in particular the operational action plan between the European Union and Western Balkans, and the joint investigations and the police cooperation, which have been in place since 2013.

---

database was set up in 1963, it became searchable on-line in 1971, then in 1997, the PubMed search engine was installed, and currently it contains more than 20 million publications from thousands of journals. During the literature research I used the following search terms: arms control, firearms delivery, arms law, administration order, police. Based on the contents of the abstracts, I deleted the non-topic articles from the list. From the remaining studies, I selected those, which specifically contained social sciences research in connection with the transport, import and export of firearms in the European Union and the transformation of the European Commission's system of rules related to the firearms control. I did not take into account the studies not dealing with the transport of firearms and the European Union's position on the firearms. I have excluded studies that have relevance to the transport, import and export activities and the field of firearms, but not on the basis of law enforcement, public health, statistical and legislative considerations. During the search activity outlined, forty studies have been identified, and I have also studied their research content and literature list for the full and effective processing of the research topic of this study. During the evaluation of the examined problems, the full texts of the studies were reviewed and I examined the details contained therein. The reviewed and used sources materials are generally suitable for secondary analysis to highlight the security policy risks associated with the transport of firearms and export-import activities in the European Union, with the focus on the risks interrelated with the trade in weapons and explosives in the context of weapons policy, and on its role to be played in identifying new security challenges from the viewpoint of restructuring the weapons rules.

AMENDMENTS TO THE RULES ON FIREARMS POSSESSION ADOPTED BY THE EUROPEAN COMMISSION

The European Commission has set up a package of proposals to amend a firearms di-rective to tighten the acquisition and possession of firearms by private individuals and the transfer of firearms to another European Union Member State.

The planned revision includes the following:[4]

-Adopting stricter (national) legal regulations prohibiting civilian possession of semi-automatic firearms. The measure states that semi-automatic firearms may not be in the possession of private persons under any circumstances, even if the deactivation of those firearms has previously been implemented in practice (in officially regulated way);

-Creation of stricter rules on the online sale of firearms to prevent the purchase of firearms, firearm pieces and ammunition on the Internet;

-Uniform regulation at Community level for the designation of firearms and the more effective traceability of weapons;

-More effective coordination and exchange of information between Member States. This productive contact and information system may assist in cases when an authorisation issued by a national authority for the possession of a firearm is not recognised by another Member State's authority as a valid authorisation. Problems arising from such situations can be eliminated by compulsorily linking Member States' official databases of weapons;[5] [4]

-Establishing common minimum criteria for specific weapons (e.g., signaling and starter pistols) so that they cannot be converted into fully functional firearms;

-Determination of stricter requirements for the dissemination and sale of deactivated firearms;

-Determination of stricter requirements for weapon collectors to reduce the risks of selling to potential offenders.

During the review, the European Commission has envisaged further additional restrictions on the use and circulation of deactivated firearms. [5] The amendment (taking into account the methods of perpetration of terrorist acts committed in the past) is primarily aimed to additionally restrict the civilian possession of firearms no longer authorising to possess, as is currently allowed, any of the most dangerous firearms falling under category 'A' – even if they have been deactivated. The European Commission delegates the implementation of the regulation to the national authority and also obliges the Member States to implement the destruction of illegally held weapons using all available forces and tools. The European Commission has identified collectors of weapons as a possible source of traffic of firearms, as persons ensuring the acquisition of firearms. According to the draft, firearms collectors should still have the possibility to acquire firearms, but under the same authorisation and declaration requirements as private persons.[6]

In order to improve the effective traceability of firearms, the European Commission has envisaged introducing stricter rules on the marking of firearms to avoid markings from being

[4] Amendments proposed by the European Commission shall also be approved by the European Parliament and the European Council.

[5] As an international example I would like to present the study explaining that the transfer of registered data on persons and organisations holding a firearm did not work effectively between Australia and New Zealand until the early 1990s. To resolve this problem, a provision was made to set up an inter-state infor-mation database, which helped to improve cooperation (in relation to firearms) between government agencies and criminal intelligence of the two countries, while maintaining the right of both countries to change or re-regulate the armaments regulation.

[6] Brokers will also be brought into the scope of the Firearms Directive, as they provide services similar to those of traders. Member States shall introduce regulations covering the registration of brokers and dealers operating within their territory.

easily erased or changed (e.g., as opposed to the markings on the label), and therefore extending the obligations in relation to imported firearms and clarifying on which elements new markings shall be placed. [6] A new regulatory element has been included in the draft saying that Member States will have to keep records of firearms for an indefinite period until the destruction of the firearm and not only for 20 years as is currently the case. Regarding tracing firearms, the European Economic and Social Committee has been seeking to submit a proposal for a directive of the European Parliament and the Council amending the Council Directive 91/477/EEC on control of the acquisition and possession of weapons. In its working document on the single market, production, and consumption, the Committee has formulated the objective of the Directive to ensure the security of citizens and to promote the functioning of the internal market by laying down rules for all stages of the life cycle of the firearm, ranging from production to destruction. [7]

REGULATION ON COMMON MINIMUM STANDARDS FOR DEACTIVATION OF FIREARMS

The Regulation lays down single criteria for the deactivation of firearms by Member States to render them inoperable for use as a firearm, which are much more stricter than the current regulations. In the context of the new security challenges affecting the European Union, the draft law proposes to tighten further up the possession of firearms classified in the most dangerous category and, at the same time envisages to strengthen the special capabili-ties of the police. [8] The regulation is based on the criteria for deactivating firearms developed by the Permanent International Commission for the Proof of Small Arms (the CIP). The proposed package of measures envisages an enhanced control over the firearm categories restricting the effective management of new security challenges[7] in the European Union, the strategic implementation of which is intended to be transferred by the European Commission (in order to ensure the effectiveness of the programme) into the legislative phase (REFIT) to ensure that the EU legislation meets the set objectives within the foreseeable future. The European Commission regularly reviews and updates the technical specifications set out in the regulation to ensure the effective deactivation of firearms in all cases.

REVISION OF THE EUROPEAN COMMISSION'S FIREARMS DIRECTIVE

The first part of the study presents and analyses the background of Directive 91/477 adopted by the European Commission on 18 November 2015, which contains proposed amendments to the control of the acquisition and possession of firearms. In this chapter, the solution structures are outlined in connection with the new security dilemmas justifying the tightening of the rules on firearms by the European Commission and affecting the European Union, which we are seeking to determine using a cooperative security model that operates with a complex toolbox.[8]

-normativism: the norms adopted by the European Parliament regarding the tightening of the rules on firearms (taking into account the value content) should be subjected to a critical

[7] Bulk irregular migration, asymmetric methods and terrorist offenses in developed countries, militarization of law enforcement agencies, strengthening of self-defense for specific areas of the private security sector, strengthening of self-defense capability, protection of key infrastructure for the care of the population, iaaues of entertainment place security.

[8] Using this model we analyse the directive and the outlined problems in an approach that the adoption and implementation of the criteria set out in the directive require a common professional consensus, with the involvement of all the actors that could be linked to lawful possession and distribution of firearms.

examination of their compatibility with the interests of Member States, market actors (arms manufacturers, distributors, professional interest organisations) and arms holders; [9]

-suitability: the legislative mechanism of the European Commission should take into account both the security policy challenges affecting the Member States of the European Union and the expectations and needs formulated in connection with the strengthening of people's confidence. In this context, the European Union's security policy concept needs to outline such solution structures in connection with new security challenges and risks, as mass irregular migration, terrorist acts committed using asymmetrical methods and special tools in developed countries, issues of necessity of militarisation of law enforcement agencies, the enhancement of self-defense in specific areas of the private security sector, the protection of infrastructures of high priority for supplying the population, issues of the security of places of public entertainment, or the addressing of challenges connected with firearms;

-complexity and comprehensive approach: new security challenges affecting the European Union require the use of complex systems of tools, including public, civilian and law enforcement solutions;

-multi-level approach: the complex system of secure stability of the European Union is shaped by state and non-state actors. Following the identification of new complex security challenges, it becomes indispensable and inevitable (following the logic of the multi-level approach model) that the strategy to be followed takes into account the interests of state and non-state actors associated with the identified security risk. Looking at this issue from another perspective: To address the new security challenges, the European Commission as a decision-making body defines in a coherent decision-making framework the interests along which a multi-level approach can be developed for efficiency, thereby reducing the injury to the interests of non-state (professional) actors;

-multilateralism: against the new security challenges facing the European Union, it is only possible to act effectively through the ongoing, intensive and effective multilateral cooperation between state and non-state actors.

Making the necessary impact assessments, those environmental, social, governmental, security and economic impacts may become identifiable that can provide a strategic overview of who may be involved in the legislative process. [10] After having analysed the security problems identified based on the impact assessment results, the European Commission provides for the policy objectives and the decision-making system and then, through examining the possible effects of the solution structures, defines a complex strategic action plan to address the security challenges effectively and quickly.

CONCLUSION

The European Commission's package of measures to tighten firearms control also in-cludes an implementing regulation laying down common minimum standards for the deactivation of firearms, which make re-activation much more difficult in case of deactivated firearms. The Firearms Directive stipulates that properly converted deactivated firearms are no longer considered firearms but pieces of metal that can freely move within the European Union's internal market without a firearm license. However, the experiences and conclusions of recent terrorist acts show that deactivated firearms may be illegally re-activated, either by using homemade firearm pieces or by using firearm pieces available through the Internet. These factors cover complex issues that require complex responses to identify and solve the problems. It is a fact that there is no single legal source with regard to the deactivation of firearms in the European Union, and this deficiency significantly increases the level of security risks. To address this problem, the European Commission has prepared a proposal pack-age that sets out rigorous and harmonised criteria how Member States shall include in their National Firearms Acts the deactivation criteria for firearms to become unfit for use as a firearm. The outlined measure is complemented by the prohibition of the possession of firearms of category 'A', which also imposes obligations on firearms holders in cases where firearms of category 'A' were deactivated. The European Commission's Implementing Regulation is based on the criteria for firearms deactivation developed by the Permanent International Commission for the Proof of Small Arms (the CIP). [11]

The European Commission has examined the role of the Internet in the illicit arms trafficking. The analysis of the Firearms Directive and preparatory studies investigating the policy field has shown that the firearms manufacturers and distributors are increasingly us-ing the Internet as a firearm sales channel. This information was backed up by police reports analysing recent terrorist attacks in the European Union. In some cases, firearms used to commit terrorist offenses were assembled from firearm parts legally purchased via the Internet. The European Commission proposes to prohibit the sale of firearms, firearm components, and ammunition via teleshopping (especially via the Internet), and the proposal provides a possibility to facilitate this for licensed traders, distributors, and brokers.

