HADMÉRNÖK

KATONAI MŰSZAKI TUDOMÁNYOK ONLINE

VIII. Évfolyam 1. szám 2013. március

NKE
BUDAPEST

A szerkesztőbizottság elnöke:
Prof. Em. Halász László ny. ezredes, DSc

A szerkesztőbizottság elnökhelyettese:
Prof. Dr. Munk Sándor ny. ezredes, DSc

A szerkesztőbizottság tagjai és egyben rovatvezetők:
Dr. Berek Tamás okl. mk. őrnagy, PhD (Biztonságtechnika)
Dr. Eleki Zoltán, PhD (Fizikai felkészítés)
Prof. Dr. Haig Zsolt mk. ezredes, PhD (Védelmi elektronika, informatika és kommunikáció)
Dr. habil. Horváth László ny. alezredes, PhD (Védelmi igazgatás)
Dr. Jászay Béla ny. ezredes, PhD (Védelemgazdaság)
Dr. Jászay Béla ny. ezredes, PhD (Védelemgazdaság)
Prof. Dr. Lukács László ny. mk. alezredes, Csc (Katonai műszaki infrastruktúra)
Dr. habil. Horváth Attila alezredes, CSc (Katonai logisztika és közlekedés)
Prof. Dr. Turcsányi Károly ny. ezredes, DSc (Haditechnika)
Dr. Földi László okl. mk. alezredes, PhD (Környezetbiztonság, ABV-és katasztrófavédelem)

Főszerkesztő: Dr. Farkas Tibor főhadnagy, PhD

Szerkesztő: Serege Gábor mk. főhadnagy

A szerkesztőség elérhetősége:
Nemzeti Közszolgálati Egyetem,
1101. Budapest, Hungária krt. 9-11. A. épület 8. emelet
Postacím: 1581. Budapest Pf.:15.
Telefon: +36-1-432-9000 /29-289/ *Fax:* +36-1-432-9025 *HM:* 29-289
e-mail: hadmernok@uni-nke.hu web: http://hadmernok.hu

Kiadó: Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
ISSN 1788-1919

Jelen számban megjelent írások szerzői:

Antal Örs – NFM;
Árvai László – Tiszacash Zrt.**;**
Baráth Artúr – Dunaújvárosi Főiskola;
Dr. Berek Tamás okl. mk. őrnagy – NKE HHK egyetemi docens;
Berki Gábor – NKE KMDI doktorandusz;
Dr. Dobák Imre – NKE Nemzetbiztonsági Intézet;
Dr. Fleiner Rita – Óbudai Egyetem NIK SZTI;
Gulyás Attila – MH ÖHP**;**
Gyarmati József – NKE HHK egyetemi docens;
Háber Péter ny. ezredes;
Dr. Hornyacsek Júlia őrnagy - NKE HHK egyetemi docens**;**
Horváth Attila őrnagy – MH BHD;
Horváth József;
Jéri Tamás bv. alezredes – Kalocsai Fegyház és Börtön;
Dr. Kassai Károly mk. ezredes – HM Informatikai és Információvédelmi Főosztály;
Dr. Kolonics Gábor o. őrnagy;
Dr. Komjáthy László ny. tű. alezredes - NKE KVI adjunktus;
Kondás Katalin - Büntetés-végrehajtás Országos Parancsnoksága;
Kovács Róbert;
Kovács Zoltán;
Kozák Attila – Nyíregyháza Katasztrófavédelmi Kirendeltség;
Dr. Kóródi Gyula ny. o. alezredes
Miskey Tamás tű. alezredes – Veszprém Megyei Katasztrófavédelmi Igazgatóság;
Molnár Zsolt – Óbudai Egyetem;
Prof. Dr. Munk Sándor ny. ezredes – NKE HHK egyetemi tanár;
Nagyné dr. Takács Veronika – NKE KMDI doktorandusz;
Dr. Németh András okl. mk. százados – NKE HHK egyetemi docens;
Nikodém Edit;
Péri Márton - Pázmány Péter Katolikus Egyetem ITK;
Prisznyák Szabolcs – NKE HHK HDI doktorandusz;
Rácz László István - Közigazgatási és Igazságügyi Minisztérium;
Szabó Tibor;
Szentgáli Gergely – Budapest Corvinus Egyetem;
Takács Zoltán; Teknős László – NKE HHK KMDI doktorandusz;
Tiszolczi Balázs Gergely – Magyar Államkincstár

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Berek Tamás - Takács Zoltán
berek.tamas@uni-nke.hu - taki.zoli@freemail.hu

RFID TECHNOLÓGIA ALTERNATÍV FELHASZNALÁSI LEHETŐSÉGEI A KÓRHÁZBIZTONSÁG TERÜLETÉN

Absztrakt

A vagyonvédelmi koncepció kialakítását követően a komplex biztonsági rendszer tervezésekor komoly elemző és értékelő munkát követel meg a védelmi alrendszerek helyes arányainak kialakítása. A kórházbiztonság egy speciális objektumvédelem, melyet az ott dolgozók, az ott kezeltek, és az oda látogatók tesznek speciálissá az összetett feladatok miatt. Az objektumvédelem szakterületei közül a szerzők a kórház létesítmények megvalósítható beléptető és mozgáskövető alrendszereivel foglalkoznak, melyek épületirányítási rendszerbe integráltan üzemeltethetők az RFID[1] technológia által biztosított lehetőségek kihasználásával.

In order to configurate a safeguarding conception, we have to create a complex security system. We have to make a plan, the plan has to be analised and interpreted. We have to configurate the right propotion of the defend systems.
The hospital security is special area of the facility security because of the personnel, the patients and visitors, which are located in the facility. The authors deal with acces control-, and tracking systems, which may integrated into the facility management system with opportunities provided by RFID technologie

***Kulcsszavak**: komplex biztonsági rendszer, beléptető rendszer, RFID technológia ~ complex security system, access control system, RFID technologie*

1 RFID (Radio Frequency Identification)

Egészségügyi létesítmények védelmének előkészítése és tervezése, valamint az ezzel összefüggő feladatok végrehajtása néhány terület tekintetében meghatározó sajátossággal bír. Az egyik és talán a legfontosabb az, hogy akár szakrendelőről, akár kórházlétesítményről beszélünk, számításba kell venni, hogy az objektumba látogatók köre igen széles és az objektumon belüli tevékenység, a dolgozók, a betegek és a kapcsolódó tárgyak eszközök védelmét úgy kell biztosítani, hogy az objektumba történő szabad be és kilépés általános elvek szerinti korlátozása nem megoldható.

A Vagyonvédelmi Nagykönyv meghatározását alapul véve az objektum egy pontosan körülhatárolható terület, melyen felépítmények találhatóak különböző funkciókkal. A veszélyeztetettség mértékét a működés, az üzemeltetés biztonsági foka, a felhasznált különféle anyagok, technikai eszközök, információk kereslete, értéke, értékesíthetősége, a terület bűnügyi fertőzöttsége, működés rendje a napszak, az alkalmazott védelmi rendszer megbízhatósága, a beavatkozás, az elhárítás objektív- szubjektív gyorsasága, a nemkívánatos cselekmények jellege és azok területi kihatása határozza meg. [1] Nincs ez másként az egészségügyi betegellátó létesítmények esetében sem, azok védelme összetett feladat.

Részletesen tárgyalva a témát a védelem tárgyaként történő felosztást alkalmazva annak számos elemét lehetne meghatározni és elemezni, mi azonban jelen írásunkban a létesítmény területén zajló tevékenységre, valamint annak kereteként kezelt intézmény rendjének biztonságára koncentrálva azok védelmének technikai támogatását nagy hatékonysággal biztosítani képes RFID technológia alkalmazási lehetőségire kívánjuk felhívni a figyelmet.

Az RFID rendszer telepítésének jellemzői között említhető, hogy megfelelően kialakított informatikai háttérrel kell, hogy rendelkezzen, amely akár a kiépítés folyamán, akár később moduláris rendszerben is kialakítható. A rendszer kiépítéséhez szükség van RFID író – olvasó berendezésre, amely a kártyákra az adatok felviszi, illetve azokat használat után letörli avagy átírja. Ehhez javasolt olyan író – olvasó alkalmazása, amely támogatja proximty illetve classic kártyatípusok használatát. Ilyen eszközökre nem csupán a recepciókon, hanem minden osztályon szükség van, hiszen ha a beteget további vizsgálatokra küldik, abban az esetben a kártyákon tárolt adatokat le kell törölni, és felül kell írni az új információkkal. Az író eszköz a RS485 (v. RS232) portokon keresztül az új információt közli a központi informatikai rendszerrel.

Olyan szoftvert kell kiválasztani, illetve kifejleszteni, amelyben az információ az informatikai rendszer hordozza, nem pedig a kártya. Ilyenkor az adatok a rendszerben vannak eltárolva, és az adatokhoz lesz hozzárendelve egy kód, amit maga a kártya hordoz. Az adatok felvitele után a kártyát az olvasó eszközhöz közelítve az adatokhoz a rendszer társítja a kártyát. Lehetséges a kártyára is írni az adatokat, azonban az elvesztési veszély miatt az adatok arra nem jogosultak kezébe kerülhetnek, ha azt sikerül az intézmény területéről kijuttatni.

A rendszer működtetése a RFID antennákkal, aktív és passzív kártyákkal (a betegek, látogatók részére passzív, míg a dolgozók részére aktív), megfelelően kialakított informatikai rendszerrel, illetve kapurendszerekkel történik.

A BETEGEK BIZTONSÁGA

Akkor, amikor a betegek biztonságáról beszélünk, elsődlegesen a közelmúltban sajtónyilvánosságot kapott kórházi lopások és látogatók által elkövetett garázda cselekmények jutnak eszünkbe. Látszatra lehet, hogy egyszerű megoldást találni: mind a mentőbejáratokon, mind, pedig a személybejáratoknál létesített ellenőrző áteresztő pontok a recepciósok hatékony együttműködésével lehetővé teszi az intézet területére történő szabályozott beléptetést.

Természetesen a beléptető pontok telepítése és az azokon történő követhető belépések nagymértékben csökkenthetik az illetéktelen behatolásokat, növelve ezáltal a betegek, valamint a szakdolgozók értékeinek védelmét, a betegbiztonság azonban többet jelent a betegek fizikai védelmének biztosításánál.

A Magyar Egészségügyi Eljárás Standardok kézikönyv – az egészségügyi szolgáltatás minőségértékelésére szolgáló specifikus követelmények gyűjteménye - kinyilvánítja, hogy az egészségügyi szolgáltatónak eljárást kell kidolgoznia és alkalmaznia a betegek értékeinek, személyes tárgyainak védelmében, azok ellopásának megakadályozására. Különösen fontos ez a betegek azon csoportjainál, akik helyzetüknél fogva kiszolgáltatottak – a sürgősségi ellátásban részesülő, és a döntésképtelen betegek esetében.

A betegek betegellátó osztályon történő elhelyezése során a beteg személyes tárgyain kívül ruhájának tárolásáról és őrzéséről is gondoskodni szükséges. Mindezt biztosíthatja egy olyan szekrényrendszer, melyet a beteg a számára kiadott RFID tag, vagy kártya nyit-zár.

A beteg részére kiállított RFID kártya alkalmazásával nem csak a beléptetés szabályozható, az illetéktelen forgalom redukálása mellett – amely magában hordozza a vagyon elleni bűncselekmények elkövetésének veszélyét is – a beteg regisztrációjára és betegirányításra is alkalmas. Mindezt lehetővé teszi az RF antennaegységek folyosókra történő telepítése és a vevőegységek duplikálása, amivel nem csupán az áthaladást, hanem az áthaladás irányát is lehet észlelni. Amennyiben a kártya hordozója helytelen irányba halad, akkor a vevőhöz történő közelítés esetén fény- vagy hangjelzéssel közli, hogy téves az irány.

A recepciókon kapott belépőkártyákkal, valamint a folyosókra telepített RFID olvasókkal közösen egy olyan rendszer kialakítása, amely a recepción beprogramozott adatok alapján egy térkép nélküli eligazodást tesz lehetővé az épületen belül kényelmi funkcióval is szolgálhat. Sőt ez a kártya, mint egy érkezési sorrendet is jelölő eszköz a várótermekben vitás érkezési sorrendek helyett egy teljesen egyértelmű sorrendet állíthat fel.

A kijelölt zónát elhagyva jelzi a kártya viselőjének a helyes irányt, illetve a kapukba beépített fény- és hangjelző rendszereken keresztül üzenetet küldhet a viselőnek, az irány meg nem változtatása, esetén riasztást személyzetnek. Az intézet elhagyása folyamán a kártya a recepción leadható, és korlátlan esetben újraírható.

A másik jellemző probléma, a besurranó tolvajok által elkövetett lopások visszaszorítása érdekében is hatékony lehet a megfelelően kiépített rendszer alkalmazásba vétele.

A beléptető pontokat a vészhelyzet irányító központon keresztül rendszerbe kötve megkapjuk a mozgáskövető rendszert, melynek az előnye a már ismert mozgáskövető rendszerekkel szemben az, hogy nem mozgáskövető kamerákkal történik a mozgások ellenőrzése, hanem annál jóval tágabb szabadságot biztosító áteresztő kapukon keresztül. Gyakorlatilag a mozgáskövető rendszer a kapukon való áthaladást regisztrálja annak irányával együtt, így a tartózkodási szekció megállapítható, illetve az épületben való tartózkodás.

A szándékoltan, vagy tévedésből „elkóborolt” látogatók esetében egy bizonyos idő elteltével a helytelen irányba folytatott haladás jelzéssel párosul a személyzet részére, tudatva az illetéktelen belépést. Ebben az esetben a személyzet érdeklődhet a belépő szándékáról, és szükség szerint intézkedhet. Útbaigazít vagy kivezettet. Minden ilyen rendszer kiegészítéseként IR vagy lézersorompót kell telepíteni, hiszen az RF vevőantennák csak a kártyával közlekedők mozgását érzékeli. E kiegészítésre azért van szükség, mert a kártyát szándékosan vagy esetleg vétlenül elhagyva ellenőrizetlenül lehet az intézeten belül mozogni. Abban az esetben, ha kártya nélküli mozgást észlel a rendszer, abban az esetben szintén riasztja a személyzetet.

Minden címke külön – külön jogosultsággal látható el, tehát akinek az állapota azt megengedi, az az intézeten belüli jogosultsággal látható el, tehát figyelmeztető jelzés csak akkor jelentkezik, ha a kezelt jogosulatlanul kívánja az intézményt elhagyni, illetve olyan területre kíván belépni, amely az előre definiált mozgási jogosultságába nem lett felvéve (pl.

betegektől elzárt területek). Ezzel a megoldással gyakorlatilag úgy oldható meg a mozgáskövetés, hogy a beteget nem követjük minden időpillanatban lépten-nyomon. A mozgási tevékenységét csak különleges – előre definiált – esetekben szükséges ellenőrizni, melyet megfelelő jogosultságokkal rendelkező személyek végezhetnek. Amennyiben az előre meghatározott helyen nem jelent meg adott időn belül a beteg, akkor lehet ellenőrizni, hogy legutoljára mely áteresztő ponton haladt át, és milyen irányba, tehát a vélt tartózkodási helyét lehet leszűkíteni. Rendkívüli esemény bekövetkezése esetén a törvényben meghatározott (vizsgáló) szervek a megfelelő törvényi felhatalmazás birtokában utólagosan kivizsgálhatják az ügyben érintett személyek mozgását, ha az esetleg a rendkívüli eseménnyel összefüggésbe hozható.