The overall finding and conclusion of the research is that illicit trafficking in firearms is a serious problem in itself and poses a security risk that significantly contributes to social insecurity caused by the perpetration of violent or compulsive offenses and other crimes (such as drug smuggling, trafficking in human beings, as well as terrorist attacks). [12] These security risks pose a significant threat to the security of the EU Member States and their citizens. In the European Union, the nature and scale of illicit firearm trafficking are difficult to assess due to the hidden nature of the problem. Within the framework of crossborder cooperation, the Member States and law enforcement agencies of the European Union take joint actions in combating illicit firearm trafficking in a number of cases. [13] We can also identify significant issues in dealing with crossborder illicit trade in illegal firearms. [14]

The provisions of the Directive are met by Member States on a uniform basis, but different structures have been used in the Member States with regard to the legislative framework for the fight against illegal firearms. This concerns the definition of offenses, the type and extent of sanctions to be applied to legal and natural persons, the aggravating or mitigating circumstances and the degree of neglect and intent. The international[9] and EU legal frameworks affecting the

[9] The United Nations Convention against Transnational Organized Crime, adopted by General Assembly resolution 55/25 of 15 November 2000, is the main international instrument in the fight against transnatio-nal organized crime. It o pened for signature by Member States a t a High-level Political Conference con-vened for

illicit trafficking in firearms are widely defined and give the signatories considerable discretion as regards the implementation of key provisions. The adoption, at the European Union level, of minimum rules against illicit firearm trafficking, would be beneficial for the police and the investigative authorities of the Member States allowing to reduce the legal uncertainty generated by differences in national legal systems, which would facilitate prosecution and greatly reduce the possibilities of criminals to use loopholes. [15]

The fight against illicit firearms trafficking requires the Member States to adopt a uniform and effective EU-wide legislation. Nevertheless, it is essential for the European Union, the Member States and the competent authorities to initiate cooperation and dialogue, at the national level and the EU level on policy issues, with financial and economic analysts, firearms manufacturers and traders, further with hunting clubs, sporting associations and professional chambers to reduce illicit firearm trade and to combat illicit online weapons trafficking.

A number of stakeholders reacted negatively to the ban on some semi-automatic firearms proposed in the package of measures by the European Commission, which measures are deemed to be an unnecessary and burdensome limitation by hunter and sports shooter societies objecting the lack of data from preliminary impact studies that could support expected legal, economic and professional implications. The conclusion can be drawn that the amendment to the Firearms Directive is necessary to address terrorist acts committed with firearms and the new security challenge affecting the European Union. It should be noted that the regulation may adversely affect the conditions of competition both within the internal market and the international market in a number of professional and economic fields closely linked to the legal possession of firearms (pushing back the online trade; weapons-related cultural heritage; historical weapon collections; research in connection with firearms; paid hunting).

REFERENCES

[1] Risiko durch EU - das Ende der halbautomatischen Waffen? 2015.11.18. https://www.all4shooters.com/de/Shooting/Waffenkultur/Ende-der-halbautomatischen-Waffen/ (download time: 19.01.2018)

[2] Európäische Kommission verschärft EU-weit Kontrolle von Feuerwaffen. Európäische Kommission – Pressemitteilung. IP/15/6110. Brussels, 18.11.2015.

[3] WINTEMUTE G.: *Broadening denial criteria for the purchase and possession of firearms: need, feasibility, and eff ectiveness*. In: Webster D, Vernick J. (Eds): Reducing gun violence in America; Johns Hopkins University Press 2013. pp. 78-81.

[4] BRENT DA, Perper JA, Moritz G: *Firearms and adolescent suicide: a community case control study;* American Journal Diseases Children. 147. (1993) pp. 1066-1071.

[5] Directive (EU) 2017/853 of the European Parliament and of the Council of 17 May 2017 amending Council Directive 91/477/EEC on control of the acquisition and possession of weapons. Official Journal of the European Union 2017.

---

that purpose in Palermo, Italy, on 12-15 December 2000 and entered into force on 29 September 2003. The Convention is further supplemented by three Protocols, which target specific areas and mani-festations of org anized crime: the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Espe-cially Women and Children; the Protocol against the Smuggling of Migrants by Land, Sea and Air; and the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition. Countries must become parties to the Convention itself before they can become parties to any of the Protocols.

[6] HEMENWAY D.: *Private guns, public health*; University of Michigan Press 2004. pp. 84–85.

[7] Working document of the Section for the Single Market, Production and Consumption on the Proposal for a Directive of the European Parliament and of the Council amending Council Directive 91/477/EEC on control of the acquisition and possession of weapons. INT/777. Brussels, 26.01.2016.

[8] Commission Proposals to strengthen control of firearms: Questions & Answers. MEMO/15/6111. Brussels, 18.11.2015.

[9] TRÓCSÁNYI L., SCHANDA B.: *Introduction to constitutional law; The Fundamental Law and Hungary's constitutional institutions.* Methods of Constitutional Law. HVG-ORAC Lap- és Könyvkiadó; 2014. pp. 54-56.

[10] WEBSTER D, VERNICK J, MCGINTY E, ALCORN T.: *Preventing the diversion of guns to criminals through eff ective fi rearm sales laws.* In: Webster D, Vernick J. (editors) Reducing gun violence in America. Johns Hopkins University Press; 2013. pp. 115-118.

[11] EIGEL, C.: *Internal Security in an Open Market: The European Union Addresses the Need for Community Gun Control.* In: Boston College International and Comparative Law Review. 18. (1995) pp. 430-431.

[12] SPAPENS, A.C.M.: *Trafficking in Illicit Firearms for Criminal Purposes within the European Union, Euro-pean Journal of Crime.* In: Criminal Law and Criminal Justice. 15. (2007) pp. 359-381.

[13] Europol coordinates joint action against arms trafficking in the Western Balkans. (https://www.europol.europa.eu/newsroom/news/europol-coordinates-joint-action-against-arms-trafficking-in-western-balkans (download time: 21.05.2018)

[14] COOK J. Philippe, CUKIER Wendy, KRAUSER Keith: *The illicit firearms trade in North America.* In: Criminology and Criminal Justice. 9. (2009) pp. 265-286.

[15] Study to Support an Impact Assessment on Options for Combating Illicit Firearms Trafficking in the European Union. European Commission. Brussels, 2014. pp. 94-97.

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

MENTAL LOAD CAUSED MENTAL AND BEHAVIORAL CHANGES

PSZICHÉS TERHELÉS ALATTI VISELKEDÉSI VÁLTOZÁSOK

ZÓLYOMI, Zsolt

(ORCID ID: 0000-0002-2800-1430)

zszolyomi1@gmail.com

Abstract

People are far different personalities, different characteristics, so of course they have different ways to live a stress situation or in an emergency situation. By calling experience, in terms of my study I was classified into three groups of people. The first group is the set of persons who do not have experience in the armed forces, in other words, it is the range of ordinary occupations, civil persons. The second group represents those individuals who have experience in the armed forces, with training, but they were not in real danger or in battle conditions. The third group includes those who served in a special forces, with experience gained from the deployment in combat conditions.

Keywords: *physiological effects, mental load, stress, behavioral changes, danger, emergency situation*

Absztrakt

Az emberek amennyire különböző személyiségek, más-más tulajdonságokkal rendelkeznek, így természetesen különféleképpen élik meg a stresszhelyzetet, a vészhelyzetet is.
Tapasztalataim előhívásával, vizsgálatom szempontjából három csoportba soroltam az embereket. Az első csoport azoknak a személyeknek a halmazát jelenti, akik nem rendelkeznek fegyveres erőknél eltöltött tapasztalatokkal, más szóval a köznapi foglalkozást űző, civil személyek körét jelenti. A második csoport azokat a személyeket öleli fel, akik rendelkeznek fegyveres erőknél eltöltött tapasztalatokkal, kiképzéssel, de valós életveszélyben, illetve harci körülmények között nem voltak. A harmadik csoportba azok tartoznak, akik valamilyen speciális alakulatnál szolgáltak, rendelkeznek bevetési, harci körülmények során szerzett tapasztalatokkal.

Kulcsszavak: *pszichológiai hatások, mentális teher, stress, viselkedésbeli változások, veszély, vészhelyzeti szituáció*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.15.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.28.

INTRODUCTION

Some of the people believes they can handle stress situations with adequate behavior, others thinks they would fail during a serious stress event. The real situation can be different or moreover opposite of their believes. Someone thinks he/she would able to direct people during an emergency situation, other ones would need direction from someone. According to some opinion we can predict the likelihood how the people will cope with extreme stress situations. According to my observations and experiences it is not completely possible to modelling the real life threatening situations in advance so it is not possible to forecast who will act and how, who will win who will fail. That measurement can work in the real life threatening situation only.

People are far different personalities, different characteristics, so of course they have different ways to live a stress situation or in an emergency situation. By calling experience, in terms of my study I was classified into three groups of people. The first group is the set of persons who do not have experience in the armed forces, in other words, it is the range of ordinary occupations, civil persons. The second group represents those individuals who have experience in the armed forces, with training, but they were not in real danger or in battle conditions. The third group includes those who served in a special forces, with experience gained from the deployment in combat conditions.