Az RFID-tag beteget érintő azon kényelmi funkciója, hogy a transzponder helyzete az intézményen belül behatárolható, a betegkövetés, betegirányítás rendszerét támogatja, de ezen túlmenően a beteg biztonságát is szolgálhatja azzal, hogy megfelelő rendszerbe telepített beléptető pontok a belépést megakadályozza olyan területeire az intézménynek, ahol a beteg közvetett felügyelete gyakorlatilag megszűnik (gépészeti, kiszolgálási stb. helyiségek). Ez még akkor is lényeges, amikor teljes cselekvőképessége birtokában lévő betegről beszélünk, tekintettel arra, hogy vannak olyan vizsgálatok, beavatkozások, melyeket követően a beteg összezavarodik, figyelme csökken. Olyan betegek esetében, akik cselekvőképességükben korlátozottak, ez a funkció a beteg védelme szempontjából kiemelt. Abban az esetben is, ha a részükre kijelölt területet elhagyják és másik, a betegek által látogatható területre térnek, akár egy másik osztályra, az egészségügyi szakszemélyzet jelzést kap, így későbbi felesleges keresésektől mentesülnek az alkalmazottak. Az ő esetükben nem attól kell tartani, hogy értéktárgyakat eltulajdonítanak, hanem arra kell ügyelni, hogy a részükre kijelölt osztályt felügyelet nélkül ne hagyják el. Az osztály felügyelet nélküli elhagyásával nemcsak a többi beteget vagy látogatót zavarhatják az estleges zavart magatartásukkal, hanem a különböző gyógyszerekhez, gyógyászati eszközökhöz vagy segédeszközökhöz esetlegesen hozzáférhetnek, ezekkel magukban vagy másokban akaratlanul kárt okozhatnak.

Egy másik általános biztonsági elvárás a betegek fizikai inzultusoktól történő védelme.

Különösen a magas kockázatú betegcsoportok, a gyermekek, a fizikailag vagy szellemileg korlátozottan cselekvőképes egyének, az idősek, és az eszméletlen betegek kiszolgáltatottak.[2]

Gyakran az egészségügyi létesítmény élőerős szolgálata önmagában nem képes biztosítani ezt, ezért a kitűzött célok elérése érdekében feltétlenül szükséges komplex szemlélettel megtervezni és felépíteni az objektumvédelmet az egészségügyi intézmény biztonságvédelmi programjának elkészítését követően. Annak elektronikus komponensébe integrált RFID alrendszer természetesen önmagában nem kulcsa a megoldásnak, de hatékonyan támogathatja a biztonsági komplexumot több, a következőkben ismertetett összetevőn keresztül.

Azokban az esetekben, amikor a beteg nem kommunikációképes, vagy szellemileg cselekvőképtelen, a betegellátás is nehézségekbe ütközik a beteg és orvos közötti együttműködés hiányában. A beteg ruházatába elrejthető, vagy más formában alkalmazott RFID-tag (fekvőbeteg ellátás), - amely a komfortérzetet nem befolyásolja, továbbá a személyiséghez fűződő jogokat nem sért – hatékonyan segítheti a szakvizsgálatok adminisztrációs fázisát is. A szakvizsgálatot végző orvos asszisztense RFID olvasó segítségével az összes elérhető klinikai adatot, illetve a beteg személyes adatait képes elérni.

1. ábra: Karkötőbe integrált transzponder a beléptetés kedvelt eszköze az alkalmai tartózkodású területeken

A dokumentációk standardizált formai és tartalmi megjelenése – ami a különböző egészségügyi szolgáltatások közötti ellátás folyamatának folytonosságát hivatott biztosítani, lehetővé teszi a beteg ellátással kapcsolatos adatainak tárolását. A betegek adatainak ilyen módon végzett lekérdezése valójában az adatokhoz hozzáférők körét is csökkenti, így megfelelő védelmi protokollokkal a beteg adatvédelmét is biztosítja.

A személyes adatok védelmét és az érintett személyiségi jogait – jogszabályok által szabályozott esetek kivételével - az adatkezeléshez fűződő más érdek nem sértheti, így az érintett személyes és egészségügyi adatait a gyógykezelésben részt vevő egészségügyi személyzeten kívül illetéktelenek nem ismerhetik meg [3]

A rendszerben meghatározott jogosultságokat az egészségügyi dolgozók RFID transzponderén is lehet rögzíteni, így az adatokat megismerők körének korlátozása, illetve azok azonosítása is megvalósítható.

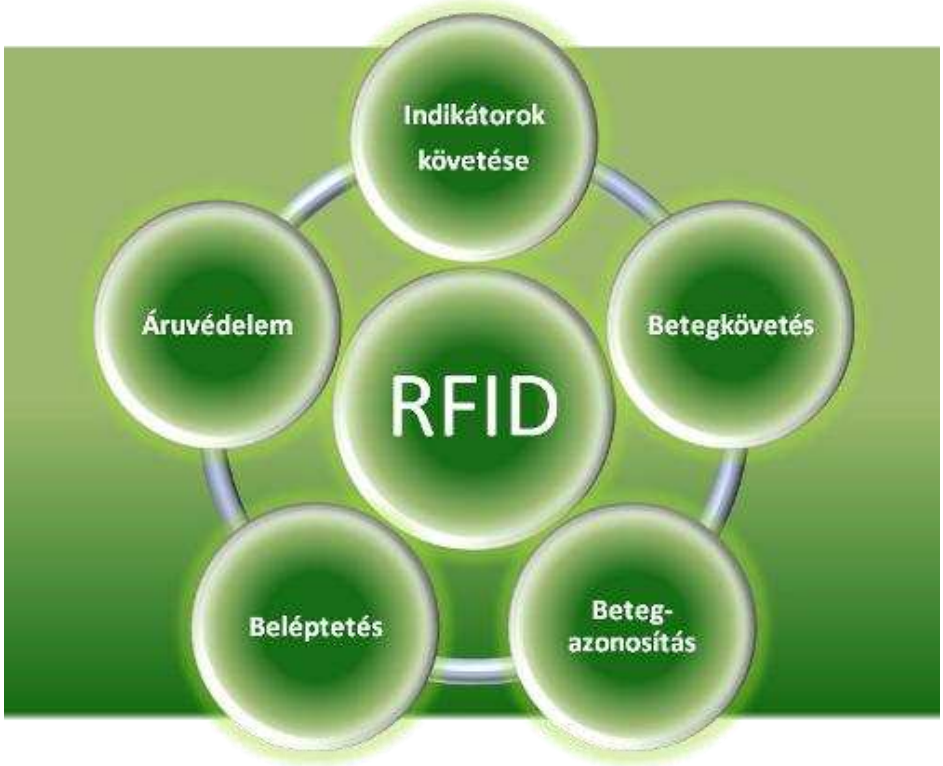
A betegazonosító rendszer működéséről szóló EüM irányelv (1/2005. EüK. 1.) által meghatározott kötelezően előírt beteg beazonosítást is nagymértékben megkönnyíti, és biztosabbá teheti az RFID technológia alkalmazása pl. diagnosztikai beavatkozás, műtét előtt, más szervezeti egységbe történő átadás-átvétel, továbbá, szállítás stb. esetén. Az elmúlt években nem egy esetben hallhattunk tévesen végrehajtott műtétekről, beavatkozásokról, a nem kellő körültekintéssel végzett betegazonosítás miatt.

A betegazonosítás más esetekben is létfontosságú, így a gyógyszeres kezelések alkalmával is. Minden beteg dokumentációjának tartalmaznia kell a számára rendelt gyógyszereket, a szedési gyakoriságot, dózist és időtartamot és természetesen a fekvőbeteg ellátásba részesülő beteget a gyógyszerbeadás előtt azonosítani kell, amit a beteg transzponderének leolvasása révén gyorsan biztosítható.

A megfelelő gyógyszerelés hordozhat magában egészségkárosító kockázatot gyógyszerérzékenység, illetve más anyagokkal történő interakciók tekintetében. A beteg számára korábban felírt gyógyszerhatóanyagok és dózisok is azonnal elérhetővé válnak az RF tag leolvasását követően, illetve az egyes korábban már előfordult gyógyszer-érzékenységi reakciók. Az is kiderülhet gyorsan, hogy a kezelésre javasolt gyógyszer hatóanyaggal korábban már más kezelőorvosnak nem sikerült komoly áttörést elérnie, így szintén idő takarítható meg, ami a gyógyulás mellett a betegellátás hatékonyságát is javítja.

Azt is jelzi a RF betegkövető rendszer, hogy a beteg, akihez látogatóba érkeznek az osztályon tartózkodik, azaz látogatható, vagy valamelyik diagnosztikai osztályon esetleg valamelyik műtőben. Amikor visszakerül az osztályra, a recepción az az információ jelenik meg hogy a beteg látogatható. A rendszer képes arra, hogy monitorozza a látogatási időben az adott osztályon jelen levő látogatók számát. A túlzott látogatóforgalom nem csak zavarja a többi beteget, hanem biztonsági kockázatot is jelent. Ha az engedélyezett látogatószámot

elérte a beteg, illetve az osztály akkor a látogató továbbhaladását ideiglenesen blokkolni lehet mindaddig, amíg a beteghez látogató ki nem lép az ellenőrző- áteresztő ponton, és a kártyáját le nem adja. Ezután a rendszer automatikusan szabad utat jelez az újonnan érkező látogatók számára.



2. ábra: RFID technológia felhasználási területei a kórházbiztonságban

AZ EGÉSZSÉGÜGYI ELLÁTÁSI FOLYAMAT BIZTONSÁGA

Az egészségügyi szektor kinyilvánítottan magas kockázatú terület melyet jól jellemez az érintett államigazgatási szervezet (EüM) egyik 2007-es kiadványában megjelentetett magyarázat: „a nem kívánatos események – melyek inkább a kezelés, mint a megbetegedés következményei- halálhoz vezethetnek, komoly károkat, komplikációt és a beteg szenvedését okozhatják.” [4]

A leggyakoribb ellátási hibák ugyanezen kiadvány hasábjain ismerhetők meg, melyek:

- Nozokomiális (kórházi) fertőzések
- Téves diagnózis, téves terápia
- Gyógyszerelési hiba
- Technikai hiba

Technikai hibákhoz sorolható károsodás pl.: a betegek cseréje, műtéti eszközök testben való bent felejtése komoly következményekkel járó probléma.

A fent hivatkozott kiadvány statisztikai adatokkal is szolgál a tárgyalt területet illetően. „A klinikai diagnózisok - a nemzetközi kórbonctani vizsgálatok szerint - az esetek 8,8-24,4%-ban tévesek. Gyógyszerelési hiba történhet a felírás és a gyógyszerbeadása során. Ez utóbbi kiküszöbölése a fekvőbeteg intézmények egyik legfontosabb, a betegek biztonságát szolgáló feladata.” [5]

A Magyar Egészségügyi Eljárás Standardok kézikönyv az egészségügyi ellátó intézmények tevékenységének felülvizsgálati szempontjait is tartalmazza, melyek között

szerepelteti, a gyógyszerelési hibák kellő időben történő jelentését, illetve a beteg ellátási folyamatának dokumentáltságát.

A betegfelvételkor, és az ellátás alatti egyedi azonosításnak, a beteg és a dokumentáció egyértelmű összerendelésének követelményére a betegek biztonsága tárgykörben már kitértünk, azonban ezen követelmények teljesülése a betegellátás biztonságát is szolgálja egyben.

A fekvőbeteg ellátásban betegdokumentációnak tartalmaznia kell többek között a személyazonosító adatokon kívül, az értesítendő személy elérhetőségét, a kórelőzményt, a diagnózist és a gyógykezelési tervet megalapozó vizsgálati eredmények, vizsgálatok elvégzésének időpontját, a betegség megnevezését, az elvégzett beavatkozások idejét és eredményét, a gyógyszer túl-érzékenységre vonatkozó adatokat valamint a bejegyzéseket tevők nevét és a bejegyzések időpontját. [6]

A gyógyszerek beadása tudást, gyakorlatot és tapasztalatot igényel. Az egészségügyi ellátó intézmény munkatársai között meghatározott képesítéssel rendelkezők azok, akik rendelkeznek a gyógyszerek beadásához szükséges kompetenciával, akiknek jogosultságát a belépőkártyájukon történő rögzítésével többek között a gyógyszerkészítményekhez történő hozzáférést lehet szabályozni és ellenőrizni az RFID technológia segítségével. A biztonságos gyógyszereléshez minimálisan előírt egyebek mellett a beteg azonosítása, továbbá a gyógyszer és annak dózisának valamint a beadás idejének és gyakoriságának egyeztetése a rendeléssel, melyet szintén lehetővé tesz a rendszer.

Az RF elérésű digitális betegdokumentáció nem csupán az egyes vizsgálatok, beavatkozások tényét és azok eredményeit, hanem a bejegyzést tevő személyét és a bejegyzés időpontját is képes tárolni. A betegellátás biztonságát fokozza az is, hogy a beteg kórelőzményeit, a beavatkozásokat és korábban felsorolt adatokat tartalmazó, a beteg valamennyi, az ellátási folyamat során keletkező dokumentációja az intézményben archiválásra kerül. Ez egyébként újfent felveti a betegjogi illetve a személyiséghez fűződő jogok biztosításának kérdését, a betegdokumentáció kezelése, tárolása során teljesülnie kell az adatkezelési, adatvédelmi előírásoknak. Az egyes adatkörökhöz való hozzáférési jogosultság pedig az egészségügyi személyzet proxy kártyájára írható.

A kórisme megállapításának, vagy akár a gyógykezelés hatékonysága értékelésének folyamatába integrált szakvizsgálatok elvégzése alkalmával vizsgálatot elvégző osztály által megkívánt minden lehetséges adat - amely a szakvizsgálat eredményességét támogatja- másodpercek alatt elérhetővé válik az adott vizsgálatot végző osztály asszisztense által üzemeltetett mobil RFID olvasó segítségével a rendszer megléte esetén. A szakorvos által közölt leletet a kórlaphoz kell csatolni, amely szintén gyorsan megtörténik azzal, hogy a beteg transzponderére áttöltik azt.

A betegség megállapítása, vagy a kezelés megítélése érdekében megtartott konzílium hatékonyságát fokozhatja, ha a tanácskozást lefolytató szakorvosok egyidejűleg le tudják olvasni és tanulmányozni tudják a beteg kórelőzményét, kezeléseit, gyógyszeres terápiája adatait, stb. Ugyanakkor az osztályos orvos ezzel kapcsolatos előkészítő munkáját is meggyorsítja a rendszer azzal hogy biztosítja, hogy a tanácskozáson a betegre vonatkozó minden kórelőzményi, vizsgálati, gyógykezelési adat a résztvevő orvosok rendelkezésére álljon. A tanácskozás eredménye is természetesen szintén a beteg transzponderére kerülhet.

A betegek elhelyezése során a MEES2 alapján a betegellátó osztályon a beteg ruháját és személyes tárgyait jegyzékbe kell venni, és gondoskodni kell azok tárolásáról és őrzéséről. Mindezek elvégzését végző egészségügyi szakdolgozó munkáját segíti egy olyan

[2] MEES: Magyar Egészségügyi Ellátási Standardok

szekrényrendszer, mely nyitását, zárását a beteg RFID tag segítségével önállóan tudja kezelni. Az osztályon elhelyezett betegre vonatkozó ápolási, élelmezési utasítást az osztályos orvos szintén rögzíteni tud a beteg RFID adathordozóján, amit a bármikor leolvashat. Az esetlegesen előforduló áthelyezés esetén a beteg kezelésének és állapotának adatait a korábbi kezelőorvos az új osztályos orvos számára a beteg átadásával át tud adni az összes többi okmánnyal együtt. Más intézménybe történő átvételnél szintén alkalmazható ez az eljárás.

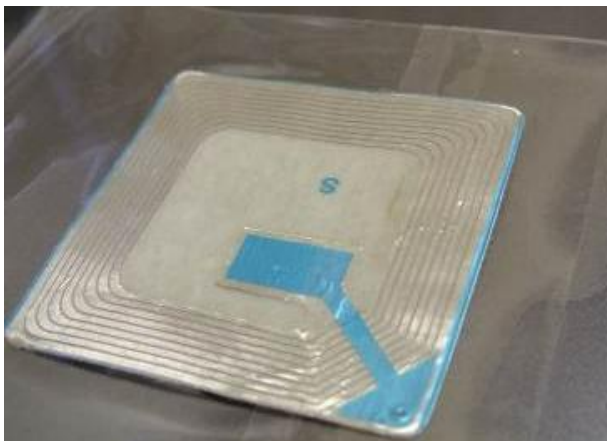
A betegellátási folyamat része tájékoztatás, ideértve a beteg hozzátartozójának tájékoztatása, ami általában személyesen történik, de nem kizárólagosan. Az egészségügyben a betegről szóló információkkal történő tájékoztatás körülményei is szabályozottak. A beteg hozzátartozóinak tájékoztatása az esetek egy részében lehetséges telefonon keresztül is, azt, azonban, hogy az osztály orvosai közül ki milyen mértékben és mikor adhat tájékoztatást a beteg állapotáról egy kidolgozott analógiával rögzíthető, a telefonon tájékoztatást adó személy a számára megadott jogosultsági szintnek megfelelően jut hozzá a beteg adataihoz.

A műtéti beavatkozások színtere, a műtőhelység egy speciális területe az egészségügyi objektumnak. Egyrészt természetesen az ott végzett tevékenység jellege, másrészt a berendezések és felszerelések, amelyek indokolják azt, hogy az ellátási biztonság aspektusából néhány gondolatot megjegyezzünk ezzel kapcsolatban.

A műtőrészlegben a szabályoknak megfelelően rendszerint csak azok az egészségügyi dolgozók tartózkodhatnak, akiknek állandó szolgálati helye a műtőrészleg, vagy esetenként oda beosztottak. A kijelölt személyeken kívül mind a beteg, mind pedig az ellátás biztonsága megköveteli, hogy az oda történő belépés szabályozott legyen. A belépési jogosultság ellenőrzésével, a műtő beléptető kapuja jelzi (nem akadályozza) és rögzíti az jogosulatlan belépést, illetve a bent tartózkodó személyek adatait (név). A beléptető terminálok ugyanis az alapfunkciójukon túlmenően számosbiztonsági, információs és nyilvántartási funkcióval rendelkezhetnek. A kártyák, vagy tag-ek installálásakor a dolgozó minden szükséges adatát meg lehet adni, akár a vércsoportot is, így számítógépen folyamatosan figyelemmel kísérhetőek a beléptető rendszer által felügyelt területen történő mozgások és egyéb felügyelt események. Idő és dátum mentése minden eseményhez, így mindig másodperc pontosan lekérdezhető minden információ, kártyánként, ajtónként, kártyaolvasónként is.

3. ábra:32 mm-es transzponder felhasználásra készen

A műtőhelyiségben csak műtős öltözetben (köpeny, sapka, maszk, lábbeli, stb.) szabad tartózkodni, ugyanakkor távozáskor a műtősrészlegből a műtős ruházatot kivinni nem szabad melynek ellenőrzésére szintén a fenti ruhadarabokba ágyazott RFID tag jelét érzékelheti a műtő beléptető kapu olvasója, jelzést adva. A műtétet követően a beteg ébredőbe való felvétele és az innen való elbocsátás ideje is dokumentált a belépési ponton történő áthaladással.



4. ábra: Beágyazható papírvékony transzponder

A műtéti beavatkozás előtt és után is szükség van bizonyos szakvizsgálatok elvégzésére. A betegellátó osztályok és a diagnosztikai osztályok közötti együttműködés RFID alapú betegkövetés támogatásával a diagnosztikai rendelők egyenletes terhelését segítheti elő azzal, hogy az egyes rendelők aktuális leterheltségét monitorozva a beteget ahhoz az egységhez irányítja, ahol éppen a legkevesebben vannak. Ez mind a beteg biztonságérzetéhez, mind pedig az ellátás optimalizálásához hozzájárul.

Ugyanakkor az ápolási munka rendjébe tagozódott ápolási terv pontos végrehajtását, valamint az orvos által előírt vizsgálati, kezelési és terápiás terv végrehajtását szintén segítheti az alkalmazott RFID technológia. Az ápolási dokumentáció adatai az anamnézis, az állapot felmérés, az ápolási diagnózis és az ápolási terv vonatkozásában folyamatosan elérhetővé válik az arra jogosult ápolási szakszemélyzet és az orvosok számára betegenként.

Elbocsátás során pedig a zárójelentést, melyet az osztályos orvos ad ki a betegnek, elektronikusan a beteg kártyájára lehet tölteni, valamint annak kórházi példányának archiválása is gyorsabbá válik. A beteg azt papírmozgás nélkül át tudja adni kezelőorvosának, aki egy mobil RFID olvasóval át is veheti a dokumentációt.

ÖSSZEFOGLALÁS

Az egészségügyi létesítmények területén kialakított ellenőrzött munkaterületek és munkafolyamatok védelme kiemelt fontosságú. Önmagukban a beléptető rendszerek nem képesek a védelemre, az áthaladási pontok forgalmát bonyolítják le. Az RFID rendszerek is csak részeit képezik az elektronikai védelemnek, ami a komplex biztonsági rendszernek egy komponense. Az RFID technológia természetesen nem ad megbízható megoldást a kórházbiztonság minden területére és önmagában történő alkalmazása egyáltalán nem biztosítja az átfogó védelem körülményeit. Az aktív kártya már saját beépített energiaforrást tartalmaz. A működtetés során az olvasó kódolt rádiófrekvenciás jelet bocsát ki a kártya felé, amit az szintén kódolt jellel viszonoz. Minden esetben meg kell vizsgálni egy komplex rendszer RFID komponensének hatását, ugyanis, az RFID tag által visszasugárzott (módosított) jel zavart okozhat más rádiós eszközökben.

Az RFID eszközök kiválasztásánál elsősorban azt kell figyelembe venni, hogy a kapukat milyen távolságra helyezzük el egymástól, hiszen a kártyák hatótávolsága is behatárolt. Továbbá azt kell figyelembe venni, az eszköz működési frekvenciáját annak érdekében, hogy a kórház berendezéseit ne zavarja. A proximity kártya legkedveltebb, korszerű azonosítási eszköz, amely az RFID technológiáján alapuló rádiós adatátvitellel működik. Szinte bármilyen alkalmazásban megoldást nyújt. Hatalmas gyakorlati jelentősége abból származik, hogy segítségével adatokat lehet nyerni az adathordozó megérintése nélkül, mert az adatátvitel elektromos vagy mágneses hullámok segítségével történik. A fényképpel, felirattal

ellátható kártyák igen kedveltek, de kulcsra tehető, öntapadós, karóra kivitelű és henger formájú szerelhető azonosítók is megtalálhatók a kereskedelmi forgalomban. A kórházi dolgozók számára az aktív proximity kártya használata javasolható, amelynek egy, nem csak azonosításra szolgáló vészhívóval ellátott változata a napjainkban gyakran tapasztalható egészségügyi dolgozókat ért fizikai inzultusok tükrében igen hasznosnak tűnik. Az eszközbe integrált vészhívó gomb segítségével azonnal lehet az élőerős szolgálatot riasztani az esetleges támadás esetén.

A kórházbiztonság komplex fogalom. Az egészségügyi létesítmények veszélymentes állapota fenntartása érdekében összetett biztonságtechnikai alrendszereket kell összehangolni, melyek közül csak egy az RFID technológia, mely egyedül önmagában természetesen nem alkalmas a létesítményi biztonság összes területén felmerülő probléma kezelésére.

A jól kiépített rendszernek azonban számos olyan funkciója üzemeltethető, amely a fenti célok teljesítése mellet közvetve szolgálja a beteg biztonságát, a gyógyító-munka biztonságát, az ápolási munka biztonságát és ezekkel együtt összességében a betegellátás biztonságát.

Felhasznált irodalom

[1] Lukács György: Új vagyonvédelmi nagykönyv, CEDIT Kft., Budapest, 2002.

[2] [6] Magyar Egészségügyi Ellátási Standardok Kézikönyv (MEES)1.0 változat Egészségügyi Minisztérium 2007.

[3] 1/2005. (EüK. 1.) EüM irányelv a betegazonosító rendszer működéséről

[4] Betegbiztonság az egészségügyben, tájékoztató kiadvány, Egészségügyi Minisztérium, 2007

[5] A betegek biztonsága, elkerülhetők-e a hibák? - Egészségügyi Minisztérium előadás anyag 2005. in: Betegbiztonság az egészségügyben, tájékoztató kiadvány, Egészségügyi Minisztérium, 2007

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Horváth József
horvath0101@gmail.com

A ZÁRTLÁNCÚ VIDEÓ MEGFIGYELŐ RENDSZEREK JÖVŐJE

Absztrakt

A zártláncú video megfigyelő rendszer fontos része a biztonsági rendszereknek és fontos mindenkinek, aki a bűnözés ellen harcol és szeretné megvédeni tulajdonát. Jelen cikk bemutatja a zártláncú video megfigyelő rendszerek fejődését, alkalmazásának jogszabályi hátterét, fontosabb elemeit, illetve a fejlesztések jelenlegi helyzetét (integrált rendszerek, HD CCTV).

The CCTV is important part of the security systems and important for everybody, who would like to fight against the crime and would like to defend the private ownership. This article presents the evolution of the CCTVs, the legal environment of the application, the important elements and the current the situation of the development (integrated systems, HD CCTV).

Kulcsszavak: zártláncú, CCTV, megfigyelőrendszer, kamerarendszer, HD CCTV ~ closed-circuit, CCTV, monitoring system, camera system, HD CCTV

ZÁRTLÁNCÚ VIDEÓ MEGFIGYELŐ RENDSZEREK

A CCTV rendszer kialakulása

A zártláncú videó megfigyelő rendszer (Closed-circuit television, továbbiakban CCTV) alkalmazásának célja egy adott terület (lakások, épületek, ipari és mezőgazdasági létesítmények és területek, pénzügyi és egyéb objektumok) megfigyelése, igény esetén az események rögzítése.

Valós zártláncú videó megfigyelő rendszerként történő alkalmazás első alkalommal 1942-ben, Peenemünd-ben (Németország) történt, ahol a V-2 rakéták indításának megfigyelésére került telepítésre a rendszer. [1]

Térfigyelési célból számos helyen telepítettek később kamararendszert, így 1956-ban Hamburgban, 1959-ben Hannoverben ideiglenesen az ipari vásár miatt megnövekedett belvárosi forgalom miatt, illetve 1960-ban Frankfurtban a közlekedési szabálysértések és a forgalom ellenőrzésére, valamint gyűlések és nyilvános összejövetelek megfigyelésére. Angliában 1960-tól kezdték alkalmazni a CCTV rendszereket, azonban itt már úttörő módon állandó jelleggel. Itt elsődlegesen a tömeg megfigyelésére használták, például a thai királyi család londoni látogatása idején. Később a British Railways telepített ilyen rendszereket a vágányokat ért rongálások miatt. Ténylegesen a bűncselekmények megelőzése érdekében történő CCTV rendszer telepítés 1968. szeptemberében, az Egyesült Államok Olean (New York állam) városában történt. Itt 8 kamerarendszer került kiépítésre, melyek képeit a helyi rendőrség napi 24 órán keresztül figyelte. Érdekesség az, hogy időzítés alapján forgó kamerák kerültek alkalmazásra a hatékonyság növelése érdekében. [1]

Napjainkban oly mértékben elterjedt az alkalmazásuk, hogy nem tudunk úgy elmenni otthonról dolgozni, bevásárolni vagy szórakozni, hogy valahol ne találkoznánk fejünk felett elhelyezett kamerákkal. Egyre több munkahelyen is alkalmazzák vagyonvédelmi céllal (alapanyagok, termékek védelmére, rongálások megelőzésére).

1. kép: Térfigyelőkamerák[1]

2. kép: Figyelmeztető jelzés a kamerás megfigyelésre [2]

A kamerák és az azok létére figyelmeztető jelzőtáblák pszichológiailag is elrettenthetik az elkövetőt. Amennyiben a rendszer rögzíti az eseményt, az a bűnüldöző szervek számára nagy segítséget jelenthet az elkövetők elfogásában, az esemény rekonstruálásában illetve az eljárás során bizonyítékként is felhasználható lehet.

1 http://www.domesticinvestigations.org/personal-protection/cctv.html, letöltve 2013. február 15.

2 http://www.popsci.com/technology/article/2011-08/new-cctv-system-would-use-behavior-recognition-zero-crimes, letöltve 2013. február 15.

1.2 A CCTV rendszer hasznossága

A CCTV rendszerek bűnözés visszatartó hatása nehezen bizonyítható, mivel nem lehet olyan területet kialakítani, ahol kiküszöbölhető lenne minden egyéb változás, amely befolyásolhatná a mérési eredményeket. Ilyen eset lehet akár a közvilágítás ideiglenes kiesése, melynek okán a CCTV rendszerek alkalmazásának hatékonysága csökken, lehetőséget teremtve bűncselekmények elkövetésére. Sok fórumon hallani, hogy megelőző szerepet tulajdonítanak a rendszernek, azonban azt sem lehet vizsgálni, hogy a CCTV rendszer felszerelése nélkül az adott területen növekedett-e volna a bűnözés mértéke vagy nem.

A rendszer számos ellenzője azzal érvel, hogy alapvető jogaink sérülnek, azonban fontos hogy egy 2000-ben készített elemzés alapján a megkérdezettek 64 %-a hasznosnak tartja az ilyen rendszerek alkalmazását. [2]

Lényeges, de szerintem nem elemzett fogalom a megfigyelt területre történő belépéssel kapcsolatban használt „ráutaló magatartás", melyet a vagyonvédelmi törvény is említ. Ennek lényege, hogy amennyiben a kihelyezett figyelmeztető táblák ellenére belép az adott személy a megfigyelt területre, azzal elfogadja és „hozzájárul" a saját megfigyeléséhez. Nem találni olyan elemzést, amely azt vizsgálná, hogy milyen hátrányok érik (pl. hosszabb menetidő, stb.) azon személyeket, akik el szeretnék kerülni a kamerákat, de nem bűncselekmény tervezése miatt, hanem egyszerűen azért, mert nem értenek egyet ezen rendszerek alkalmazásával.

1.3 A CCTV rendszer alkalmazásának jogi alapjai

Közterületen kizárólag a rendőrség, illetve az önkormányzati közterület felügyelet üzemeltethet térfigyelő kamerát. [3]

A megfigyelő rendszer vagyonvédelmi szolgálatok általi kezelését a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól 2005. évi CXXXIII. törvény „A személy- és vagyonvédelmi tevékenységet végző személyre vonatkozó szabályok" című fejezete részletesen tárgyalja. Ezen törvény tartalmazza azon korlátozásokat, melyek figyelembe vételével üzemeltethet a vagyonőr megfigyelő rendszereket. Fontos az is, hogy a vonatkozó, az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti adatvédelmi jogok megtartására is ügyelni kell. Az elektronikus megfigyelőrendszer vagyonőr által történő működtetése csak magánterületen, illetve a magánterületnek a közönség számára nyilvános részén történhet. Az alkalmazás feltétele a megfigyeléshez való hozzájárulás, mely a ráutaló magatartással is megadható. Azaz, ha az elektronikai megfigyelésre figyelmeztető jelzések ellenére bemegyünk például egy bevásárlóközpont területére, azzal beleegyezésünket adtuk a megfigyeléshez. Lényeges az, hogy bizonyos helyeken (pl. öltöző, próbafülke, mosdó, illemhely, kórházi szoba, szociális intézmény lakóhelyisége, stb.) nem lehet elektronikus megfigyelést alkalmazni. [4]

A vagyonvédelmi társaságoknak a fenti törvényben foglaltak alapján kell a felvételeket, mint adatokat kezelniük kép-, hang-, vagy kép- és hangrögzítés esetén. Alapesetben, amennyiben a rögzített kép-, hang-, valamint kép- és hangfelvétel nem kerül felhasználásra, a rögzítéstől számított három munkanap elteltével meg kell semmisíteni, illetve törölni kell. A rögzítéstől számított harminc nap elteltével kell megsemmisíteni, illetve törölni azon felvételeket, melyek nyilvános rendezvényen, közforgalmú közlekedési eszköz állomásán, megállóhelyén az emberi élet, testi épség, személyi szabadság illetve terrorcselekmény és közveszély okozás megelőzése miatt vagy jelentős értékű pénz, értékpapír, nemesfém, drágakő kezelése során, annak védelme érdekében kerültek rögzítésre. A rögzítéstől számított hatvan nap elteltével kell megsemmisíteni, illetve törölni azon felvételeket, melyek pénzügyi tevékenység (pl. pénzügyi szolgáltatás, befektetési-tőzsdei tevékenység, biztosítási tevékenység) helyszínéül szolgáló nyilvános magánterületeken kerültek rögzítésre. [4]

2. A CCTV RENDSZEREK KIÉPÍTÉSE

Fontos, hogy a video megfigyelő rendszer tervezését a felhasználó/megrendelő által megfogalmazott elvárások alapján kell végrehajtani, azonban az is lényeges, hogy a megrendelő is rendelkezzen a rendszer minimális szintű ismeretével, így elkerülve a túlzott elvárásokat.