MENTAL LOAD CAUSED MENTAL AND BEHAVIORAL CHANGES

The first group, that is, with no experience in the military or police forces, are civilians. Fortunately there is not any or only very rarely nowadays a crisis situation where their lives may be in danger. Most of them may experience that feature in traffic accidents only. The smaller bumper to bumber accidents are stressful, but very fast therefore, psychological and behavioral changes in this kind of crisis situations does not occur. People get a little scared, then calm down after the event, they are glad that escaped the incident relatively easy. The more serious potential deaths or more deaths ending accidents also take place very quickly, if good-pass solution has been chosen by the driver, and he was lucky, then he/she could survive the accident if the wrong solution has been chosen and had no luck, then he/she may lose his/her life unfortunately. In these cases, the physiological effects of an emergency situation has developed over tenths of seconds, by loss of consciousness or death to an end immediately. [1]

The same characteristic of this group, if they become a subject of threat or violence, most of them are getting in panic, unable to think and act normally, the fear and dread completely overwhelmed their personality. They can not act and the received instructions are not able to grasp and execute. Accordint to my experience, their proportion is around 70% of the entire population.

During the raid of dangerous, armed criminals often happened that the arrested person was in so deep panick to urinate and / or defecate as he was not able to control himself, they were unable to hold back.

My experience shows within this group with missing military or police background, about 20% of the people, can be made according to the number of people who can be directed and the instructions, with some help enforced. E.g.: sit there, go there, do this or that, etc.

Based on my observations approximetely only 10% of the proportion of people who is in a panic situation did not get panic, but immediately focusing on the search for a solution on how to get out from the crisis situation, assess how can find escape routes, and what kind of opportunities are there. That person can effectively be thinking, making quick decisions, has the ability to weigh and choose the most effective solution, and to achieve this goal is the best strategic and tactical path method to figure out, laid out, and act accordingly.

In a rapid course of emergency situation when a few seconds only available to detect the situation, bypass and getaway, solutions with the least possible damage for reflection and execute the best possible solution then almost any organ emergency mode supports us the greatest possible performance for all mental and physical peak power of order.

In this moment we are a couple of incredible mental and physical efforts are able, when the time changes us, that our perceptions of time. We feel as if little had expanded the time had slowed down the happenings around us and we were given time to think through a lot more things, more things were perceived as normal, non-crisis state of our loads.

The second group is different from the first, that they have some level of training and experience, he spent the armed forces, in compliance with the basic psychological tests and inspections. My assessment point of view, they have already provided selectively on a higher level group, but my observations shows that there is no significant difference between the first and second groups experiencing life-threatening capabilities. [2]

In support to my opinion, I want to present two events. In both cases happened in the United Nations police and military peacekeeping mission, the first in Cambodia, in May 1993, the second in Angola in the spring of 1996.

The first case aimed at police officers who were my colleagues in a nearby Vietnamese border, Cambodian village in the jungle. One was a black African, the other came from a Maghreb country. There were tropical climate with almost 100% humidity, than the local population almost everyone has a weapon, usually AK-47, drugs, smuggling, shootings continuous have been heard and the active presence of the Khmer Rouges was characterized that period at the time.

During the elections in each of us (Police Observers) had to move out to a polling point for six days and there to keep watch over the elections in peace and security. The two colleagues reported sick, one with a neck ache the other one was complaining about general malaise and they traveled to the capital city to Phnom Phen where UN had the German field hospital for examination, so they could not participate in the ensuring of the election unfortunately. [3]

After the election, which would otherwise have taken place without any security issue in our district that two colleagues have arrived back in our village and dressed in bullet-proof vests and helmets, with a cambodian interpreter using one of our off road truck raced up and down the village to boundless relief, and thus raise concerns without any atrocity.

The local residents, has only just jumped away from them, but they confronted by a cambodian military jeep and the cambodian soldiers were forced to pull off the road.

The souting teenage soldiers jumped off their jeep, captured the cheerful team on the way when they turned backage from the end of the round cheerful team that saw the barricade of armed soldiers, they tried to turn back, but then they saw that the back is caught around them. Then they left behind the car and the interpreter, they jumped into the lush vegetation along the road and fled by running rushing till the first UN-inhabited house, which was 3-400 meters away. Then I arrived with one of my colleauge to the scene by driving our off-road car and I saw the following. They car was standing across of the middle of the road with open doors, beside of it was standing our sobbing and frightened interpreter, a number of armed soldiers in front of us. We could see the soldiers behind in the rearview mirror each other was using the back sides of the trees as a shelter, then a soldier jumped in front of my car who was shouting with us like hell by shaking a machine gun with his finger on the trigger of the gun. While he was shaking the machine gun, my Asian companion slide down on the seat as far as he could to take advantage of the engine cover. By holding my both hands in the air I signaled that I do not have a weapon and after they opened my door and took me out, I called the interpreter by shouting and asked him what happened and what the soldiers want. It was difficult to understand him, because the soldiers were still shouting with us and the interpreter was heavily sobbing, they wanted us to bring the people here, who pushed them out of the way and handing our

officers over for them. I still held my hands in the air and tried to calm the soldiers down through the interpreter, I said we fulfill all their wishes, just let us leave the site and I will bring the Africans colleagues back. They partially accepted my term I could leave the site by my car, but only me, alone and they kept back my Asian colleague and the interpreter. I promised to my colleagues I will be back with our UN colleagues for help, I saw the fear in their eyes, but I tried to encourage them. I was afraid that one of the overheated solders was losing his self-control and shoot after me, but fortunately it did not happen. I reached the house within two minutes, where our European commander already was there with some of our officers and the two perpetrators too. For the sake of our subject, it was interesting that both of them had lost all their equipment during their escape but even had their boots left, one of them because of comforts aspect never put on his boots adequately, did not ever thight his shoestring and the other one was wearing a zippered ankle boots authorized in his own country. They were so frightened that they could not coordinate their movements, their body were twitching, where they moved, especially with their heads rotating right and left, but their eyes were the most talkative, they could not look at anyone and nothing, their eyes glimpsed in the distance, or moved quickly in disorder. They were completely drenched in sweat and had a terrible odor, and their sweat was more pervasive and more unbearable than usual. We have taken several measures, after talking to the commander in private, outlining the possibility of not returning to the scene with the Africans colleagues, we can expect that they will attack us at night. We reported to the UN military observers who arrived at the scene armed and the command of the Cambodian soldiers to disarm their people when they reported this to us, we have been started only after to go to the scene. We did not succeed in convincing our African collegau that he had to go back and reconcile, he was just saying he did not go anywhere, so we managed to get him into the car with high physical efforts. While we were approaching to the scene, we had to hold him back with almost superhuman powers to avoid he do not get rid of it. On reaching the scene, we saw that the Cambodian command arrived and disarmed its men, and the UN armed military observers have already protected the scene. We listened to the complaints, promised that no more similar cases would occur, and then with a handshake they wanted to seal the peaceful closure of the case. The African did not want to get out of the car and shake hands with the insulted soldiers, who was half the size of my nearly two-meter-tall colleague. We could only solve this by holding his hands with two of us, but as if he was shaking like hit by electricity when his hand came to the hands of the Cambodian soldier. Probably because of this peace-making action, we have not been attacked by the Cambodian offended soldiers. Both colleagues had been removed from our duty station/willage on the same day, and they were repatriated to their home countries and the mission ended for them. To sum up, the fact that the two colleagues were members of armed forces, went through some sort of psychological screening, armed training, do not yet say that they were able to withstand the psychic load in a hostile confrontation or in this kind of similar situation. Especially it was the worse as they caused themselves that hostile situation which lead them into panic. Almost the same reaction were demonstrated by them that the majority of the first group had not been able to withstand the psychhic load, the life danger. Instead of all sorts of rational solutions, only the rushing escape was carried out, even without thinking or helping each other, individually, separately. The aforementioned physiological changes, powerful sweating, trembling with fear, "like an animal forced in the corner", superficial breathing, and dread decreased just even hours later.

The second case happened a few years later in a remote small village in Angola. Where half a dozen of us were serving half-police, half-military observers, representing all sorts of nations and continents. The country was still opposed by the government, the FAA and the insurgents, UNITA, a cease-fire was in place, in principle there were no major battles, only minor raids, the country was divided into two parts, but these were not contiguous areas but sporadically were located. The willage where our teamsite was located was under the control of the

government, but around us about 10 kms UNITA were controlling. Everything was undermining, the roads and the fields, every day we heard more explosions, local residents were starving. The supply can arrived by a small aircraft two-weekly from our UN regional center, but when the weather was unfavorable, it happened several times that the flight had been missed. Sometimes we were suffering missing supply of food, fuel, etc. for weeks or month. Under these circumstances, we were only able to investigate cases, like attacks each other camps, willages in the direction of the others hinterland, when a liaison officer entered our off-road vehicle and he showed the way, he knew where the minefields they were deployed. Those who did not go out for this kind of investigations stayed at home as a duty and emergency officer at the radio. In the evening at six o'clock the darkness comes with malaria mosquitoes, only one sollution was existed real protected place was to go to bed under the mosquito net. The continual emergency, the hardship and the terrible monotony of the months have overturned the nerves of several colleagues, the lucky ones have been relocated or left for leave. Unfortunately, a less fortunate European, middle age military officer could not cope with everyday tension and monotony. First of all, he did not dare to get out of the house, or to go out to patrol, or investigate a minor attack, he was unable to occupy himself by next to the duty radio or in his room, did not read, did not listen music, did not do sport exercises. He became more and more silent, locked inside him, and for days she sat with his face supported by two of his hands at the radio table. We tried to help him, but panic and anxiety were so overwhelming of him that all of our attempts failed and we needed to requested a medical evacuation for him by a helicopter rescue. [4]

Later, I heard that he had been repatriated in his home country and discharged from army on medical reason as he was mentally collapsed. In this case, he had not manage the impacts of a significant, sudden panic, but a small, continuous psychic load over a long period caused the colleague to have been unable to process the tension, he was constantly in fear and panic, and this constant psychological burden had disrupted the mental harmony of him, which made him unable to act and work.