Tudnunk kell, hogy milyen körülmények között (nappal-éjjel, kül- vagy beltéren) tervezett a használata, van-e igény a kapott kép rögzítésére vagy a felvétel távoli elérésének lehetőségére, a megbízó vagy biztonsági szolgálat fogja üzemeltetni.

2.1. A CCTV rendszer részei

A megfigyelőrendszer főbb elemei:

1. Kamerák és objektívek: a kamerák lehetnek bel vagy kültéri, fekete-fehér vagy színes kamerák, fix, forgatható, cső vagy célkövető kamerák. Az objektív a kamera képalkotó eleme, amelybe elhelyeznek egy, a beeső fény mennyiségét szabályozó elemet, az íriszt. Léteznek fix, manuális vagy auto íriszes, fix vagy változtatható fókusztávolságú objektívek.
2. Monitorok és videójel kapcsoló eszközök: korábban fekete-fehér vagy színes CRT monitorokat alkalmaztak, napjainkban főként az LCD és plazma monitorok a jellemzőek. A kamerák által biztosított képek monitoron történő megjelenítéséhez szükséges eszközök:
   a) képléptetők: a bemenetekre adott videojeleket egymás után jeleníti meg a monitoron;
   b) képosztó: a bemenetekre adott videojeleket osztott kép formájában (minden képet egyidőben) tudja megjeleníteni;
   c) video-multiplexerek: a bemenetekre adott videojeleket képesek léptetve vagy osztott kép formában megjeleníteni, illetve képes az egyes képeket önmagukban is megjeleníteni;
   d) video-mátrixok: bármelyik kimenetén megjeleníthető egy adott kamera képe.
3. Képrögzítők: korábban az úgynevezett „Time-lapse” (időben elnyúló folyamatok képi rögzítése) videófelvevőket alkalmazták. Ma már a rögzítés önálló DVD felvevővel vagy a számítógép merevlemezére történik. A DVD felvevő előnyei a kompatibilitás (meghibásodás esetén könnyen cserélhető), megbízhatóság, helyszükséglet, a PC-hez képest kedvezőbb ár. A számítógépes konfiguráció előnye, hogy amennyiben rendelkezünk már olyan számítógéppel, mely alkalmas a feladatra (megfelelő operációs rendszer, digitalizáló kártya), akkor ez a legolcsóbb megoldás. A rögzítés lehetséges időtartama sok jellemzőtől függ, ilyen például az alkalmazott eszközben a rendelkezésre álló merevlemez mérete, a beállított minőség (nagyobb felbontás esetén nagyobb merevlemez szükséglet) vagy a percenként rögzített képkockák száma.
4. Adatátviteli eszközök: kábeles, mikrohullámú vagy rádiós átviteli út kialakításához szükséges eszközök. [5]

További lehetséges elemeket jelentenek például az internetes távoli elérés eszközei. Internetes kapcsolat kialakítása esetén fontos a megfelelő sávszélesség biztosítása. A feltöltési sebesség határozza meg a készülékünkön elérhető képfrissítési sebességet. A kameravezérlés, a kameramozgatás, felvételek visszakeresése is megoldható bizonyos technikai feltételek megléte esetén. [6]

Napjainkban minden területen megfigyelhető az IP alapú rendszerek terjedése és ez igaz a CCTV rendszerek esetében is. Fontos azonban, hogy nem mindig az IP alapú videomegfigyelő rendszer a jó választás, mivel ennél a típusnál a jó minőségű videóképhez

minden esetben szükséges a megfelelő megvilágítás biztosítása. A gyakorlatban a leghatékonyabb megoldást a hibrid rendszerek biztosítják, melyek gyenge megvilágítási körülmények között is jól értékelhető képet biztosítanak. [7]

A monitorrendszer elhelyezéséhez és a biztonsági/kezelőszemélyzet megfelelő elhelyezéséhez központi megfigyelőhelyiség kialakítása szükséges. A helyiségnek biztosítani kell a jogszabályokban meghatározott adatkezelés feltételeit és a tartós ott tartózkodás megfelelő körülményeit (jogosulatlan belépés kizárása, szellőzés és klíma, megfelelő fényviszonyok, munkaasztal, stb.).

3. kép: Megfigyelő helyiség Londonban [3]

2.2 A CCTV rendszer működésképtelenségének lehetséges okai

A CCTV rendszerek működésképtelenségének számos oka lehet. Az első és legfontosabb a nem megfelelő telepítés. Ma Magyarországon törvényileg meghatározott végzettséggel rendelkező személyek végezhetik ilyen rendszerek tervezését és telepítését. Így elkerülhetőek az olyan hibák, mint például a 4. képen látható anomália. Itt ugyanis a szálloda kamerarendszerének képei a szobákban lévő televízió készülékeken is láthatóak. A nem megfelelő védelem az időjárás viszontagságai ellen a terület megfigyelését vagy a kamera mozgatását akadályozhatja (pl. hó, fagyás, stb.). A rendszer telepítése előtt a megfigyelt terület típusát elemezni kell. Ha a rendszer őszi időszakban telepítésre, akkor figyelemmel kell lenni arra, hogy tavaszi-nyári időszakban a fák lombjai az addig meglévő rálátást gátolhatják. Kiemelt figyelmet kell fordítani a megfelelő fényviszonyokra, mivel a kamera elhelyezésének helytelen megválasztása esetén a kamerára az optimálistól eltérően, túl sok vagy túl kevés fény jut, így annak képe nem használható. Mindig a legfrissebb szoftververziót kell alkalmazni lehető legtöbb szolgáltatás kihasználása érdekében. Problémát jelent a számítógéppel kapcsolatban a jelszavak elfelejtése vagy a számítógép alkatrészeinek meghibásodása. A különböző elemek és alkatrészek a kezelési és üzemeltetési utasításokban meghatározott karbantartások végrehajtását igénylik. Számos esetben előfordul, hogy anyagi okok miatt nem végzik el az időszakos karbantartásokat, azonban ezzel hosszabb távon nagyobb műszaki meghibásodásokkal kell számolni. Számolni kell a kamerarendszer elemeinek szándékos tönkretételével is. [8]

[3] http://londoners.blog.hu/2008/09/13/big_brother_london_figyel_teged, letöltve 2013. február 23.

4. kép: Megfigyelő kamera képe a szállodai szoba televíziókészülékén

A videó megfigyelő rendszerekkel az MSZ EN 50132 szabványcsalád foglalkozik, például:

1. MSZ EN 50132-1:2010 Riasztórendszerek. Zárt láncú televíziós megfigyelőrendszerek biztonságtechnikai alkalmazásokhoz. 1. rész Rendszerkövetelmények;
2. MSZ EN 50132-7:2006 Riasztórendszerek. Zárt láncú televíziós megfigyelőrendszerek biztonságtechnikai alkalmazásokhoz. 7. rész: Alkalmazási irányelvek

2.3 A CCTV jövője

Integrált rendszerek

Napjainkban egyre elterjedtebb az integrált rendszerek alkalmazása. Az integrált rendszer működésének lényege, hogy egy rendszerben bekövetkező változás egy hozzá csatlakozó rendszerben reakciót generál. A behatolás-jelző rendszer, a beléptető rendszer vagy az őrjárat-követő rendszerek jelzésének hatására elindítható a CCTV felvételének indítása/leállítása. A beléptető rendszerek monitorjain a belépési pontnál lévő CCTV kamera képe és a belépési pontnál tartózkodó személy rendszerben eltárolt képe a biztonsági személyzet részére egy kijelzőn látható. A CCTV rendszerben érzékelt mozgás (ez a kép változásának vizsgálatával oldható meg) hatására elindul a felvétel rögzítése. Lehetséges a riasztás kiváltása vagy a távfelügyeletet ellátó szolgálatnál vagy kivonuló szolgálatnál. [5]

HD CCTV

A HD CCTV (Nagyfelbontású Zártláncú Televíziózás) nagy előnye lehet, hogy a már meglévő analóg rendszerünk fejlesztése esetén nem igényel külön kábelezési munkálatokat, a videojel koaxiális kábelen kerül továbbításra. A rendszer úgy került kialakításra, hogy a kamerák és a vevő cseréjével végrehajtható a fejlesztés. A 720p HD CCTV majdnem háromszor, míg az 1080p hatszor akkora felbontást nyújt, mint az analóg rendszerek. A HD CCTV rendszer progresszív letapogatású, így nem jelentkezik az analóg rendszerekre jellemző, a váltottsoros letapogatásból eredő villódzás és elmosódottság. HD CCTV rendszer telepítésénél fontos, hogy a HD-SDI (vagy az SMPTE 292M szabvány) gyártó által történő garantálása esetén nem lehetnek kompatibilitási problémák az eszközök ill. rendszerek között. [9]

A HD CCTV által biztosított néhány további előny:

1. megbízható minőség és valós kép, mivel a HD CCTV nem bontja csomagokra az átvinni kívánt képet az alkalmanként túlterhelt hálózaton, így a késleltetés is minimális;
2. valósidejű gyorsdóm-vezérlést biztosít, mivel nem alkalmaz semmilyen tömörítést, ami a jel késleltetését okozná. Azaz a kezelő nem tapasztalhat késést a vezérlő mozgatása és a gyors dóm mozgása között. [9]

HD CCTV rendszerek telepítőjeként az alábbi két lehetőséggel találkozhatunk:

Teljes HD-SDI kiépítés esetén	Hybrid HD-SDI Analogue Installation
Kiinduló helyzet	
- nincs létező CCTV rendszer; - van létező rendszer és a fejlesztéshez pénzügyi keret; - igény a nagy felbontásra az azonosítás érdekében;	- van létező CCTV rendszer, melyekhez HD kamera szükséges; - nincs létező CCTV rendszer és nincs szükség nagy felbontású képre;
Érvek mellette	
- a nagy felbontás egyének azonosítását teszi lehetővé; - könnyen telepíthető koax kábelre; - nincs szükség számítógépes szakemberre a telepítéshez;	- a meglévő analóg kamerák cseréje nem szükséges; - a már meglévő koax kábel használható;
Érvek ellene	
- HD kamerákkal a rendszer kialakítása drágább, mint a hibrid rendszeré;	- meglévő analóg rendszer esetén szükséges egy új DVR HD-SDI bemenettel;

1. táblázat: Teljes HD-SDI és hibrid HD-SDI rendszerek kialakításának szempontjai [10]

A HD CCTV rendszer a meglévő rendszerekhez (analóg és IP alapú) képest többet nyújt, azonban az arra történő átállásnak költségei vannak. A meglévő analóg rendszerről alacsonyabb költséggel jár HD CCTV rendszerre váltani, hiszen ebben az esetben néhány HD CCTV elem (pl kamerák, monitorok) felhasználásával lehetséges a jelenleg elérhető legfejlettebb rendszert kialakítani. A két rendszer által nyújtott kép minőségbeli különbsége az 5. képen látható.

5. kép: Analóg és HD CCTV kép minőségkülönbsége [4]

ÖSSZEGZÉS

Cikkemben röviden összefoglaltam a CCTV-k kialakulását, alkalmazásának jogi alapjait, a rendszerek alkotó elemeit, a lehetséges hibaforrásokat, valamint a jelenlegi alkalmazás irányait illetve elemeztem a rendszer által nyújtott lehetőségeket. Mint arra az előző fejezetben rávilágítottam, a CCTV rendszerek fejlődése nem állt meg és a HD CCTV rövid elemzésével megmutattam a CCTV fejlődésének újabb mérföldkövét. Az új technikai megoldás által biztosított minőségi ugrás újabb és újabb felhasználási területen jelenthet előnyt, legyen az távolabbról történő rendszámfelismerés, még könnyebb arcfelismerés, de akár egy adott terület még jobb megfigyelési lehetősége.

Véleményem szerint ezen rendszerek alkalmazása mindenképpen szükséges, mivel számos eset bizonyítja, hogy ha el nem is tántorította a tettest a bűncselekmény elkövetésétől, segített annak felderítésében. A HD CCTV alkalmazása pedig egyértelműen még egyszerűbbé teszi mindennapi életünket a még nagyobb információtartalom biztosításával.

[4] http://oktel.hu/szolgaltatas/kamerarendszer/hd-cctv/, letöltve 2013. február 24.

Felhasznált irodalom

[1] VINTECH Digital Security solutions: Back to Basics: Where Did the Video Security System Come From? (2011. ápr. 20)
Forrás: http://www.vintechnology.com/journal/uncategorized/back-to-basics-where-did-the-video-security-system-come-from/ letöltve: 2013. január 15., a szerző saját fordítása

[2] Horvát Zsolt: Rendőrségi kamerás megfigyelés Magyarországon (2006.)
Forrás:
http://tasz.hu/files/tasz/imce/s__gi_kamer__s_t__rfigyel__s_Magyarorsz__gon.pdf
letöltve: 2013. január 13.

[3] Dr. Kulcsár Zoltán: A kamerás megfigyelés és az adatvédelem. (2010. május 12.)
Forrás: http://www.adatvedelmiszakerto.hu/2010/05/a-kameras-megfigyeles_adatvedelem/
letöltve: 2013. január 13.

[4] A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól 2005. évi CXXXIII. törvény, 30. §
Forrás: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0500133.TV
letöltve: 2013. január 13.

[5] Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései. (2009)
Forrás: http://portal.zmne.hu/download/konyvtar/digitgy/phd/2009/utassy_sandor.pdf
letöltve: 2013. január 15.

[6] Videokontroll Kft.: Zártláncú videó megfigyelő rendszerek digitális rögzítéssel.
Forrás: http://videokontroll.hu/cctv_kapu/tartalom/cctv.htm letöltve: 2013. március 09.

[7] Horváth Tamás: IP alapú CCTV rendszert? Hadmérnök, VI. Évfolyam 2. szám - 2011. június
Forrás: http://www.hadmernok.hu/2011_2_horvatht.pdf letöltve: 2013. január 15.

[8] VINTECH Digital Security solutions: Surveillance Not Working? What's the Point? (2012. aug. 03.)
Forrás: http://www.vintechnology.com/journal/security-tips-2/surveillance-not-working-whats-the-point/ letöltve: 2013. január 15., a szerző saját fordítása

[9] Ecsedi Ákos: HDcctv az IP kamerarendszer lehetséges alternatívája. DETEKTOR Plusz 2011/4.
Forrás: http://detektorplusz.hu/fajl.php?id=11986 letöltve: 2013. január 15.

[10] Videocon: Videocon guide to HD-SDI CCTV
Forrás: http://www.videcon.co.uk/uploads/files/Videcon_Guide_to_HD-SDI.pdf
letöltve: 2013. február 10., a szerző saját fordítása

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Rácz-László István
laszlo-antal.hu@t-online.hu

AZ ORSZÁGHÁZ VÉDELME ÉRDEKÉBEN ALKALMAZHATÓ NEM HALÁLOS FEGYVEREK A FELADATOT ELLÁTÓ SZERVEZET SZÁMÁRA

Absztrakt

Már maga a „nem halálos fegyver” elnevezés is ellentmondást rejt magában. Mindenki tudja már gyermekkora óta, hogy bármely fegyver „küldetése” az élet kioltása, azonban sok esetben szükséges egy ilyen eszköz, amelynek segítségével időlegesen ki lehet vonni élő erőket (embereket) a műveletekből. Ilyen eszközök léteznek már, azonban hosszú időn keresztül a gumilövedékre és a könnygázra korlátozódtak. A bűnözés, a tömegmegmozdulások a terrorizmus elleni harcban folyamatosan szükség van új fegyverek, új módszerek kidolgozására. A különböző, ENSZ égisze alatt zajló béketeremtő és békefenntartó műveletek során az ilyen jellegű fegyverek alkalmazása szintén elengedhetetlen és fontos lehet. Napjainkban az Egyesült Államok mellett több ország is intenzíven dolgozik a „nem halálos fegyver” fejlesztésén, amelyek mechanikus, akusztikus, kémiai, elektromos, elektromágneses vagy optikai elven működnek.

Already himself the not lethal weapon a name hides a contradiction alone. Everybody knows that the mission of any weapons is the extinction of the life already since his childhood, but in many cases necessary a device like this, for which who there may be temporarily with his help to pull over living strengths (people_nation) from the operations. Devices like this exist already, they were restricted to the rubber bullet and the tear gas through long time however. The delinquency, the mass demonstrations there is need for the development of new weapons, new methods continuously in the fight against the terrorism. In the course of the pacificatory and peacekeeping operations going on under the different one, UN's aegis the application of the weapons with a character like this likewise essential and may be important. More countries work in our Suns intensively beside United States the not on the development of a lethal weapon, that mechanical, acoustic, they work on a chemistry, electric, electromagnetic or optical principle.

Kulcsszavak: *nem halálos fegyver, ellentmondás, harc, fegyver, működési elv ~ not lethal weapon, contradiction, fight, weapon, operation principle*

BEVEZTÉS

Az Országház Budapest egyik legismertebb középülete, a Magyar Országgyűlés és egyes intézményeinek (például Országgyűlési Könyvtár) a székhelye. Budapest V. kerületében, a Duna partján, a Kossuth Lajos téren található. Az épületet gyakran Parlamentként is emlegetik.

Steindl Imre megvalósult terve a historizáló eklektika jegyében született, barokk alaprajzú, barokk tömeghatású épület, részleteiben alapvetően neogótikus stílusú.

Maga az épület 268 m hosszú, 123 m széles és 96 m magas, alapterülete 17 745 négyzetméter, térfogata 473 000 köbméter. Központi eleme a kupola, amelynek két oldalán emelkedik a képviselőház (ma az országgyűlés) és a volt főrendiház (ma Kongresszusi terem) ülésterme. Az épületnek 27 kapuja van, belül 29 lépcsőház és 13 személy- és teherlift szolgálja a közlekedést és szállítást. Az épületben valamivel több mint 200 irodahelyiség található. A Duna felőli oldal a főhomlokzat, de a hivatalos főbejárat a Kossuth térről nyílik. Kívül és belül összesen 242 szobor (90 külső és 152 belső) van a falakon, jeles freskók és festmények is díszítik az Országházat.

Szent Korona

A 2000. évi I. törvény rendelkezése alapján az Országházban van kiállítva a Szent Korona és a többi koronázási jelvény (a koronázási palást kivételével). A korona korábban a Nemzeti Múzeumban volt megtekinthető; a törvény szövege szerint az ünnepélyes áthelyezéssel „Magyarország méltó helyére emeli a Szent Koronát, és a nemzet múzeumából a nemzetet képviselő Országgyűlés oltalma alá helyezi”. [1]

AZ ORSZÁGHÁZ VÉDELME

Köztársasági Őrezred (múlt)

A Köztársasági Őrezred (ismert még, mint Kormányőrség, vagy röviden Őrezred) egy magyarországi állami szervezet volt, mely fő feladataként védte a hazai és külföldi védett vezetőket, őrizte a kormányzati szempontból kiemelt jelentőségű objektumokat, valamint biztosította a hazai és nemzetközi állami rendezvényeket.

A közel 1200 fős Köztársasági Őrezred különálló szervként 2012. július 1-jével szűnt meg, állománya és feladatkörei a Készenléti Rendőrséghez (KR) kerültek át.

A Köztársasági Őrezred a Rendőrséghez tartozó, az Országos Rendőr-főkapitányság főigazgatósági jogállású szervezeti egysége, önálló gazdálkodású költségvetési szerv volt. A testület parancsnoka jogállását tekintve az országos rendőrfőkapitány egyik helyettese is volt egy személyben, személyének kinevezése nem az országos főkapitány, hanem a miniszterelnök hatásköre volt, az igazságügyi és rendészeti miniszter javaslatára.

2010 júniusában a Köztársasági Őrezredet az évtizedekig használatában lévő Honvéd utcai műemlék épületből több objektumba költöztették szét, nagy része a Készenléti Rendőrséggel közös, Kerepesi úti laktanyába került. A Honvéd utcai objektumot a Honvédelmi Minisztérium vette át. Az Őrezredről leválasztották a miniszterelnök és a köztársasági elnök védelmét – ezeket az újonnan megalakuló BM Terrorelhárítási Központ vette át –, a megmaradó szervezeti egységeket pedig már akkor a Készenléti Rendőrségbe tervezték beolvasztani.

A kormány 2010. november 10-i ülésén született döntés alapján a Magyar Honvédség fogja adni a kormányőrség által őrzött Szent Korona és koronázási jelvények díszőrségét, valamint a Köztársasági Elnöki Hivatal székhelyét képező Sándor-palotánál a díszelgést. [2]

Tevékenysége
Az Őrezred fő feladatai közé a védett személyek és kijelölt létesítmények védelme tartozott (személyvédelem és objektumvédelem). Önálló vállalkozási tevékenységet nem végzett, szabad kapacitásai terhére, valamint a bevételek növelése érdekében a következő szolgáltatási tevékenységekkel is foglalkozott:

- gépkocsi kölcsönzés,
- biztonságtechnikai eszközök kölcsönzése,
- személyszállítás,
- biztonsági szolgáltatások (személyvédelem, tűzszerészeti átvizsgálás),
- szállodai szolgáltatás étteremmel,
- egyéb nyomdai szolgáltatások (rendezvényekre beléptető kártyák készítése).

Jogi háttér
A Köztársasági Őrezred szakmai feladatait elsősorban a következő jogszabályok határozták meg:

- A Rendőrségről szóló 1994. évi XXXIV. törvény
- A védett személyek és kijelölt létesítmények védelméről szóló 160/1996 (XI. 5.) kormányrendelet.

Készenléti Rendőrség (jelen)
Magyarország rendőri szervei közül a legösszetettebb speciális feladatokat a Készenléti Rendőrség látja el. A szervezet a Rendőrség állandó csapaterejének bázisa, a budapesti és vidéki alegységekkel együtt több, mint 5000 főt foglalkoztat.

Munkatársai az ország minden pontján együttműködnek az arra igényt tartó területi rendőri és más állami szervvel, valamint ellátják a kizárólagos hatáskörükbe tartozó sajátos feladatokat is.

A Rendőrség speciális közrendvédelmi, csapatszolgálati egységeként a Készenléti Rendőrség részt vesz az előre nem tervezhető, halaszthatatlan beavatkozást és csapaterőt igénylő, a védett vezetőkkel kapcsolatos biztosítási feladatok végrehajtásában, ellátja a különleges szállítmányok őrzésével, a személy- és objektumvédelemmel, valamint a polgári repüléssel kapcsolatos feladatokat. Kizárólagos hatáskörébe tartozik a nemzetbiztonság területén jelentkező tűzszerészeti feladatok ellátása, az Állami Futárszolgálat irányítása, a pénz- és értékszállítás, továbbá a középfokú rendészeti képzésben történő részvétel.

Országgyűlési Őrség (jövő)
Az Országgyűlési Őrség (a továbbiakban: Őrség) alapfeladata az Országgyűlés függetlenségének és külső befolyástól mentes működésének védelme, személyvédelmi, létesítménybiztosítási feladatok, valamint az elsődleges tűzoltási és tűzbiztonsági feladatok ellátása.

Az Őrség az Országgyűlési törvény (továbbiakban OGY törvény) értelmében 2013. évtől önállóan működő központi, költségvetési szerv, amelynek gazdálkodásával kapcsolatos feladatait a Hivatal látja el, az Országgyűlés költségvetési fejezetében önálló címet képez. Az Őrség a Házelnök irányítása alatt álló fegyveres szerv, vezetője a parancsnok.

Az OGY törvény értelmében az Őrség ellátja a Házelnök személyi védelmét, az Országház, az Országgyűlés Irodaháza, valamint az Országgyűlés Hivatala elhelyezésére szolgáló épületek, valamint az abban tartózkodók biztonsága érdekében a létesítménybiztosítási feladatokat. Gondoskodik az Országház, az Országgyűlés Irodaháza, valamint az Országgyűlés Hivatala elhelyezésére szolgáló épületek területére történő belépés és az ott-tartózkodás rendjére vonatkozó szabályok betartásáról, valamint az Országházban, az Országgyűlés Irodaházában, az Országgyűlés Hivatala elhelyezésére szolgáló épületekben a

jogszabályokban meghatározott tűzbiztonsági követelmények megtartásáról, a tevékenységi körükkel kapcsolatos veszélyhelyzetek megelőzésének és elhárításának a feltételeiről. Ellátja a tárgyalási rend fenntartásával kapcsolatos, e törvényben meghatározott feladatokat, továbbá a protokolláris díszelgési feladatokat.

Annak figyelembevételével, hogy az új szervezet 2013. január 1-jei indulásához az Őrség működésére 349 fős létszámmal (– 44 fő tiszt, 295 fő tiszthelyettes, valamint 10 fő köztisztviselő) lenne szükség. [3]

A VÉDETT SZEMÉLYEK ÉS A KIJELÖLT LÉTESÍTMÉNYEK VÉDELMÉRŐL

Törvényi szabályozás

Az államháztartásról szóló 2011.évi CXCV. törvény 11.§(3) bekezdésében foglaltak alapján a Köztársasági Őrezredet a Készenléti Rendőrségbe történő beolvadással 2012. június 30. napjával a belügyminiszter megszüntette.

A közfeladatok további ellátása a Köztársasági Őrezred által

- a Rendőrségről szóló 1994.évi XXXIV. törvény,
- a Rendőrségről szerveiről szóló és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII.13) Korm. rendelet,
- a Magyar Honvédség által védendő létesítmények kijelöléséről, valamint a magyar állam folytonosságát és függetlenségét megtestesítő ereklyék köréről és az őrzésükre vonatkozó szabályokról szóló 78/2011. (V.12.) Korm. rendelet,
- a védett személyek és kijelölt létesítmények védelméről szóló 160/1996. (XI.5.) Korm. rendelet,
- a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól szóló 295/2010. (XII.22.) Korm. rendelet,
- a magyar légtér igénybevételéről szóló 4/1998. (I.16.) Korm. rendelet alapján ellátott közfeladatokat a Készenléti Rendőrség látja el.

A Magyar Köztársaság érdekei szempontjából különösen fontos személyek, a nemzetközileg védett személyek, valamint a kijelölt létesítmények védelmének szabályairól, a Rendőrségről szóló 1994. évi XXXIV. törvény rendelkezik.

Hazai védett személyek

A védett személyek körét, amint már említetem a 160/1996.(XI. 05.) számú Kormányrendelet határozza meg.

Állandó személyvédelemben részesülő állami vezetők

1. A köztársasági elnök
2. A miniszterelnök
3. Az Alkotmánybíróság elnöke
4. A Kúria elnöke
5. A legfőbb ügyész

Magyarországon tartózkodó nemzetközileg védett személyek, valamint viszonosság alapján más külföldi személy magyarországi tartózkodása alatti védelme is megoldandó.

Annak a személynek is meg kell szervezni az ideiglenes védelmét, akit az Alkotmánnyal és a törvényekkel összhangban álló közéleti tevékenysége miatt személye vagy közvetlen környezete ellen irányuló erőszakos bűncselekményekkel fenyegettek meg, illetve egyéb alapos okból védelme szükséges — kormány dönt ezen személyek védelméről a rendelet szerint a Belügyminiszter javaslata alapján — ehhez tartozik ezen személyek utazásának

biztosítása is. „A védelem kiterjed a felsorolt személyek közlekedési utazásbiztosításán kívül még a védett személy:

a) a) életének, testi épségének megóvására;
b) b) munkahelye, lakása vagy egyéb tartózkodási helye őrszemélyzettel
c) vagy technikai eszközökkel biztosított védelmére;
d) c) indokolt esetben közlekedési útvonalára;
e) d) részvételével lebonyolított hivatalos programok színhelyére;
f) e) belföldi utazására, ezeken túl a Magyar Köztársaság elnökének és miniszterelnökének a védelme kiterjed a külföldi utazásaikra is. [4]

Az előbbi bekezdésekben leírtak megegyeznek más nemzetek által meghatározott védett személyek körével. Az tény viszont, hogy vannak olyan országok ahol ezeket a védelmi intézkedéseket határozottabban tudják foganatosítani, mint nálunk. Ennek oka talán az, hogy azokban az országokban ahol határozottabb a fellépés, ott folyamatos támadásnak vannak kitéve a védett személyek. Gondolok itt például a Közel-keleti országokra, ahol folyamatos terrorcselekményekről és támadásokról hallani védett személyek és objektumok ellen. Vagy Olaszország, ahol inkább az igazságszolgáltatásban résztvevők (ügyészek, főbírók), illetve az újságírók ellen követnek el folyamatosan merényleteket kisebb nagyobb sikerrel.

Hazánkban szerencsére ekkora mértékű fenyegetettségről jelenleg nem beszélhetünk, ám ennek ellenére mindig a legrosszabbra kell készülni. Vagyis ugyanúgy ki kell képezni a személyvédelemben dolgozó állományt jelen „békeidőben” mindenre, mintha folyamatos támadások alatt állnánk. Ez azért is fontos, mert a hazánkba látogató különösen veszélyeztetett védett személyeket nemcsak a hazájukban támadhatják meg, hanem bárhol a világon, így nálunk is.

Létesítménybiztosítási intézkedés céljából kijelölt létesítmények

1. Az Országház
2. A Sándor-palota épülete
3. Az Országgyűlés Irodaháza
4. Az Alkotmánybíróság épülete
5. A Legfőbb Ügyészség épülete
6. A Külügyminisztérium központi épületei
7. A Belügyminisztérium épülete
8. Közigazgatási- és Igazságügyi Minisztérium épülete
9. Az Állami Számvevőszék központi épületei
10. Az Információs Hivatal központi objektuma

Személy- és létesítménybiztosítási intézkedés

(1)A rendőrség, valamint a rendőr a védett személy biztonsága érdekében a meghatározottakon túlmenően:

a) útvonalat, közterületet a forgalom elől elzárhat, a forgalmat korlátozhatja,
b) nyilvános és közforgalmú intézmények működését korlátozhatja,
c) magánlakásba - külön írásos utasítás birtokában - ellenőrzés, a helyszín megfigyelése és biztosítása céljából beléphet, és ott tartózkodhat,
d) területet lezárhat, és megakadályozhatja, hogy oda bárki belépjen vagy onnan távozzék, illetőleg az ott tartózkodókat távozásra kötelezheti.