The third group was observed by me from inside during a decade as I was serving for special counter-terrorist unit. To select members of the elite team, a very wide-ranging multi stage filtering system was established, the details of which would not be outlined right now. From my point of view, it is important to have a very strict, psychological screening of candidates for IQ, Rorschach, CPI, attention, etc. tests, and, in the mirror of the results an interview with a qualified psychologist was also carried out. Based on these measuring procedures, a profound, complete psychological picture could be gained from the candidate. Of all the entrance examinations or tests, the psychological examination was the one in which most applicants did not meet their proportions. We can conclude that those tests were carried out with the right rigor, since that was the one among of these examinations as the majority of the staff was afraid the most. But it was not just an access condition to get into the unit, but the quarterly psychological examinations were also part of the screening of the active unit members. So, each physical, sports, strategic, tactical, shooting, and so on exams had to comply and also with psychological examinations. [5]

SUMMARY

According to my opinion, based on my observations, with a rather in-depth and wide-ranging psychological test, greater deviances or lack of competence could be demonstrated, but it is not completely possible to detect how the individual would bear the psychic burdens in sharp, hostile situations during the deployments. The ability to live a life-threat can only be felt in life-threatening experience situations. We can get approximate information with tests and situational exercises about how the individual is likely to perform and behave but close to reality

can only be obtained if the situation is real, we can get a true picture only in the case of a sharp action, in a life-threatening situation. I have repeatedly observed that colleagues who were performing well on a daily routine shooting trainings could not reach the same result when it was a demonstration shooting where they had to handle the same practiced task for example before an intergovernmental delegations. If the bet has risen, for example, in the quarterly exams, this level of performance has deteriorated further, went under the demonstration level. During the sharp deployment, when they had to undergo extreme psychic stress, some individuals were not able to achieve even their average performance. Of course, in this group, the ratios were just the opposite of the first group studied, so they were in great numbers, thanks to their abilities, continuous trainings, excercises, careful selection and continuous screening, who performed their job perfectly under a considerable psychological load and only had a fraction of them who was unable to stand up to the expectations of their duty.

I would like to add that about the ability to live a life-threat situation I do not think there is a man who would not be afraid to solve a situation where he might be injured or lose his life. If someone claims that he is not afraid of not telling the truth or not the master of his personality. The palm will be damp, the mouth will open a little, the throat will dry out, the breathing will become more prolific, the pulse will pop up, the man's gaze will betray everything, look into his eyes and you can see if he will be able to act as it is expected or he has to remove him from that position and give him an other task. The fear has to be overcome, there are some people who can do this, there are some who can become capable of doing this by a crisis situation, and there are some who can not overcome their fears.

REFERENCES

[1] HOYOS, C. G.: *Mental load and risk in traffic behaviour*, https://www.tandfonline.com/doi/abs/10.1080/00140138808966700 (dowloaded: 04.03.2018)

[2] BOLGÁR J.: *Viselkedési kockázat vészhelyzetben*, http://www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-02-Bolgar_Judit.pdf (04.16.2018)

[3] MICHAEL, D.W.: *The UN Sponsored Elections of 1993: Were They 'Free and Fair'?,* http://www.seasite.niu.edu/khmer/ledgerwood/free_and_fair.htm (downloaded: 04.15.2018)

[4] MORRIS, P.: *Back to Angola: A Journey from War to Peace*, Zebra Press 2014.

[5] COLEBROOKE, L.: *Special Operations Mental Toughness: The Invincible Mindset of Delta Force Operators*, *Navy SEALs, Army Rangers & Other Elite Warriors*, 2015

HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

WI-FI HÁLÓZATOK KÉT KIJÁTSZHATÓSÁGI PONTJA: WPA2 ÉS ROGUE AP

TWO ERROR OPTIONS OF WI-FI NETWORKS: WPA2 AND ROGUE AP

KOSKA Melinda Henriett

(ORCID: 0000-0003-2909-8788)

koskameli@gmail.com

Absztrakt

Tavalyi év során fény derült a WPA2 titkosítási protokoll hibájára, mely több milliárd eszközt és gyártót is érint. A hiba kiküszöbölése még folyamatban van és a probléma megoldása a WPA3 lesz majd, illetve egyéb felhasználói ajánlás is megfogalmazásra került.
A Wi-Fi hálózatokhoz kapcsolt másik általam vizsgált támadási forma a rogue ap-ok, melyek engedély nélküli biztonsági rések. Mind a két esetben az adatfolyamok lehallgathatók, manipulálhatók, ezért kell különös figyelmet szentelni e két területnek.
Az Emberi Erőforrások Minisztériuma ÚNKP-17-2-I-NKE-79 kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.
Kulcsszavak: *Wi-Fi, WPA2, Rogue AP*

Abstract

Last year, became known, default of WPA2 security protocol. It means billions of devices and companies. The problem solution is still in progress, WPA3 is coming and other user's recommendations have been formulated.
Another form of attack, which connected to Wi-Fi networks is the rogue ap, that has been installed on a secure network without explicit authorization. In both cases, the data stream could be listened and manipulated, that is why the users and companies need to pay attention to these two areas.
Supported by the ÚNKP-17-2-I-NKE-79 new national excellence program of the ministry of human capacities"

Keywords: *Wi-Fi, WPA2, Rogue AP*

A kézirat benyújtásának dátuma (Date of the submission): 2018.04.25.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.10.

BEVEZETÉS

Az információs és kommunikációs technológiák a 21. század egyik legdinamikusabban fejlődő iránya, amely több területre is hatással van. A szerteágazó irányai közül az általam vizsgált terület, a wireless-es technológiák, azaz vezetéknélküli csatlakozás egy része, a Wi-Fi hálózatok biztonsága. Azon belül is a WPA2 protokoll és a Rogue Access Point (továbbiakban AP) használatakor felmerülő biztonsági kérdések.

Informatikai rendszereket majdnem mindenki használ, csak eltérő szinten. Az informatikai infrastruktúra iránt egyik általánosságban elvárt szolgáltatás a vezeték nélküli, teljes lefedettségű, mindenki számára elérhető szélessávú, gyors internet hozzáférés, csökkenő költség hozzájárulással. [1] Mivel egyre többen használják a vezeték nélküli technológiákat, fontos hangsúlyt fektetni a helyes internet, hálózatok használatára és az adatok biztonságos kezelésére.

Az emberi tényező az egyik legkritikusabb az adatszerzések útvesztőjében, azért, mert halmozottan rendelkeznek olyan jellegzetességekkel, amelyek alapján nagyvalószínűséggel potenciális áldozatokká (adatlopás, információszivárogtatás, beszervezés) válnak. Az első lényegi pont, hogy olyan adatok birtokában vannak, amelyek védendőnek számítanak, még akkor is, ha ez számukra nem triviális. A másik oldal pedig a kihasználható emberi tulajdonságra alapoz, mint például a hiszékenység, naivitás, kíváncsiság, gyors információszerzés utáni vágy, avagy a segítőkészség.

A fentebb felsorolt emberi tulajdonságokat a nethez való csatlakozáskor is ki lehet használni. Olyan támadási formákat kivitelezésére alkalmas az internet, mint például, az adathalászat, adatlopás, rosszindulatú alkalmazások elterjesztése, megfigyelés lehetősége, avagy a hálózat üzemeltető részéről olyan adatokhoz való hozzájutás, mint a böngészési információk, jelszavak és a beszélgetések. Így könnyen zsarolhatóvá válik az ember például egy-egy elküldött fénykép, üzenet által. Fokozottan igaz ez, ha a felhasználó egy nem biztonságos Wi-Fi hálózaton keresztül továbbít adatot. Másik lényeges vizsgálandó pont a tudatos és nem tudatos internetfelhasználók köre. Utóbbi kategória fejlesztéséhez szükséges meglátásom szerint, a támadások fajátinak ismerete, védekezési mechanizmusok. A hipotézisem, mely felméréseken és beszélgetéseken alapul a Nemzeti Közszolgálati Egyetem hallgatói köréből, [2] hogy a felhasználók a Wi-Fi hálózatokon keresztül történő adatforgalombiztonsága ismereteinek hiányával küzdenek.

FENYEGETETTSÉG

Egyre többen kapcsolódnak be az információ- és kommunikációtechnológiába. [3] Ennek egyik ága a wireless technológia, mely vezeték nélkül képes áthidalni óriási tereket. Így hatalmasat lendít a mobilitáson. Fizikai jelenlét nem kell ehhez a kapcsolat létrehozásához, azonban a rádiós csatorna jellege miatt, könnyebben hozzáférhető a rendszer, mint a vezetékes internet elérésnél. A vezeték nélküli kapcsolat a leginkább hatékony, rugalmas és költséghatékony megoldás a mindennapi élethez, legyen szó iparról, mezőgazdaságról, szolgáltató szektorról, avagy a privát felhasználói tevékenységekről. Minél több eszköz és ember vesz részt a kiterjesztett világban, annál több dologra kell figyelemmel lenni biztonsági szempontból. [4] Nem csak a védelem informatikai hatékonyságán múlik az adatok és a privátszféra védelme, hanem a biztonságtudatos felhasználókon is. Egy nemzetközi jó gyakorlat Németországból, hogy nem csak a felhasználókat terheli felelősség adatvédelmi szempontból, hanem az internetkapcsolatok üzemeltetői is felelnek a megfelelő biztonságért. Egyedi ügyben olyan

állásfoglalást hozott a bíróság, hogy a WLAN hálózatot nem lehet nyíltan hagyni, jelszóval kell védeni, azonban a nemzetközi joggyakorlat nem követi ezt a példát. [5]

INTERNET OF THINGS (IOT)

Az internet forradalma eddig az embereket kapcsolta össze, a következő lépés azonban a tárgyak összeköttetése (lesz), ami az Internet of Things (dolgok internete, továbbiakban IoT), mely képes a netet használva egyszerre érzékelni és kommunikálni több eszközzel. [6] Az Internet of things kifejezés már az 1900-as évek végétől használatos. A Wi-Fi és a 4G-LTE vezeték nélküli internet elérésének növekvő térnyerése, és a mindenhol jelentkező információ és kommunikáció felé vezető irány már teljesen nyilvánvaló. Mindennapos használati tárgyként már beleivódott a köztudatba a laptop, tablet, okostelefonok, okos televíziók, videójáték konzolok, de már a hűtőszekrények [7] és a légkondicionálók is. Ezen technikai eszközök teljes mértékben az emberektől függenek, olyan értelemben, hogy a tárgyak az adatokat, információkat az embertől érzékelik, vagy vele kerül kölcsönhatásba legtöbbször. Azonban az IoT sikeres elterjedéséhez szükség van számítástechnikai paradigmaváltásra, és tovább kell lépnie a hagyományos mobil eszközökön, és a mindennapos használati tárgyaknak kell összekapcsolódniuk, amelyek körülveszik az embert. A cél ezen eszközök autonóm, emberi beavatkozás nélküli, és okos viselkedése, ami egy teljes világot átfogó integrált jövő internethez vezet, s ehhez három alappillérnek kell teljesülnie; a felhasználók és a készülékeik közötti feltételnek, amelyek feldolgozzák és közvetítik az információkat, ahol releváns, és ezeket vegyítve, elemzést kell végrehajtaniuk. A három pillérhez három paradigma is tartozik, ami az internetorientáltságot, a szenzorokat, és a tudást foglalja magában.

Az IoT-ot heterogén technológiák jellemzik, amely jellegéből adódóan folyamatosan újul, időről-időre új megoldások kerülnek felszínre. Különböző biztonsági és adatvédelmi követelmények problémák látnak napvilágot, melyek megoldásra várnak. Ilyen követelmények többek között, az adatok, adatátvitelek titkosítása, engedélyezése és hitelesítése, a rendszerhez való hozzáférés szabályozás, visszautasítása rendszertől. Ez alatt az érthető, hogy nem csatlakozhat a kliens a hálózathoz. További elvárás a felhasználó és az eszköze közötti bizalom kiépítése. A hagyományos biztonsági eljárások már meghaladottak, illetve a felhasználók a már meglévő technikai megoldásokat sem használják ki kellőképpen. A felhasználók bizalmának foka, megléte határozza meg, hogy milyen eszközöket használnak a mindennapok során, illetve a támadások egyik kulcs kérdése is, hogy a célpont az érkező támadóval, vagy támadással szemben bizalommal kezeltetik-e, vagy fenntartásokkal.

Az eszköz-eszközzel való kapcsolatok rohamos növekedése nem csak az adat mennyiségét és forgalmát növelik, hanem egyéb számítógépes fenyegetések számát is. A machine to machine (azaz eszköz és eszköz közti kommunikáció, továbbiakban M2M) jelen állapot szerint nem védettek, illetve nem eléggé védettek a kibertámadásokkal szemben.

2011-ben az összekapcsolt eszközök száma elérte a Föld lakosságának teljes számát. Több milliárd új eszköz részvételét eredményezi ez a folyamat. 2013-ban a 2020-ra várható összekapcsolt tárgyak számát 24 milliárd eszközre saccolták [6, p.1645-1646], addig ugyanerre az évre vonatkozólag 2016-ban már ötven milliárd objektumra számítanak az előrejelzés szerint. [8] [9] [10]

Ebből is látszik, hogy ez az új tendencia korai szakaszában van még, de rohamos fejlődésen fog keresztül menni, [11] [12] sőt az élet területének szinte minden részét érinteni fogja, különösképpen az egészségügyet, [13] [14] [15] az ipart, a katasztrófa előrejelzést, [16] az autóipart, logisztikát, közlekedést, tehát összességében jobb életkörülményekkel kecsegtet mindenki számára. Ezért elkerülhetetlen, hogy az IoT-nak megfelelőnek kell lennie ahhoz, hogy az adatokat, amelyeket összegyűjt és továbbít, biztonságosan tárolja és továbbítsa. Az IoT sikeressége érdekében kulcsfontosságú a dolgok egyedi azonosítása. Ez teszi lehetővé, hogy az

adott eszközt egyedülállóan azonosítanak és távoli eszközöket az interneten keresztül vezérelni lehessen.

A képi világa az IoT-on alapuló alkalmazásoknak létfontosságúak, mivel ez hozza létre a felhasználó és a környezet közös pontját. A fejlesztések az érintőképernyős technológiákat részesítették előnyben és igen elterjedté tette az okostelefonokat és a tableteket. A laikus személy számára, hogy teljes mértékben részesévé tudjon válni az IoT forradalmának, vonzó, interaktív és könnyen érzékelhető vizualizációt kell létrehozni. Példaként említhető e képi megjelenési formára a 2D-ről a 3D-re váltás. Az adatokat, információkat gyorsan tudássá kell alakítaniuk az eszközöknek, ami egy kritikus pontja többek között a gyors döntéshozatalnak is. [6, p. 1649]

A felhasználó olyan módon is részt vesz ebben a körforgásban, hogy az adatok egy részét ők maguk viszik fel a rendszerbe. Példaképpen Gmail fiók létrehozásánál szükség van a teljes névre, születési dátumra, nemi hovatartozás megadására, opcionálisan mobiltelefonszám beütésére, jelenlegi e-mail címre és tartózkodási helyre, amit beállításoktól függően már előre is kitölt a rendszer. Azt ígéri a Gmail, hogy csak néhány személyes adatra van szükség az új e-mail cím létrehozásához, amelyekkel segítenek megőrizni a fiók biztonságát, és még hasznosabbá teszik a különböző szolgáltatásokat. [17] Ezeknek az adatoknak a hitelessége azonban megkérdőjelezhető, tehát a kiindulási információk nem feltétlen pontosak. Nem tudatos adatmódosításról, adat beviteli hiányról van szó, hanem az emberi mivoltnak a determináltságáról, ami időhiányban, figyelmetlenségi és pontossági problémákban nyilvánul meg. A hálózati rendszerek az emberek által bevitt adatokból indulnak ki, és onnan végzik a feladatukat, amelyek azonban mivel az alapfeltételezés nem mindig helyes, költség- idő hatékonysági szempontból kár keletkezhet. Ha a tárgyak saját maguk vehetnék fel az információkat a külvilágból emberi segítség nélkül, akkor az emberek részére olyan adat és információ halmazok állnának, melyek nagymértékben csökkentenék a veszteségeket, melyeket ma még realizálni sem lehet. [18]

Minden okos, intelligens rendszer rendelkezik hibával. Egyik vicces rendellenességet az Amazon hangvezérlésű intelligens asszisztense, Alexa, prezentálja legszemléletesebben véleményem szerint. Alexa hang alapon rendel, keres a neten, és végrehajt, azonban nem csak az adott felhasználótól érkező parancsot teljesít (akár a TV-ből hallott információt is). A „hölgy” bankkártyához van kötve, amely segítségével tud vásárolni, azonban így nem behatárolt támadási vektor tud lenni akkor, ha nincs egy megerősítő közbeékelődő folyamat beinterpretálva a megrendelés és a fizetés között, akkor ez bankkártyával való visszaélésnek is minősülhet. Illetve egy bohémebb példa az okos eszközök hibáira, szintén Alexától, hogy kineveti a felhasználót, ami inkább bosszantó, mintsem támadás, vagy rés lenne. [19]

WI-FI hálózatok

A Wi-Fi (wireless fidelity) vezetékes kapcsolat nélküli kommunikációt, hálózati technológiát jelent, amivel rádióhullámokon keresztül a vezetékes hálózathoz lehet csatlakozni. Minden vezetékes vagy vezeték nélküli hálózatnak meghatározott protokoll szerint kell működnie. Ebben a jelentésben a protokoll arra vonatkozik, hogy az adatok hogyan cserélnek gazdát. A Wi-Fi Alliance céghálózathoz tartozik a Wi-Fi termékek tanúsítása, s meghatározzák, hogy milyen szabvány alapján nevezhető egy termék Wi-Fi-nek. Ez a szabvány most az IEEE 802.11, ami adatkapcsolat és adattitkosítási metódus. [20] Több fajtája ismeretes, privát, nyilvános (közösségi tereken használt, kávézókban, könyvtárakban), nyílt (csatlakozásához nem kell jelszó) és zárt (jelszóval védett). Az adattitkosítási részében biztonságos hálózatnak hívják azt, amit titkosítási algoritmusok védenek, amelyek a WEP, WPA, WPA2. A WEP a legkorszerűtlenebb algoritmus, mely kevesebb, mint egy perc alatt feltörhető, így a használata nem javasolt.

A Wi-Fi hálózat főbb komponensei a következőkből állnak

- hozzáférési pontból, azaz Wireless Access Pointból, mely a Wi-Fi és a kábeles hálózatot összekötő útválasztó, így használhatóvá válik a vezeték nélküli hálózat.
- Kliens, ami lehet számítógép vagy program, ami hozzáfér egy szolgáltatáshoz, amelyet egy számítógép hálózathoz tartozó másik számítógép nyújt. [21] [22]

Az AP hozzáférési pontot jelent, melyen keresztül tud a Wi-Fi-t használó eszköz csatlakozni a vezetékes hálózathoz. Ez több eszköz számára elérhetőséget biztosít a hálózathoz, az IEEE 802.11-es vezeték nélküli adatátviteli protokollban, ez a szám maximum 25 lehet. Azonban, ha nagy területet kell lefedni, akkor a vezetékes hálózathoz több Access Point is tartozhat, így kiküszöbölve a maximális felhasználói csatlakozó számot és a nagy terület lefedettségét.
WLAN hálózatokban több hozzáférési pont található, emiatt szükséges egy azonosítás, mely pontosan meghatározza, hogy mely hozzáférési pont mely felhasználóhoz tartozik. Az azonosításhoz a MAC címet használja. [23] A MAC cím az egyedi hardver azonosító az eszközhöz. Neve egy rövidítésből fakad, a Media Access Controlból. Célja, hogy minden azonosító egy adott eszközt azonosítson. A probléma a beazonosítással, hogy csak a következő útválasztóig lehet visszakövetni az adott eszközt, miután elérte az útválasztót, azután már az útválasztó MAC címén keresztül folynak tovább az adatok. Másik probléma a visszakövethetőségével, hogy viszonylag könnyen megváltoztatható. Az egyén oldaláról közelítve pedig, egyértelműen azonosítja a felhasználóra vonatkozó APt, hogy melyikhez autentikáljon, azaz kapcsolódjon. Helyváltoztatással másik routerhez (útválasztóhoz) csatlakoznak, ahol adatkapcsolati rétegen használt azonosítót (basic service set identifier továbbiakban BSSID) kapnak. Az eszközök és a felhasználók (kliensek) hitelesítése az egyik legfontosabb a vezeték nélküli rendszerek működésében, ezért fontos a MAC és a BSSID.