(2) A védett személyeket - a nemzetközi jogi kötelezettségek és a viszonossági gyakorlat figyelembevételével - a Kormány rendeletben jelöli ki. A Kormány rendeletében ki nem jelölt személy ideiglenes védelmét a miniszter rendeli el. Az ideiglenes védelem tartama a 12 hónapot nem haladhatja meg.

(3)A rendőrség a védett középületek és az abban tartózkodók biztonsága érdekében az (1) bekezdés a) és d) pontjában meghatározottakon túl a be- és kilépésre az ott elhelyezett szerv vezetőjével egyetértésben szabályokat állapíthat meg.

(4) A rendőrség a védett személy vagy létesítmény biztonsága érdekében technikai ellenőrzést alkalmazhat, elrendelheti a jogszerűen birtokban tartott veszélyes tárgyak kötelező letétbe helyezését.

(5)Az (1) bekezdés a) és d) pontja szerinti intézkedést az elrendelő rendőri szerv vezetője - függetlenül az előzetesen meghatározott időtartamtól - ötnaponként felülvizsgálja, és annak eredményéről a (3) bekezdésben meghatározott vezetőt tájékoztatja. Ha az (1) bekezdés a) és d) pontja szerinti intézkedés időtartama a tizenöt napot meghaladja, az intézkedést az országos rendőrfőkapitány, valamint a terrorizmust elhárító szerv főigazgatója felülvizsgálja. Ha az (1) bekezdés a) és d) pontja szerinti intézkedés időtartama a harminc napot meghaladja, az intézkedést az országos rendőrfőkapitány, valamint a terrorizmust elhárító szerv főigazgatója legalább harminc naponként felülvizsgálja. Az intézkedés indokoltságáról, tartalmának jogszerűségéről az országos rendőrfőkapitány, valamint a terrorizmust elhárító szerv főigazgatója három munkanapon belül határozattal dönt. A határozatot a központi szerv, valamint a terrorizmust elhárító szerv honlapján közzé kell tenni.

(6)Ideiglenes védelemben részesíthető az a személy, akit közéleti tevékenysége miatt személye vagy közvetlen környezete ellen irányuló erőszakos bűncselekménnyel fenyegettek meg, illetve egyéb alapos okból védelme szükséges. [5]

NEM HALÁLOS FEGYVEREK

A nem halálos fegyverek, olyan eszközök, anyagok, eljárások, melyeket úgy terveztek, fejlesztettek és alkottak meg, hogy az emberi élet kioltása nélkül a személyi sérülés lehetőségének minimálisra történő csökkentése során a célszemélyt teljesen harcképtelenné tegye. A fenti meghatározás nem azt jelenti, hogy ezekkel, az eszközökkel ne lehetne ölni. A nem halálos fegyverek nem szakszerű használata esetén is lehet okozni halálos sérüléseket. [6]

A nem halálos fegyverek csoportosítása

A nem halálos fegyverek megjelenési formájukban igen sokrétűek és változatosak. Ugyanúgy megtalálhatók közöttük a gumilövedékek, mint a közönséges víz, vagy a különféle habok, a fény, de akár még a szagok is. A fegyverek változatosságából adódik, hogy csoportosításuk számos rendező elv alapján lehetséges. A csoportosításra vonatkozóan általánosan elfogadott változat nem létezik.

Egyik rendező elv lehet, amikor a kategorizálást az alapján végezzük el, hogy az adott nem halálos fegyverrel milyen célra, milyen hatást kívánunk elérni. Ennek megfelelően a csoportosítást elvégezhetjük a cél jellege, illetve az alkalmazott elv szerint.

A cél jellege szerint:

1. Személyek ellen alkalmazható:
    a) Fizikai elven működő fegyverek
        a) Kinetikus/mechanikus fegyverek
        b) Elektromos fegyverek
        c) Optikai eszközök
    b) Kémiai elven működő fegyverek
    c) Irányított energiájú fegyverek
        a) Akusztikus fegyverek
        b) Elektromágneses fegyverek
        c) Lézerek

2. (Hadi)technikai eszközök, infrastruktúra ellen alkalmazható:
    a) Fizikai elven működő fegyverek
        a) Mechanikus eszközök
        b) Elektromos-/Elektromos rendszerek ellen alkalmazott fegyverek
    b) Kémiai elven működő fegyverek
    c) Irányított energiájú fegyverek
        a) Elektromágneses fegyverek
        b) Lézerek

Az alkalmazott elv szerint:

1. Fizikai:
    a) Kinetikus/mechanikus
    b) Elektromos
    c) Optikai
2. Kémiai
3. Irányított energia:
    a) Akusztikus
    b) Elektromágneses
    c) Lézer
4. Biológiai
5. Egyéb.[7]

A készenléti rendőrségnél alkalmazott kényszerítő eszközök, nem halálos fegyverek csoportja, alkalmazásának lehetőségei

Testi kényszer

A rendőr - intézkedése során - az ellenszegülés megtörésére testi erővel cselekvésre vagy a cselekvés abbahagyására kényszerítést (testi kényszert) alkalmazhat.

Bilincs

A rendőr bilincset alkalmazhat a személyi szabadságában korlátozni kívánt vagy korlátozott személy

1. önkárosításának megakadályozására,
2. támadásának megakadályozására,
3. szökésének megakadályozására,
4. ellenszegülésének megtörésére.

Mozgásszabadságot korlátozó eszközök:

1. Fémből készített kézi egész- és félbilincsek,
2. Műanyagból készített bilincsek (bilincsvágóval),
3. Vezetőszáras bilincsek,
4. Kombinált anyagú testbilincsek,

Vegyi eszköz, elektromos sokkoló eszköz, rendőrbot, kardlap, illetőleg más eszköz alkalmazása

1. A rendőr a szolgálatban rendszeresített, vegyi vagy elektromos sokkoló eszközt, illetőleg rendőrbotot vagy kardlapot alkalmazhat:
    a) a mások vagy saját életét, testi épségét, illetőleg a vagyonbiztonságot közvetlenül veszélyeztető támadás elhárítására,
    b) a jogszerű rendőri intézkedéssel szembeni ellenszegülés megtörésére.

2. A rendőr a szolgálatban rendszeresített gumilövedéket, illetve pirotechnikai eszközt, könnygázgránátot, elfogó hálót, ingerlőgázt, továbbá vízágyút alkalmazhat a mások vagy saját élete, testi épsége, illetőleg a vagyonbiztonság közvetlen veszélyeztetésének elhárítására, vagy ha a lőfegyverhasználat feltételei fennállnak.

Különféle rendőrbotok, ütőeszközök, hidegfegyverek és elektromos eszközök

1. Normál- és hosszított rendőrbotok,
2. Változtatható méretű (összetolható) rendőrbotok,
3. Többcélú rendőrbotok (tonfák),
4. Elektromos sokkolók,
5. Kardok

Védekezésre, vagy akaratnyilvánításra képtelen állapotot előidéző, természetes vagy mesterséges hatóanyagú, könnyfakasztó, szemet, nyálkahártyát irritáló eszközök és anyagok

1. Mesterséges vagy természetes hatóanyaggal szerelt könnygázszóró palackok, gázsprayk, habok,
2. Mesterséges vagy természetes hatóanyaggal szerelt univerzális (lőhető, dobható) könnygázgránát,
3. Fegyverről, speciális vetőeszközről indítható, mesterséges vagy természetes hatóanyaggal szerelt könnygázgránát,
4. Kézi működtetésű, dobható, mesterséges vagy természetes hatóanyaggal szerelt könnygázgránát,
5. Könnygázutántöltő folyadékok.

Pirotechnikai eszközök és anyagok

1. Hang-gránátok,
2. Fénygránátok,
3. Kombinált hang-fény gránátok,
4. Villanó gránátok.

Szolgálati kutya alkalmazása

(1) A rendőr szájkosárral ellátott szolgálati kutyát - pórázon vagy anélkül - kényszerítő eszközként akkor alkalmazhat, ha a testi kényszer alkalmazásának feltételei fennállnak.

(2) A rendőr szájkosár nélküli szolgálati kutyát pórázon vezetve alkalmazhat, ha a jogellenesen összegyűlt tömeg enyhébb kényszerítő eszközzel nem oszlatható szét, illetve, ha az a közbiztonságot súlyosan veszélyeztető csoportosulás szétoszlatásához vagy a rendőri intézkedéssel szembeni tevőleges ellenállás leküzdéséhez szükséges.

(3) A rendőr szájkosár és póráz nélküli szolgálati kutyát alkalmazhat

a) súlyos sérüléssel fenyegető támadás elhárítására;

b) súlyos bűncselekmény elkövetésével alaposan gyanúsítható személy elfogására;

c) a személye ellen intézett támadás vagy az életét, testi épségét közvetlenül fenyegető magatartás elhárítására.

Útzár, megállásra kényszerítés

A rendőrség közút forgalmának korlátozását vagy közút lezárását rendelheti el a bűncselekmény elkövetésével megalapozottan gyanúsítható személy, valamint a bűncselekmény elkövetőjének elfogására és a külön jogszabályban kijelölt létesítmények védelmére, ennek során - a közlekedés biztonságát is figyelembe véve, külön jogszabályban meghatározott feltételekkel - útzárat telepíthet.

Útzár alkalmazása során a rendőrség járművek áthaladását torlaszszerűen vagy más módon lassító, megakadályozó építményt, technikai berendezést vagy ezek hiányában bármilyen eszközt telepíthet, amellyel a rendőri intézkedés foganatosítása elől járművel menekülő személyek feltartóztatása, elfogása elérhető.

A bűncselekmény elkövetésével megalapozottan gyanúsítható személy, valamint a bűncselekmény elkövetőjének elfogása érdekében - ha járművel menekül - a rendőrség mások személyét és biztonságát nem veszélyeztetve a járművet követheti és megállásra kényszerítheti.

A csapaterő alkalmazása

(1) A rendőrök csapaterőben alkalmazhatók

a) az alkotmányos rend erőszakos megváltoztatására irányuló bűncselekmény (Btk. 139. §), a lázadás (Btk. 140. §), valamint a rombolás (Btk. 142. §) elkövetése esetén;

b) a személyek élet- és vagyonbiztonságát tömegesen veszélyeztető események megszüntetésére vagy az ilyen következményekkel járó erőszakos cselekmények megakadályozására és az elkövetők elfogására;

c) súlyos bűncselekményt elkövető, szökésben lévő fegyveres személy felkutatására, elfogására;

d) terrorcselekmény felszámolására, a túszok kiszabadítására;

e) eltűnt személy vagy tárgy felkutatására;

f) katasztrófa megelőzésére és következményeinek elhárítására;

g) a gyülekezési jogról szóló törvény hatálya alá tartozó vagy más jelentős rendezvény rendjének biztosítására;

h) védett személy, veszélyes szállítmány vagy az állam működése, vagy a lakosság ellátása szempontjából kiemelten fontos létesítmény őrzésére, védelmére;

i) nagy területű helyszín biztosítására;

j) törvényben meghatározott más esetben.

(2) Csapaterő alkalmazása során a rendőrség a 17. § (1) bekezdésben írt jogokat indokolt mértékben korlátozhatja, területet személy- és járműforgalom elől elzárhat.

Tömegoszlatás

(1) Ha a jogellenesen összegyűlt, illetőleg jogellenes magatartást tanúsító tömeg a szétoszlásra irányuló rendőri felszólításnak nem tesz eleget, a rendőrség az e fejezetben szabályozott kényszerítő eszközök alkalmazása mellett a tömeggel szemben a következő eszközt, illetőleg intézkedést alkalmazhatja:

a) vízágyút,

b) pirotechnikai eszközt,

c) ingerlőgázt,

d) elfogó hálót,

e) lóháton vagy járműkötelékben végzett kényszeroszlatást.

(2) Az (1) bekezdésben említett eszköz alkalmazására a tömeget előzetesen figyelmeztetni kell.

(3) Tilos a tömeget korlátozni a helyszínről történő eltávozásban.

(4) Tilos a tömegoszlatásra lőfegyvert használni.

A csapaterő alkalmazása során a rendőr a csapaterő parancsnokának utasítása szerint köteles eljárni.

(1) A tömeg szétoszlatására irányuló csapaterő alkalmazása során a rendőrség a helyszínen lévők egyéni felelősségét nem vizsgálja.

Közös szabályok
(1) A kényszerítő eszköz alkalmazására az érintettet - ha az eset körülményei lehetővé teszik - előzetesen figyelmeztetni kell.

A testi kényszer és a bilincs kivételével kényszerítő eszköz - a jogos védelem esetét kivéve - nem alkalmazható a láthatóan terhes nővel és a gyermekkorúval szemben.
(3) Ha a rendszeresített kényszerítő eszköz nem áll rendelkezésre, vagy a használatára nincs lehetőség, a rendőr a bilincs, a rendőrbot vagy az útzár helyett más eszközt is igénybe vehet, ha a helyettesített eszköz alkalmazásának törvényi feltételei fennállnak és az, az azzal elérni kívánt törvényes cél megvalósítására alkalmas.
(4) A rendőrségnél rendszeresített robbanófegyverek a lőfegyverrel esnek egy tekintet alá.
A kényszerítő eszköz alkalmazását jelenteni kell a szolgálati elöljárónak.

A lőfegyverhasználatot - annak következményétől függetlenül - az intézkedést követően haladéktalanul jelenteni kell a szolgálati elöljárónak. [8]

2013. JANUÁR 01.-ÉN MEGALAKULÓ ORSZÁGGYŰLÉSI ŐRSÉG JOGOSULTSÁGAI, TÖRVÉNYI SZABÁLYOZÁS

A parlament döntése értelmében 2013. január 1-jén létrejön az Országgyűlési Őrség, a házelnök irányítása alatt álló fegyveres szerv. Ezen felül a jövőben a korábbiaknál erősebb fegyelmi jogköre lesz az ülést levezető elnöknek. Az új országgyűlési törvény úgy rendelkezik, hogy az önálló költségvetési szervként működő őrségnek feladata lesz egyebek mellett a házelnök személyi védelme, az Országház és az Országgyűlési Irodaház biztosítása, tűzbiztonsági és protokolláris feladatok ellátása.

Az Országgyűlési Őrséget a parancsnok vezeti majd, akit a házelnök nevez ki. Az őrök a rendőrségi törvényben meghatározottak szerint fokozott ellenőrzést hajthatnak végre, ruházatot, csomagot, járművet vizsgálhatnak át, magánlakásban és közterületnek nem minősülő helyeken is intézkedhetnek, kép-, illetve hangfelvételt készíthetnek, helyszínt biztosíthatnak. Kényszerítő eszközként bilincset, vegyi eszközt, elektromos sokkoló eszközt, rendőrbotot, lőfegyvert ugyancsak a rendőrségről szóló törvényben meghatározottak szerint használhatnak majd. A parlamenti tárgyalási rend fenntartásával kapcsolatos feladatok ellátása során kényszerítő eszközként azonban kizárólag testi kényszert alkalmazhatnak. Az őrségnek nyomozóhatósági jogköre nem lesz.

Működésüket a 2012. évi XXXVI. törvény az Országgyűlésről szabályozza. [9]

ÖSSZEGZÉS

Az utóbbi időben nemcsak Magyarországon, de szerte a világon megnőtt a jelentősége és kiemelten fontos az állam működése, illetőleg a lakosság ellátása szempontjából kulcsfontosságú létesítmények és tevékenységek, valamint a pótolhatatlan nemzeti értéket képviselő javak jogellenes cselekményekkel szembeni fokozott védelme. E védelem alapvető kérdése, hogy a szolgálatot teljesítő állomány, milyen eszközökkel, fegyverzettel van ellátva, és milyen hatékony, elméleti és gyakorlati kiképzést kapott.