Hálózati protokollok

Az azonosítás és a biztonság megőrzéséhez elengedhetetlen ismerni a nyílt rendszerek összekapcsolásának referenciamodelljét, az Open Systems Interconnection Reference Modelt (továbbiakban OSI). Rétegelt felépítésű, mely a hálózati protokoll meghatározásában játszik szerepet. Alulról építkezik, és csak azokkal az adatokkal tud dolgozni, melyeket az alsóbb rétegből kap, felfelé pedig csak egy lépcsőt ugorhat. Az OSI referenciamodellje meghatározza két számítógép közti kommunikáció feltételét. Vetélytársa a TCP/IP lett, így mára ennek a modellnek csak egy részét alkalmazzák.

- Legalsó rétege a fizikai réteg, ahol a bitek kijutnak a kommunikációs csatornára.
- Második szintje a modellnek az adatkapcsolati réteg, ahol létrejön a két hálózati elem között az adatok továbbítása. Azonosításra visszautalva, a MAC címek találhatóak itt.
- Hálózati réteg követi az adatkapcsolati réteget, ahol adatátvitelhez szükséges eljárások találhatóak, mint például útválasztó választás. Itt az egyik legjellemzőbb protokoll maga az IP.
- Amennyiben az adat elindul a kommunikációs csatornára, már rendelkezik adatkapcsolattal. A két végpont és az útválasztó megválasztása is már lezajlott, akkor a szállítás lesz a következő lépcsőfok.
- Ezután a csomópontok kommunikációján múlik az adatok áramlása, ami a viszony réteg.
- Ha az adat végig haladt ezen a folyamaton, akkor alkalmasnak kell lennie, hogy a végfelhasználó számára megfelelő formában álljon rendelkezésre, ez lesz a megjelenítési réteg.
- A hetedik réteg dolga a bejövő adatok értelmezése. [24]

A hálózati protokollok, amely leírja, hogy az eszközök milyen módon tudnak egymással kommunikálni, a fentebb felsorolt szintekhez kapcsolódva többféle csoportosításban jelennek meg. A lentebb kiemelt területek a laikusok számára általam legtöbbször előforduló elemek. Az OSI modell legalsó szintjén, az L1-es szinthez tartozik az Ethernet (amely a legelterjedtebb hálózati megoldás, nagy sebességgel), USB, Wi-Fi és Bluetooth.

A kommunikáció akkor jön létre, ha jelen van egy adatkapcsolati réteg, amelyen keresztül zajlik az adatok hibamentes, biztonságos szállítása a hálózati csomópontok között. Az információkat keretbe rendezik, szükség szerint tördelik és ellátja kiegészítő címekkel, plusz egyéb ellenőrző információval. Az L2-es szinthez az ARP tartozik, (angolul Address Resolution Protocol), és az IP címet és a MAC címet rendeli egymáshoz. Az ICMP (Internet Control Message Protocol) tartozik még ide, amelyet az interneten használnak, s legtöbbet a hibák meghatározásánál felfedezhető. Adatcsomagokat figyeli, hogy hibásan érkezett vagy nem, hányszor érkezett meg, vagy elveszett a hálózatban, illetve az egymás után küldött csomagok sorrendjét is figyelemmel kíséri. [25] [26] A DHCP egy dinamikus állomáskonfiguráló (Dynamic Host Configuration Protocol) kliens-szerver protokoll, (amely tartozhat az L3-as szinthez is, ekkor relay-nek nevezik) amelytől a hálózati állomások az IP, illetve egyéb protokollokkal kapcsolatos információkhoz hozzájutnak a rendszergazda közvetlen beavatkozása nélkül, így időt, pénzt és energiát spórolnak meg. Feladata, hogy egy IP címet egyszer osszon ki.

A harmadik szinten található az IPv4, IPv6, mely a hálózati protokollok csoportjába tartozik, tartalmazza a címzett és a küldő címet, valamint a portjait. A routerek ezek alapján döntenek a csomagok továbbításról.

Az L4-ik szintjén a TCP van, ami egy kommunikációs protokoll, mely mostanra az egyik legelterjedtebb lett a gondos kidolgozása miatt. Folyamatosan ellenőrzi adatfolyamatot, így megbízhatósága is kitűnő. [27] Magasabb szintű szervíz protokollok csoportjába tartozik a Hypertext Transfer Protocol (kérdés-válasz protokoll, továbbiakban HTTP), ami az egyéni felhasználók szempontjából a legtöbbször előbukkan, mivel az URL címben legtöbbször HTTP-s címekkel találkozhatnak. Ugyanezen szervíz protokollhoz tartozik, az Interactive Mail Access Protocol (levelezési protokoll, továbbiakban IMAP), mely segítségével kezelhetők, illetve távoli elérésre alkalmasak a leveleket. Először csak a fejlécet küldi el, ami alapján lehet dönteni egyes levelek külön letöltéséről, azonban nagyobb tárhelyet is igényel, ezért nem terjedt el. [28] A POP3, mely a levelezési protokollok csoportjába tartozik, amellyel letölthetők a levelek. [29] Az SMTP is idetartozik, amely szintén levelezési protokoll. [30]

A szintek legfelső fokához a DNS (Domain Name System) tartománynévrendszer tartozik, mely alkalmazási protokoll, mint a DHCP. A tartományneveket kezeli, szükség szerint átalakítja numerikus azonosítókká. Ez segít abban, hogy különböző területről, különböző eszközökkel ugyanaz az oldal jelenjen meg a világhálón, habár változtak a körülmények. A felhasználók számára egyszerűsít, mivel csak számokból álló kombinációkat nehezen jegyeznek meg, azonban egy domén nevet (mint például https://akk.uni-nke.hu/), azt sokkal könnyebben, viszont ez a könnyítés nem használható a hálózaton belüli kommunikációban, s a DNS ezt hivatott átkonvertálni numerikus leírássá. Az internet struktúrájában kettő névtér létezik, az általam itt taglaltat és az IP-címteret. A Domain Name System felelős az első szegmensért, és fordítási szolgáltatást nyújt az IP-címterek és a DNS nevek között.

WPA2 titkosítási protokoll

A Wi-Fi Protected Access 2 (továbbiakban WPA2) a vezeték nélküli rendszerek protokollja immáron 15 éve, amelyet a titkosítás érdekében, azaz adatok megőrzése céljából fejlesztettek ki. 2017 októberében Mathy Vanhoef rátalált egy olyan hibára, amely szerint a protokoll, vagyis a titkosítási folyamatot leíró szabvány a hibás, nem pedig az egyes rendszereket létrehozó termékek vagy kivitelezésük. [31] Ez azt jelenti, hogy a teljes átmenő adatforgalom

megfigyelhető, illetve bármi elhelyezhető az adott eszközön, akár további megfigyelés céljából is.

Amikor vezeték nélküli csatlakozás létrejön, akkor a hálózati vezérlővel megegyezik a kliens a titkosítási kulcsról. Telepítés után ezen keresztül fognak az adatcsomagok vándorolni a titkosítási protokollt (jobb esetben a WPA2-őt) használva. Azonban, amikor megérkezik ez a titkosítási kulcs, előfordulhat, hogy többször küldi el, mert a rendszer számol a térben elvesző adatokkal, így pedig a számlálót (nonce), ami az adatcsomagok forgalmát nézi, lenullázza. Erről az anomáliáról (Key Reinstallation AttaCKs) kapta a nevét a felfedezés, a KRACKs. A titkosításnak az lenne a kiindulópontja, hogy nem ismétlődhet meg a titkosítási kulcs lekérése-elküldése, főleg úgy, hogy lenullázza a számlálót, mintha addig semmi sem történt volna. Ez azonban nem valósul meg. A támadó a titkosítási kulcs lekérésénél kapcsolódhat be, lenullázhatja a számlálót, innen a WPA2-be is bele lehet nyúlni, és a hálózati csomagokkal minden megtehető, amire a támadónak szüksége lehet, mint például bankkártya adatok megszerzése, jelszavak visszafejtése, chatelések elérése, e-mailekhez és képekhez való hozzáférés. A támadást több féle módon is el lehet követni, egyik példája az elvileg mindig eredményes brute-force, ami egy számítógépes program, és az összes lehetséges jelszókombinációt kipróbálja, hogy megszerezze a titkosítást biztosító kulcsot és bejusson a rendszerbe. [32] Minél hosszabb a jelszó, és minél összetettebb, szótár alapon nem kitalálható, annál időigényesebb feltörni, illetve bizonyos rendszerek, mint a Gmail, pár próbálkozás után letiltja bejelentkezést. A hálózati konfigurációtól függően nem csak adatok megszerzésére irányulhat ez a folyamat, hanem adatok bevitelére és manipulálására is. A támadás az összes Wi-Fi hálózat ellen hatásos, és bármilyen okoseszköz áldozatul eshet, de érdemes megemlíteni a kevésbé védett Androidos rendszereket, melyeken az adat visszafejtés egyszerűbb és gyorsabb is. Az Android operációs rendszer Linux-alapú és körülbelül évente kétszer új verzió kerül a piacra. A WPA2-es hibák a 6.0-és újabb verziókat érintik, amely azt jelenti, hogy 800 millió okostelefont és tabletet. Az alapvető probléma ebben az esetben, hogy a kliens az all-zero titkosítási kulcsot telepíti az eredeti kulcs helyett. [31] Magát a WPA2 titkosítást milliárdnyi vezeték nélküli eszközön használnak.

A CERT (Computer Emergency Response Team), egy szakértői csoport, akik a megfelelő eljárások alkalmazásában segíti a szervezeteket, ügyfeleket, kormányokat, a számítógépes hálózati incidenseknél, mint ahogy ezt az esetet is. [33] Az amerikai CERT figyelmeztetést adott ki a hibáról: „*az US-CERT tudomást szerzett a hibáról a WPA2 biztonsági protokoll négyirányú kézfogásakor észlelt problémáról. A szabvány minden típusa érintett*.” [34] Készítettek egy listát, hogy mely gyártók érintettek, idetartoznak többek között az Android Open Source Project, az Apple, a Microsoft Corporation, a Samsung Mobile, a Sony Corporation, melyek mobilkészülék gyártók, illetve okos eszközökre fejlesztenek ki operációs rendszereket. A Microsoft Corporation volt az első, aki reagált a problémára és elsőként dobott piacra frissítést ennek a hibának a kiküszöbölésére. Továbbá ide sorolható a Cisco Systems, Juniper Networks, Fortinet, Ubiquity és a D-Link System, a Netgear, a TP-LINK, melyekkel általában routerek és modemeknél lehet találkozni. A Dell, a Toshiba Electronic Devices & Storage Corporation és a Lenovo cég is érintettek, akik laptop gyártó cégek. A Google sem képzett kivételt. [35]

A támadások megelőzésére többféle módszer is lehetséges. Amennyiben és amikor az új termékek frissítése megjelenik, élni kell a lehetőséggel. A szakértők javasolják a router firmware-jének (mikroprogramjának) a módosítását. A Wi-Fi hálózat jelszó frissítése, mint megoldás, nem eredményez megoldást. Olyan hálózatokon, ahol ismeretlen eszközökhöz csatlakozik a kliens, nem bízhat meg az adatok biztonságát védő, illetve nem védő rendszerekben, mert nem ismertek a körülmények, a technikák, ilyen esetben a felhasználónak saját magának kell megteremteni azt a közeget, ahol az adatai biztonságban vannak. 2018 januárjában már fejlesztés alatt áll a Wi-Fi Protected Access 3, azaz a WPA3. Ez már védelmet

nyújt a brute-force jellegű szótársa támadásoktól is és a magasabb szintű biztonságot igénylő cégek, szervezetek, kormányok magasabb bit számú biztonsági réteggel dolgozhatnak. [36]

Rogue AP

A Wi-Fi hálózat egy osztott közeg, s a biztonságra, védelemre meglátásom szerint Magyarországon a kevesebb pénzből kivitelezett megoldások nyertek teret, ami által nem lesznek védve az adatok.

A Rogue AP, magyarul csaló hozzáférési pont, ami a Wi-Fi hálózatnál jelent kockázatot. A Wi-Fi kiépítésénél többféle biztonsági funkciót iktatnak be, hogy a támadásokat kivédjék. A rogue AP támadások ezekben a WLAN hálózatokban hoznak létre engedély nélkül biztonsági réseket vagy puha hozzáférési pontot, és a Wi-Fi teljesítményét csökkenthetik is. [37] Több megoldási kivitelezése lehet, melyeknél a fizikai ott létnek nem minden esetben kell már teljesülnie. Legegyszerűbben az aircrack-ng program tesztelésével mutatható be a vezeték nélküli hálózat AP kihasználhatósága. Ez egy wireless-es auditing tool, mely nem csak tesztelésre használható, hanem akár a hálózat feltörésére is és teljesen egyszerűen letölthető a netről. Windows operációs rendszerre telepíteni sem kell, mivel egy .zip fájl töltődik le és azt kell kicsomagolni. Az Airdump.ng-vel meghatározhatók a hálózatok információi (mint például a BSSID, és a Wi-Fi router MAC címe) és a felcsatlakozott klienseké is, a jelerősséggel, az elveszett csomagok számával, csak néhányat kiemelve. A jelerősség azért élvez kiemelt fontosságot, mert az okos eszközök a legerősebb jel keresésre vannak beprogramozva, így, ha a támadó erősebb jelet tud kibocsátani, mint a meglévő hálózat, amellyel kommunikál, akkor a felhasználó miután deautentikálták az alaprendszerből a támadó eszközére fog felcsatlakozni. Mivel az átmenő adatforgalom a résnek köszönhetően lehallgatható, a kliens és a szerver közti hitelesítési adatok, titkosítási kulcsok egy az egyben megszerezhetők. E rétegek után lehetőség van az Airplay-ng-vel a kliens és az AP közötti kapcsolat megszakítására. Ez egyfajta szolgáltatásmegtagadás, a Wi-Fi deauthentication, azaz hitelesítési támadás. A klienseket mivel a szerver már nem hitelesítettnek érzékeli, lecsatlakoztatja a hálózatról, így rákényszeríti a program a felhasználó eszközét, hogy a nem megfelelő csatlakozási pontot használja.

A rogue AP-ok elkerülése érdekében vezeték nélküli behatolás-megelőző rendszereket telepítenek, amelyek figyelik a nem ismert, jogosulatlan rádiófrekvenciákat. A rogue pontot a felhasználó maga is létrehozhatja abban az esetben, ha meg kívánja osztani a számítógépes vezetékes hálózati hozzáférését vezeték nélküli ügyfelekkel. Gyakori hiba, hogy a routert, amelynek a feladata, hogy a különböző vezetékes hálózatokat összekapcsolja, kiterjessze és a közöttük lezajló adatforgalmat lebonyolítsa, nem titkosítják le, nem építenek bele védelmi eszközöket, így a védett rendszerhez szinte zöld utat ad a felhasználó annak, aki jogosulatlanul szeretne hozzáférni. Ennek elkerülése a forgalommonitorozásban rejlik, mint például a rogue AP detection. Ez a kereső azonosítja a biztonságos hálózathoz csatlakozni kívánt nem engedélyezett eszközt, személyt, és elszigeteli. Ez a technika nem ütközik jogi problémákba, azonban az elhatárolása már felvet különböző jogi aggályokat. A vezeték nélküli környezetbe belépő ilyen jellegű támadások felfedezése költséges lehet, és külön figyelmet kell rá fordítani. A rogue AP detection megszünteti a szolgáltatást és „hallgatja” a jeleket, többféle megoldása létezik a megfigyelésre, egyik, hogy automatikusan vizsgálja csatornákat például 50 msként vagy kézi vezérléssel. Ezután azonosítja, hogy mely Access Point-ok rogue-ak és melyek érvényesek és része a hálózatnak. A vezérlőnek küldi el a következő összegyűjtött adatokat; a jogosulatlan felhasználó csatlakozó pontjának MAC címét, a jogosulatlan felhasználó csatlakozó pontjának a nevét, a jogosulatlan felhasználó csatlakoztatott kliensek (ami a számítógép, vagy azon futó program, mely hozzáfér a hálózathoz) MAC címét. Továbbá milyen vezeték nélküli rendszerhez kapcsolt protokollal rendelkezik az eszköz (WEP, WPA, WPA2), preamblet, amely a kezdeti szinkronizációra használt 64 bit, a jel-zaj viszonyt (signal- to-noise ratio), mely a hasznos és zavaró jel arányát fejezi ki dB-ben kifejezve, illetve a vevő-jelerősség

mutatót (RSSI). Egy riasztást generál, amely a hálózati rendszergazdához fut be. Tehát hiába ismeri fel a rendszer a behatolót, előbukkan az emberi tényező, hogy foglalkozik-e vele és milyen lépéseket tesz ez ellen, ha egyáltalán a rogue AP detectiont alkalmazzák a hálózaton. [38] Ez a gyakorlatban úgy képzelhető el, hogy egy meglévő vezetékes hálózathoz tartozik egy vezeték nélküli rendszer, mint például egyetemeknél. Fizikálisan a vezetékes végpontnál létre lehet hozni Wi-Fi magán hálózatot, melynek az SSID-je ugyanolyan nevű lesz, mint az adott, már meglévő vezeték nélküli hálózaté. Amennyiben nem érzékeli, nem készít log elemzést a Wi-Fi rendszerről, illetve monitorozás nem történik az incidensről, az idők végezetéig ki lehet használni ezt a rést, s a privát hálózaton keresztül átmenő teljes adatforgalom ellenőrizhető és irányítható.

AJÁNLÁSOK

- A VPN, virtuális magánhálózatok, használata mindig erősen ajánlott, mert ezzel a kiépített hálózattal az eredeti hálózaton keresztülmenő adatforgalom nem látható, mivel titkosítva van. Ez a megoldás nem csak titkosításra ad lehetőséget, hanem adatfolyamok elkülönítésére is. [39]
- Javasolt adatvédelmi beállításként a MAC-cím (hálózati kártya számsorozata, amely a hálózat azonosítására szolgál) szűrést érdemes használni, így csak azok a gépek tudnak csatlakozni a hálózathoz, amelyek a MAC címük alapján engedélyezve vannak. Távoli hozzáférést magánszemélyeknél kellően fontos megváltoztatni tiltás módra, ez alól kivétel, ha olyan a munkahely, ahonnan összeköttetést kell a céges és a magángépek között létrehozni. Előbb említett lehetőség a Windows 7,8 és a 8.1-es verzióján alapbeállítás volt. A távoli hozzáférés tiltását akár mobileszközről is véghez lehet vinni, ezért kell fontolóra venni, hogy szabad megváltoztathatóságot meghagyják-e a drótnélküli adminisztrációnak. Ezáltal csak az tud változtatni a router beállításain, aki közvetlenül csatlakozik hozzá. [40]
- Megfelelő biztonsági intézkedések a különböző vezeték nélküli eszközök világában (1. számú táblázat)

	Titkosítás	**Hitelesítés**	**VPN**	**Zárolás és távoli hozzáférés**	**Hozzáférés szabályozás**
Viselhető intelligens eszközök (szemüveg, okos órák)	X	X			
Otthoni okos eszközök (riasztó rendszer)	X		X		
Applikációk	X				X
Felhő alapú eszközvezérlés (okostelefon, tablet)				X	

[41]

1. számú táblázat: Megfelelő biztonsági intézkedések a különböző vezeték nélküli eszközök világában, (saját szerkesztés)