Az objektumok védelme összetett feladat. A védelmi komplexum bármely részelemének hiánya vagy gyengesége kihat a teljes biztonsági rendszer hatékonyságára, főleg, abban az esetben, amikor a részelemek is bonyolult biztonsági alrendszerek (beléptető rendszer; biztonsági monitoring rendszer élőerős szolgálat stb.). A zavarmentes működés követelményeinek biztosítása létfontosságú. Az elektronikai és mechanikai védelmi alrendszerek magas fokú integráltsága mellett továbbra is fontos szerepe van az azokat üzemeltető és döntéshozó élőerős szolgálat tevékenységének, felkészültségének, a kiképzettség szintjének. [10]

A fegyverek fejlődése két irányba mutat: halálos és nem halásos fegyverek. Nem halálos fegyver alatt értünk minden olyan eszközt, anyagot és eljárást, amelyet kifejezetten úgy terveztek, illetve alkalmaznak, hogy a szemben álló fél élőerejét, valamint technikai eszközeit, infrastrukturális létesítményeit semlegesítse, azokat a harcból kivonja, harcképességüket korlátozza, alkalmazásukat lehetetlenné tegye.

A nem halálos fegyvereket több ok miatt hozták létre. Ezek – bizonyos esetek kivételével – csak csekély mértékű sérüléseket, a környezetben pedig minimális járulékos károkat okoznak. Jelentős szerepük van akkor, ha a hagyományos fegyverek alkalmazása nem lehetséges, nem célszerű, vagy katonailag nem indokolt (például tömegoszlatásnál), ugyanakkor a katonák önvédelemi képességét mégis biztosítani kell. Felhasználásuk alternatív lehetőség a parancsnok számára.

A jövő hadseregei két féle képen lesznek felszerelve. Elsősorban a szegény országokban maradnak a hagyományos tömeghadseregek, amelyek hagyományos fegyverekkel lesznek felszerelve. A gazdag országok a professzionális kisebb haderő felé fejlődnek, akik a csúcstechnikájú fegyverek révén jóval nagyobb erőt képviselnek. Itt jelentkezik az igény is a nem halálos fegyverekre.

Felhasznált irodalom

[1] Dr. Csorba László - Sisa József - Szalay Zoltán: Az Országház, Képzőművészeti Kiadó KFT, 2001. Budapest

[2] A Magyar Honvédség által védendő létesítmények kijelöléséről, valamint a magyar állam folytonosságát és függetlenségét megtestesítő ereklyék köréről és az őrzésükre vonatkozó szabályokról szóló 78/2011. (V.12.) Korm. rendelet

[3] 2012. évi XXXVI. törvény az Országgyűlésről

[4] A védett személyek és kijelölt létesítmények védelméről szóló 160/1996. (XI.5.) Korm. rendelet

[5] A Rendőrségről szóló 1994.évi XXXIV. törvény

[6] Bartha Tibor: A nem halálos fegyverek alkalmazásának lehetőségei a Magyar Honvédségnél, különös tekintettel a nem háborús tevékenységek végrehajtása során Nemzetvédelmi Egyetem Doktorandum- 2002.4. szám 1. kötet

[7] Dr. Bartha Tibor: Nem halálos fegyverek, Egyetemi jegyzet Zrínyi Miklós Nemzetvédelmi Egyetem 2009.

[10] Bodrácska Gyula – Berek Tamás: Megelőző intézkedések szerepe a komplex vagyonvédelem területén, építőipari beruházások során, 2010. Hadmérnök, www.hadmernok.hu/2010_1_bodracska_berekt.php

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Tiszolczi Balázs Gergely
tiszolczi.balazs@gmail.com

GONDOLATOK A KÓRHÁZI SZEMÉLY- ÉS VAGYONVÉDELEMRŐL

Absztrakt

Az egészségügy célrendszerének megvalósítása az alaptevékenység (gyógyítás) ellátása során jut érvényre, alapvető működési sajátosságként pedig (többek közt) említhetjük azt a széleskörű folyamatokat támogató, az alaprendeltetéstől némileg elkülönülő, a sokak által ún. perifériásnak tekintett (de nem feltétlenül az), kiszolgáló tevékenységrendszert, amely nélkül a fő rendeltetés nem, vagy csak nehezen, jelentős korlátozásokkal lehetne megvalósítható. Ide sorolható többek közt a kórházi objektumok védelmét biztosító őrszolgálat ellátása, amelynek szintén különleges szabályokkal kell szembenéznie mind a szervezés, a stratégiai tervezés, mind a végrehajtás, az operatív feladatellátás során. A biztonsági őr képzés napjainkban sokat emlegetett átalakulása okán jelen cikkben vizsgálom meg, mely speciális, az általános elméleti és gyakorlati ismeretektől eltérő, vagy eltérő szintű tudásanyagot kell elsajátítania, illetve mely készségekkel és kompetenciákkal kell(ene) rendelkeznie egy olyan vagyonőrnek, aki feladatát kórházi vagy egyéb egészségügyi intézményben látja el.

The realization of healthcare objectives is enforced during the main activity (healing). Besides, as an operational speciality we can mention (among others) the serving system of activities that promotes widespread processes although it is separate from the basic activity to a certain extent and it is considered to be peripheral (though it is not really so). Without the above system, the main purpose could only be realised either with difficulty or with significant limits. This includes (among others) the tending of protection service in health care facilities, which also has to face special rules during organizing, strategic planning and it is the same when executing operational tasks. In the course of the transformation of the training security guards mentioned frequently nowadays, I am examining here in this article what kind of special theoretical and practical skills (different from the common ones) need to be acquired and what kind of skills and personal competence should be possessed by those people serving as a security guard in a health care facility.

Kulcsszavak: *egészségügy, biztonság, speciális készségek, őrzés-védelem ~ health care, security, special skills, guarding*

A VAGYONŐRI JOGOK ÉRTELMEZÉSE KÓRHÁZI KÖRNYEZTEBEN

A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (továbbiakban: VVtv.) [1] a védelmet ellátó vagyonőr számára a megbízó közterületnek nem minősülő létesítményének őrzése során viszonylag széleskörű intézkedési jogosultságokat biztosít. Így munkája végzésekor jogosult a területre belépő vagy az ott tartózkodó személyt kiléte igazolására, a belépés, illetőleg a tartózkodás céljának közlésére, jogosultságának igazolására felhívni, ennek megtagadása vagy a közölt adatok nyilvánvaló valótlansága esetén az érintett belépését, ott tartózkodását megtiltani, és távozásra felszólítani. [1/26.§] Kórházi objektumok esetén a célrendszer és a működési sajátosságok némileg korlátot szabnak, illetve speciális feltételekhez kötik a fent ismertetett jogosultságok gyakorlását. A védelem tervezésénél és a szolgálat ellátásánál az egyik legfontosabb szakmai szempont az adott objektum működési rendje, a tevékenység jellege. Maga a kórház a beteg, vagy akut állapotban lévő emberek ellátására, gyógykezelésére, ápolására, fektetésére szolgáló intézmény, amelyik gondoskodik a beteg emberek életszükségleteinek kielégítéséről is. [2] Ebből a meghatározásból következik, hogy a kórházi tevékenység többek közt az egyik legfontosabb alapjogunk, a testi és lelki egészség érvényesítésének fontos eszköze. Magyarország Alaptörvénye [3] Szabadság és felelősség fejezete foglalkozik azon alapvető jogok tartalmával, amelyek minden embert egyaránt, egyenlő mértékben megilletnek. Tartoznak ide a fent említett, „klasszikus” alapjogok ugyanúgy, mint az ún. harmadik generációs jogok (például a betegjogok, vagy a személyes adatok védelméhez való jog). Az Alaptörvény rendelkezéseivel egyetlen, a hierarchiában alacsonyabb helyet elfoglaló jogszabály sem tartalmazhat ellentétes rendelkezéseket. A jogok lényeges tartalmának ismerete, maximális figyelembe vétele a belső védelmi szabályozás kialakításánál, a védelmi intézkedések tervezésénél és a feladat közvetlen ellátásakor is alapvető elvárás.

A BELÉPÉSI JOGOSULTSÁG MEGÁLLAPÍTÁSA, A BELÉPÉS MEGTAGADÁSA

A szolgálatot ellátó vagyonőr a VVtv. alapján az általa védett létesítménybe, területre való jogosulatlan belépést megakadályozhatja, a jogosulatlanul bent tartózkodót onnan eltávolíthatja. [1/27.§]

Az Alaptörvény deklarálja, hogy Magyarországon mindenkinek joga van a testi és lelki egészséghez, amely cél elérése többek közt az egészségügyi ellátás megszervezésével segíthető elő. [3/XX.Cikk]

A fenti alapjog részeként, annak érvényesülését elősegítve az egészségügyről szóló 1997. évi CLIV. törvény alapján [4] minden betegnek joga van – jogszabályban meghatározott keretek között – az egészségi állapota által indokolt, megfelelő, folyamatosan hozzáférhető és az egyenlő bánásmód követelményének megfelelő egészségügyi ellátáshoz. *Megfelelő* az ellátás, ha az adott egészségügyi szolgáltatásra vonatkozó szakmai és etikai szabályok, illetve irányelvek megtartásával történik, illetve *folyamatosan* hozzáférhető az ellátás, amennyiben az egészségügyi ellátórendszer működése napi 24 órán keresztül biztosítja annak igénybevehetőségét. [4/7.§]

Az állampolgári jogok országgyűlési biztosának OBH 2985/1997. hivatkozási számú jelentése [5] egy panaszbeadványt idéz, melyben a panaszos erős fejfájása miatt elvégzett vizsgálat eredményéért indult a kórházba. A portán megállították, mivel nem volt nála a beutaló. A panaszos elmondása alapján emiatt akarták korlátozni az egészségügyi intézménybe történő belépését, és vele szemben durva bánásmódot alkalmaztak. A vizsgálat eredményeképpen az ombudsman megállapította, hogy a beutalóval nem rendelkező *beteg* a belépési jogosultság szempontjából nem minősülhet illetéktelen személynek, nem indokolható, hogy beutaló hiánya miatt ne engedjenek be betegeket a kórházba. Amennyiben

a beteget elzárják a kórház, illetve a rendelőintézet épületébe való bejutás lehetőségétől, egyben az egészségügyi ellátás igénybevételének lehetőségétől is megfosztják. Megállapítása szerint sérti a betegek (legmagasabb szintű) testi egészséghez való jogát és ezáltal alkotmányos visszásságot okoz, hogy az egészségügyi intézet épületébe kizárólag beutaló felmutatásával lehet bejutni.

A belépési jogosultság (károsodott egészségi állapot) megállapítása kórház esetében sem tartozik a személy– és vagyonőr kompetenciájába, és az ombudsmani állásfoglalás szerint a beléptetés ezen szakaszában nem is rendelkezhet a megbízó által előírt/biztosított olyan eszközzel, ami alapján ez számára egyértelműen megállapítható lenne. (Pl. megfelelően kitöltött beutaló, berendelő lap, stb.) Azt a kérdést, hogy a betegségre hivatkozónak (a kórházba belépni szándékozónak) valóban szüksége van-e orvosi ellátásra, és az ellátáshoz való hozzájutása indokolt- e, az orvoson illetve az egészségügyi szakszemélyzeten kívül senki más nem döntheti el, ezért számára lehetővé kell tenni, hogy állapotát az arra jogosult személy mérhesse fel. Betegségre, romlott egészségi állapotra utaló nyilvánvaló tény, vagy „csak" arra való hivatkozás esetén bárminemű korlátozás, amely az egészségügyi szolgáltatás igénybevételét akadályozza, alkotmányos alapjogokat sért(het), [6] és nem teljesülhet továbbá az egészségügyi törvényben meghatározott folyamatosan hozzáférhető (igénybe vehető) ellátás követelménye. [6/p.153]

A jogosultság kérdését azonban nem csak a beteg oldaláról kell megvizsgálni. A kapcsolattartás joga megilleti a beteget annak fekvőbeteg-gyógyintézeti elhelyezése során, így jogosult más személyekkel akár írásban, akár szóban kapcsolatot tartani, továbbá *látogatókat fogadni*, valamint általa meghatározott személyeket a látogatásból kizárni. A látogatók fogadásának jogát a beteg az intézetben meglévő feltételektől függően, betegtársai jogainak tiszteletben tartásával és a betegellátás zavartalanságát biztosítva gyakorolhatja. Ennek részletes szabályait, a jogok tartalmának korlátozása nélkül, a fekvőbeteg-gyógyintézet házirendje határozza meg. [4/11.§] Bár az egyes intézményeknek megvan a lehetősége arra, hogy ezen jog érvényesülését némiképp szabályozott körülmények között biztosítsa, a gyakorlat mégis azt mutatja, hogy az intézmények nagy részét tekintve szinte szabadon, jelentős korlátozások nélkül lehet a betegeket látogatni, függetlenül az érkezés idejétől és az egyes kórterembe érkező személyek számától.

A hozzáférhetőség okán egy másik területet is érinteni kell a gyalogosforgalmon kívül, ez pedig a kórház területére gépjárművel való behajtás szükségessége. Az állampolgári jogok országgyűlési biztosának OBH 4152/2002 számú jelentésében [7] egy esetet vizsgál, ahol egy vidéki kórházban a belső szabályozás (főigazgatói utasítás) miatt súlyos beteget, életveszélyes sérültet személygépkocsival szállító magánszemélyek is csak adott pénzösszeg előzetes megfizetése esetén hajthattak be a kórház területére. A vizsgálat tárgyát ezúttal is a már hivatkozott testi egészséghez való jognak és az egészségügyi ellátás folyamatos hozzáférhetőségének való megfelelőség szolgáltatta. A vizsgálat eredményeként a biztos megállapította, hogy a deklarált alapvető emberi jogok semmilyen módon nem korlátozhatóak, az egészségügyi ellátáshoz való hozzáférés nem tehető függővé az ún. kapupénz megfizetésétől. Ezen alapjogok érvényesülése nem függhet továbbá attól, hogy a beteg mentővel, avagy személygépkocsival érkezik-e az egészségügyi szolgáltatóhoz. *A panaszolt intézmény főigazgatói utasítása előidézi a testi és lelki egészséghez való joggal összefüggésben az egészségügyi ellátáshoz való jog sérelmének a közvetlen veszélyét.*

Az ombudsman ajánlást tett továbbá arra, hogy az intézmény a behajtás rendjét a hivatkozott jogszabályoknak megfelelően alakítsa át úgy, *hogy az maradéktalanul megfeleljen egészségügyi intézmény funkciójának.* A vizsgált kérdéskörben nem hagyható figyelmen kívül az az igény sem, hogy az egészségügyi intézmények területén éppen az egészségügyi ellátás zavartalansága érdekében a gépjárművek forgalmát és a várakozást – akár várakozási díj megállapításával – szabályozni kell. A gyakorlatban sokszor találkozunk azzal az elterjedt

megoldással, miszerint a betegeket szállító gépjárművek be - és kihajtását minden esetben térítésmentesen biztosítják az intézmények (a behajtás és az első negyed/félóra ingyenes), azonban a további benntartózkodásért már az előre megállapított parkolási/várakozási díjat kell fizetni.