- Hotspoton keresztül történő adatforgalomra érdemes a client isolation biztonsági funkciót használni. Ez megakadályozza a vezeték nélküli ügyfelek kommunikálást egymással. [42]

KÖVETKEZTETÉSEK

Az információs és kommunikációs technológiák komplexen érintenek mindenkit és a terjedő wireless-es technológiák új típusú biztonsági felkészültséget kívánnak, mely hiányzik a felhasználók oldaláról is. A kiberbűnözés célpontjainak jelentős részét az egyének adják, mint például a hallgatók. Ez a korosztály legtöbbet pubokban, gyorséttermekben, publikus nyílt Wi-Fi hálózattal rendelkező helyeken, hotspotok mentén fordulnak meg és csatlakoznak fel a Wi-Fi-re. A felhasználók legtöbbször nincsenek tisztában azzal, hogy milyen hálózatra lépnek fel. A hipotézisem, hogy a felhasználok a Wi-Fi hálózatokon keresztül történő adatforgalombiztonsága ismereteinek hiányával küzdenek, ami valós probléma. Az általam vizsgált két pont, a WPA2 hiányossága és a Rogue AP-ok, a kliensek által igen nehezen észrevehető veszélyforrások, ezért fontos ismerniük. A problémák legtöbbször három esetben jelentkeznek, amikor nincs teljes lefedettségű Wi-Fi hálózat, illetve a jelerősség nem megfelelő, és ezt használja ki a támadó, egy erősebb jelerősségű eszközzel, vagy a hálózaton nincsen detektálás, illetve, ha van detektálás, azonban emberi mulasztás miatt nem valósul meg a védelem. A Rogue AP-ok engedély nélküli biztonsági rések, ahol a felcsatlakozott eszközök adataihoz könnyen hozzá lehet férni, majd a kapcsolatot a kliens és a szerver között a támadó megszakítja (Wi-Fi deauthentication), majd a felhasználó eszközét kényszeríti a csaló hozzáférési ponthoz való csatlakozásra. Ez ellen a szervezet és az egyén is védekezhet. A szervezet felől az úgynevezett Rogue AP detection, behatolás-megelőző rendszerrel lehet kiváló védelmet biztosítani, avagy hozzáférés szabályozást alkalmazni, amellyel a nem rendszergazdai szintű hozzáférők nem oszthatják meg a hálózatot külső személlyel, eszközzel. Privát oldalról a többfaktoros hitelesítést és titkosítást sem szabad figyelmen kívül hagyni. Bármilyen hálózat használat esetén a VPN hálózat használata, MAC szűrés, avagy client isolation technikák jó megoldások lehetnek bárki számára, azonban, hogy figyelmet fordítson a felhasználó adatai biztonságba helyezésére, ahhoz először meg kell győzni, hogy fontos adatok birtokában van, és védeni kell ezeket.

FELHASZNÁLT IRODALOM

[1] WANT, R.- DUSTDAR, S.: *Activating the internet of things [guest editors'introduction*],” Computer, vol. 48, no. 9, pp. 16–20, 2015.

[2] KOSKA Melinda: Wi-Fi hálózatok biztonsági kockázata, NKE, 2018

[3] International Telecommunication Union: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, (letöltve: 2018.02.20)

[4] KIFÜ: Közérthetően az IT biztonságról http://kifu.gov.hu/sites/default/files/IT_brosura_v7.pdf, 7, (letöltve: 2018.02.20.)

[5] Origo: Bírság járhat a nyitott wifiért Németországban. http://www.origo.hu/techbazis/internet/20100514-birsag-jarhat-a-nyitott-wifiert-nemetorszagban.html, (letöltve: 2018.02.20.)

[6] GUBBI, J. et.al*: Internet of things (iot): A vision, architectural elements, and future directions*, Future Generation Computer Systems, vol. 29, no. 7. 1645–1660, 2013.

[7] ALKAR, A.- BUHUR, U.: *An Internet based wireless home automation system for multifunctional devices*, IEEE Transactions on Consumer Electronics 51 1169–1174, 2005.

[8] DARIANIAN, M.- MICHAEL, M.P.: *Smart home mobile RFID-based Internet-ofThings systems and services*, in: 2008 International Conference on Advanced Computer Theory and Engineering, 2008, 116–120.

[9] AIREHROUR, D. et. al.: S*ecure routing for internet of things: A survey*, Journal of Network and Computer Applications, vol. 66, 198–213, 2016

[10] EMMERSON B.: *M2M: the Internet of 50 billion devices*, Huawei Win-Win Magazine Journal (4) (2010) 19–22.

[11] MIORANDI, D. et. al.: *Internet of things: Vision, applications and research* challenges, Ad Hoc Networks, vol. 10, no. 7,1497–1516, 2012.

[12] DA XU, L.: *Enterprise systems: state-of-the-art and future trends*, IEEE Transactions on Industrial Informatics, vol. 7, no. 4, 630–640, 2011.

[13] PANG, Z. et.al.: *Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things*, in Advanced Communication Technology (ICACT), 2013 15th International Conference on. IEEE, 2013, 529– 534.

[14] MISRA, S. et. al.: Security challenges and approaches in internet of things,2016

[15] DOMINGO, M. C.: *An overview of the internet of things for people with disabilities*, Journal of Network and Computer Applications, vol. 35, no. 2, 584–596, 2012.

[16] ZHOU, H. et. al.: *Design and research of urban intelligent transportation system based on the internet of things*, in Internet of Things. Springer, 2012, 572–580.

[17] Google-fiók Súgó: https://support.google.com/accounts/answer/1733224?hl=hu, (letöltve: 2018.02.20.)

[18] ASHTON, K.: *That ''Internet of Things'' thing*, RFiD Journal, 2009.

[19] ABC News: Amazon says it's working to fix Alexa's laughing problem http://abcnews.go.com/GMA/News/amazon-working-fix-alexas-laughing-problem/story?id=53594464, (letöltve: 2018. 04. 10.)

[20] Wi-Fi Alliance: https://www.wi-fi.org/who-we-are, (letöltve: 2018.03.30.)

[21] ILLÉSI Zsolt: *Wifi hálózatok igazságügyi szakértői elemzése: Wifi hálózatok felderítése*. In Hadmérnök, 2009. szeptember 3. http://hadmernok.hu/2009_3_illesi.pdf, (letöltve: 2018. 03.15.)

[22] SADOSKI, D.: *Client/Server Software Architectures – An Overview*, Software Technology Roadmap, 1997-08-02.

[23] JUNIPER Networks: Tech Library https://www.juniper.net/documentation/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-ssid-bssid-essid.html#jd0e46, (letöltve: 2018.03.30.)

[24] SZABÓ Bálint- MÁRFÖLDI Endre: *Számítógépes hálózatok*. http://www.tankonyvtar.hu/hu/tartalom/tamop425/0005_24_szamitogepes_halozatok_scorm_03/333_az_osi_modell.html, (letöltve: 2018.03.30.)

[25] HupWiki: Információs háttértár https://wiki.hup.hu/index.php/Datagram-orient%C3%A1lt_kommunik%C3%A1ci%C3%B3s_protokoll

[26] HupWiki: Információs háttértár https://wiki.hup.hu/index.php/ICMP, (letöltve: 2018.03.30.)

[27] HupWiki: Információs háttértár https://wiki.hup.hu/index.php/TCP, (letöltve: 2018.03.30.)

[28] HupWiki: Információs háttértár
https://wiki.hup.hu/index.php/IMAP,(letöltve: 2018.03.30.)

[29] HupWiki: Információs háttértár
https://wiki.hup.hu/index.php/POP3,(letöltve: 2018.03.30.)

[30] HupWiki: Információs háttértár
https://wiki.hup.hu/index.php/SMTP, (letöltve: 2018.03.30.)

[31] VANHOEF, M.- PIESSENS, F.: *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2*. In Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS). ACM 2017

[32] PC WORLD: *Így törhető fel bármelyik titkosítás*
https://pcworld.hu/szoftver/igy-torheto-fel-barmelyik-titkositas-138341.html, (letöltve: 2018.03.30.)

[33] HEGYESHALMI Richárd: *Óriási gond van a wifi biztonsággal*
https://index.hu/tech/2017/10/16/oriasi_gond_van_a_wifi_biztonsagaval/, (letöltve: 2018.03.30.)

[34] BBC News: *Wi-fi security flaw 'puts device at risk of hacks'*
http://www.bbc.com/news/technology-41635516, (letöltve: 2018.03.30.)

[35] CERT Software Engineering Institue: *Vendor Information for VU#228519*
https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4, (letöltve: 2018.03.30.)

[36] Gdata: *Biztonságosabb lesz a vezeték nélküli internet*
https://virusirto.hu/blogbejegyzesek/2018/01/12/biztonsagosabb-lesz-a-vezetek-nelkuli-internet/, (letöltve: 2018.03.30.)

[37] MARECO, D.: Rogue AP Detection: What Is It & Why Your WLAN Design Needs It
https://www.securedgenetworks.com/blog/rogue-ap-detection-what-is-it-why-your-wlan-design-needs-it, (letöltve: 2018.02.20.)

[38] CISCO: Rogue Detection under Unified Wireless Networks
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70987-rogue-detect.html, (letöltve: 2018.02.20.)

[39] SZIGETVÁRI Zoltán: *A VPN-ről*
https://www.itkommando.hu/site/a-vpn-rol/ (letöltve: 2018.03.30.)

[40] GData: *Hogyan védjük meg a wifi hálózatunkat?*
https://virusirto.hu/blogbejegyzesek/2015/04/26/hogyan-vedjuk-meg-a-wifi-halozatunkat/ (letöltve: 2018.03.30.)

[41] CTIA: *The Wireless Association*. Mobile Cybersecurity and the Internet of Things Empowering M2M Communication. (2014, December 2, 2014).
http://www.ctia.org/docs/default-source/default-document-library/ctia-iot-white-paper.pdf (letöltve: 2018.03.30.)

[42] CISCO: *Wireless Client Isolation*
https://documentation.meraki.com/MR/Firewall_and_Traffic_Shaping/Wireless_Client_Isolation (letöltve: 2018.04.15.)