A SZEMÉLYAZONOSSÁG IGAZOLÁSA

A VVtv. további lényeges rendelkezése, hogy a személy- és vagyonőr tevékenysége gyakorlása során jogosult az intézkedésében érintett személyt felhívni kilétének igazolására. Ha az általa erre felkért személy önként és hitelt érdemlően nem igazolja kilétét, a személyazonosság megállapítására – indokolt esetben – igazoltatásra jogosult hatósági személyt kérhet fel. [1/27.§]

A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban Infotv.) [8] előírásai szerint: személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. [8/4.§]

Az Adatvédelmi Biztos 2002. évi beszámolója [9] egy konkrét panaszbeadványt idéz, amelyben a panaszos kifogásolta, hogy egy egészségügyi intézetben biztonsági szolgálat ellenőrzi a látogatók személyazonosságát és rögzíti adataikat. Az intézménnyel kapcsolatban az Adatvédelmi Biztos megállapította, hogy:

„A VVtv. lehetővé teszi azt, hogy a vagyonőr a megbízó közterületnek nem minősülő létesítményének őrzése során a területre belépő vagy az ott tartózkodó személyt kiléte igazolására, a belépés, illetőleg a tartózkodás céljának igazolására felhívja. Ez a rendelkezés azonban nem jelent korlátlan felhatalmazást arra, hogy a vagyonőr meghatározott intézménybe látogatók személyazonosságát ellenőrizze. Az adatvédelmi törvény alapján ugyanis személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet; csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, és csak a cél megvalósulásához szükséges mértékben és ideig. *Az, hogy a vagyonőr mikor ellenőrizheti a látogatók személyazonosságát, az általa védett intézmény jellege, elrendezése, valamint a személy- és vagyonvédelem szükségessége alapján határozható meg.* Az [érintett intézmény] az egészségügyi ellátó hálózat része, közintézmény, ebből kifolyólag az intézet vezetőjének a jogköre a belépés rendjének meghatározását illetően szűkebb, mint egy magántulajdonban lévő létesítmény tulajdonosának. További korlátot jelent a látogatók személyazonosságának ellenőrzésére az, hogy az érintettek nagy része beteg. Az ő esetükben a látogatás ténye önmagában különleges adatnak minősül,[1] hiszen abból, hogy ilyen minőségükben jelennek meg az intézetben, következtetni lehet betegségükre […]. Ebből kifolyólag a szolgálat csak azokat a személyeket szólíthatja fel kilétük igazolására, akik nem betegként kívánnak belépni az épületbe. Ha a látogató azt állítja, hogy ő az [intézmény] betege, személyazonosságát a vagyonőr nem ellenőrizheti, az érintettet nem szólíthatja fel kiléte igazolására. Ebben az esetben a vagyonőrnek a látogatót az intézmény dolgozójához kell irányítania, aki az [intézmény] nyilvántartásából, az előjegyzési naptárból, beutalóból meggyőződhet arról, hogy az érintett betegként tartózkodik az épületben; a nyilvántartásban nem szereplő betegek esetén pedig az érintett adatait az egészségügyi dokumentáció részeként rögzítheti."

[1] *Különleges adat:* […] egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat [...] [8/3.§]

ELEKTRONIKUS MEGFIGYELŐ RENDSZER

A vagyonőr a megbízó közterületnek nem minősülő létesítményének őrzése során jogosult: […] elektronikai vagyonvédelmi rendszert alkalmazni. [1/26.§] A vagyonőr elektronikus megfigyelőrendszert kizárólag magánterületen, illetve a magánterületnek a közönség számára nyilvános részén alkalmazhat, ha ehhez a természetes *személy kifejezetten hozzájárul*. A hozzájárulás ráutaló magatartással is megadható. Ráutaló magatartás különösen, ha az ott tartózkodó természetes személy a magánterület közönség számára nyilvános részén a megfelelően elhelyezett ismertetés ellenére a területre bemegy, kivéve, ha a körülményekből egyértelműen más következik. A vagyonőr az elektronikus megfigyelőrendszer működése útján kép-, hang-, valamint kép- és hangfelvételt a kötelezettségeit meghatározó szerződés keretei között, a szerződésből fakadó kötelezettségei teljesítése céljából, *az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti adatvédelmi jogok érvényesítése mellett*, illetve e törvényben meghatározott korlátozó rendelkezések betartásával készíthet, illetve kezelhet. E tevékenysége során vagyonőrzési feladatokat ellátó személy adatkezelőnek minősül. [1/30.§]

Annak érdekében, hogy az elektronikus megfigyelőrendszer kórházi alkalmazásának tényleges lehetőségeit megállapítsuk, a vagyonőri feladatokat ellátó személyek elektronikus megfigyelőrendszer üzemeltetési jogát szükséges összevetnünk a tárgykörben keletkezett ombudsmani ajánlásokkal. Megjegyzendő, hogy bár az adatvédelmi biztos intézménye megszűnt, funkcióját átvéve a feladatokat jelenleg a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) látja el, mely a korábbi biztosi ajánlások alkalmazhatóságával, hivatkozhatóságával kapcsolatos megkeresésemre arról tájékoztatott, hogy az egészségügyi intézményekben végzett kamerás megfigyelések terén a Hatóság osztja az ombudsmani időszakban kialakított álláspontot.

Az adatvédelmi biztos egyik, 2000-ben kiadott ajánlásában [10] kifejti, hogy törvény eltérő rendelkezésének, illetve az érintettek hozzájárulásának hiányában közterületen, közintézményben (hivatali időben), nyilvános magánterületen (a hivatalos nyitva tartás ideje alatt) *csak megfigyelést végző képfelvevő, illetve személyazonosításra alkalmatlan képeket rögzítő berendezések üzemeltethetők; a megfigyelés tényéről és módjáról tájékoztatni kell az érintetteket.*

Az épített környezet alakításáról és védelméről szóló 1997. évi LXXVIII. törvény (továbbiakban: Étv). [11] értelmező rendelkezései alapján a kórházak közhasználatú építmények,[2] amelyek használata nem korlátozható. Ezeknek egyik fontos jellemzője azonban, hogy a tulajdonos (használó) a funkció és a működőképesség megtartása érdekében bizonyos területek igénybevételét megtilthatja, korlátozhatja[3] (ennek joga a közintézmény említett fogalmának meghatározásából is világosan kitűnik), ami teljesen érthető is, hiszen egy kórház esetében a műtők, raktárak, gyógyszerek stb. elhelyezésére szolgáló területek nyilván nem azok a területek, amelyeket bárki korlátozás nélkül igénybe vehet. Más értelmezés szerint a tulajdonos (használó) az építmény csak egyes, a célrendszer betöltéséhez

[2] *Közhasználatú építmény:* az olyan építmény (építményrész), amely– a település vagy településrész ellátását szolgáló funkciót tartalmaz, és használata nem korlátozott, illetve nem korlátozható (pl. alap-, közép-, felsőfokú oktatási, *egészségvédelmi, gyógyító,* szociális, kulturális, művelődési, sport, pénzügyi, kereskedelmi, biztosítási, szolgáltatási célú építmények *mindenki által használható részei*), továbbá – használata meghatározott esetekben kötelező, illetve elkerülhetetlen (pl. a közigazgatás, igazságszolgáltatás, ügyészség építményeinek mindenki által használható részei), valamint, amelyet – törvény vagy kormányrendelet közhasználatúként határoz meg. [11/2. §]

[3] További kérdésként merül fel, melyek ezek a területek és a használat szabályait ki és milyen formában állapíthatja meg. A gyakorlatban ezek már kialakultak, de jogi szabályozását tekintve még hiányosságok tapasztalhatók. A testi – lelki egészség megőrzése, helyreállítása, az egészségügyi ellátás zavartalansága érdekében definiálni kell egészségügyi intézmények esetében a forgalomtól elzárt területek típusait és szabályozni kell azok használatát.

elengedhetetlenül szükséges részeit teszi mindenki által látogathatóvá. Ezen nyitott épületrészek az elektronikus megfigyelőrendszer alkalmazása szempontjából a VVtv. értelmező rendelkezései szerint leginkább a magánterület közönség számára megnyitott részeként értelmezhetők. [6/p.156]

Szintén a hivatkozott 2000-es ajánlás része, hogy nyilvános magánterületen, illetve magánterületen csak abban az esetben rögzíthetők a berendezések által közvetített, személyazonosításra alkalmas képek, ha – a rögzítés céljának, módjának, a felvételek tárolási idejének és helyének, valamint az adatkezelő szervezet ismeretében – *az érintettek egyértelműen hozzájárultak, illetve hozzájárulhatnak személyes adataik kezeléséhez*. Amennyiben – törvényi felhatalmazás hiányában – olyan közterületen, vagy nyilvános magánterületen történik képrögzítéses megfigyelés, amelyet a személyes adataik kezeléséhez hozzájárulni nem szándékozók is kénytelenek felkeresni, vagy ott megjelenni, akkor lehetővé kell tenni, hogy az érintettek kérésére a rájuk vonatkozó felvételeket soron kívül töröljék.

Fentiekkel összefüggésben az adatvédelmi biztos 2572/K/2007-3 ügyszámú ajánlása [12] említhető, melyben egy beadvány kapcsán azt vizsgálja, hogy önkormányzati fenntartású rendelőintézet folyosóin, váróhelységeiben felszerelhető-e elektronikus megfigyelőrendszer vagyonvédelmi és bűnmegelőzési célból. Az üggyel kapcsolatban a biztos kifejti, hogy „a rendelőintézetbe látogató állampolgárok számára egy kezelésen vagy vizsgálaton való megjelenés már önmagában is kellemetlenséget, nehézséget jelenthet, ezért indokolt, hogy személyes adataik kezelésével összefüggésben különleges érzékenységgel járjanak el. Az Avtv. szabálya alapján az érintett adatkezeléshez történő hozzájárulása akkor teljes, ha megfelelő tájékoztatáson alapul és önkéntes. *Az egészségügyi intézménybe való belépéskor az érintettnek nincs választási lehetősége, hogy hozzájárul vagy sem a képfelvételhez, hiszen valamilyen egészségügyi oknál fogva szükséges felkeresnie a kérdéses rendelőintézetet.* Ebből viszont az következik, hogy az önkéntes hozzájárulás elve sérülne abban az esetben, ha elektronikus megfigyelőrendszer *venné fel és rögzítené* az érintett állampolgár jelenlétét, tevékenységét az egészségügyi intézmény folyosóján, váróhelységében."

Szintén ezen ajánlásában kinyilvánítja, hogy ellenzi a térfigyelő kamerarendszer kiépítését bármely egészségügyi intézmény területén, mivel az érintettek személyes adatok védelméhez fűződő joga sérülne, hiszen nincs lehetőségük önkéntesen beleegyezni személyes adataik ilyen módon történő kezelésébe. Vagyonvédelem céljából olyan megoldás alkalmazását tartja elfogadhatónak, mely a legkevésbé sérti az egészségügyi szolgáltatást igénybevevők privát szféráját. *Ennek egyik módja lehet, hogy humán erővel – például biztonsági szolgálat felállításával – oldják meg a vagyonvédelmi és bűnmegelőzési feladatokat.*

Összefoglalva: az adatvédelmi biztos ellenzi a térfigyelő rendszerek kiépítését az egészségügyi intézmények területén. Azonban ha mégis elhelyeznek ilyeneket, csak úgy lehet megtenni, hogy *csak megfigyelést végző képfelvevő, illetve személyazonosításra alkalmatlan képeket rögzítő* berendezések üzemeltethetők - hacsak valamilyen úton az üzemeltetők nem szerzik be minden egyes beteg írásos hozzájárulását a személyazonosításra alkalmas képek rögzítéséhez - a megfigyelés tényéről és módjáról tájékoztatják az érintetteket, és lehetővé teszik, hogy az érintettek kérésére a rájuk vonatkozó felvételeket soron kívül töröljék.

A lehetőségeket tovább árnyalja az a tény, hogy bár a kizárólag személyes megfigyelést végző elektronikus rendszerek üzemeltetése nem számít adatkezelésnek, de a kamerák elhelyezésénél figyelembe kell vennünk az Alaptörvény rendelkezését, miszerint az emberi méltóság sérthetetlen. Minden embernek joga van az élethez és az emberi méltósághoz. [3/ II. Cikk] Ezzel összhangban vannak a VVtv. azon rendelkezései is, miszerint nem alkalmazható elektronikus megfigyelőrendszer olyan helyen, ahol a megfigyelés az emberi méltóságot sértheti, így különösen öltözőben, próbafülkében, mosdóban, illemhelyen, kórházi szobában és szociális intézmény lakóhelyiségében. [1/30.§] (Ezen rendelkezés azonban csak a

vagyonvédelmi célból üzemeltett berendezéseket érinti, életvédelmi célból, megkötötten alkalmazható megfigyelőrendszer.)

Ha pusztán személyes megfigyelés céljából illetve azonosításra alkalmatlan képeket rögzítő eszközöket helyezünk is el az egészségügyi intézmény területén, azt is differenciáltan, az emberi méltóságra tekintettel kell megtennünk. Az intézmények területén tehát - akár történik rögzítés, akár nem - a következő helyeken lehet elfogadható az elektronikus megfigyelőrendszer használata:

főbejárat, egyéb, a betegek, látogatók be-, és kiléptetésére szolgáló bejáratok, liftek előterei, büfé, stb. A folyosókon, illetve várókban elhelyezett kamera alkalmazása már jóval nagyobb körültekintést igényel, hiszen ha jogilag nem is, megítélésben mindenképpen különbséget kell tennünk egy szemészeti, illetve egy bőr-, és nemibeteg gondozó vagy nőgyógyászat várója között. De ide sorolhatók a mentőbejárathoz vezető útvonalak is, hiszen sok esetben súlyos sérülteket, magatehetetlen állapotban lévő embereket szállítanak, ezért a telepítés helyét minden intézménynél alapos mérlegelés után, az intézményen belüli részeknél egyedileg kell meghatározni, tekintettel a betegellátás természetére, módjára, jellegére. Természetesen a betegek, látogatók által igénybe nem vett helyeken (zárt magánterületek), pl. szervizbejárat, anyagmozgatási útvonalak, személyzeti bejáró stb. elhelyezhető kamera, de itt is figyelembe kell lenni az általános előírásokat, amelyek a munkavállalók személyes adatainak védelméhez való jogát érintik. [6/p.158]

Bár nem tartozik szorosan a tárgyhoz, de ehelyütt mindenképpen szólni kell arról, hogy a statisztikák, illetve személyesen végzett felmérések szerint kórházakban leginkább azokon a helyeken követik el a betegek, látogatók értékei, testi épsége elleni cselekményeket, ahol a védelmet szervezők számára nincs lehetőség elektronikus megfigyelőrendszert alkalmazni (fekvőbeteg osztályok, krónikus rehabilitáció, stb.) Emiatt, és a fentiekben összefoglaltak okán *elmondható, hogy a kamerás megfigyelés (az elhelyezésnél az ombudsmani ajánlásokban és a jogszabályban foglaltakat maximálisan betartva) a betegforgalom által érintett területeken az utólagos azonosításra, a folyamatban lévő bűnesetek észlelésére, megszakítására rendkívül korlátozottan használható, a belépési jogosultság megállapítására pedig kórházak esetében egy-két nyilvánvaló esettől eltekintve egyáltalán nem alkalmas*. [6/p.159]

Bár elképzelhető, hogy a védelmi szakmában néhányan vitatni fogják az állítás helyességét, de az ismertetett okokból és a jelenleg rendelkezésemre álló statisztikák alapján a kórházak területén az egyébként igen költséges elektronikus megfigyelőrendszerek kiépítése helyett szükségszerűen a gyakorlatban jobban működő védelmi módszerekre kellene koncentrálnunk. A teljes igazsághoz az is hozzátartozik, hogy a magyarországi intézmények csak egy korlátozott számát érintően rendelkezem statisztikai adatokkal arról, hogy az ismertté vált bűnesetek tekintetében mennyinél volt szerepe a területen működő kamerarendszernek akár a megszakításban, akár az utólagos rekonstrukcióban, és természetesen nem lehet számszerűsíteni a rendszerek demonstratív (és ez által prevenciós célokat szolgáló) jellegéből származó bűnalkalmak elmaradást sem. Jelenleg azonban egy kórházbiztonsági kutatás keretén belül széleskörű adatgyűjtés van folyamatban fentiek minden kétséget kizáró megerősítésére (adott esetben cáfolatára).

MEGÁLLAPÍTÁSOK

A személy- és vagyonvédelem általános eszköz és eljárásrendszerének egyes elemei kórházak tekintetében nem, vagy csak részben alkalmazhatók, és egyes módszerekről éppen azért mondunk le, hogy ne gátoljuk az alapfeladat hatékony ellátását, illetve hogy tiszteletben tartsuk a testi – lelki egészséghez és az emberi méltósághoz való jogot, továbbá biztosítsuk a személyes adatok védelmét. Ha már újra az alapjogokat érintjük, joggal merülhetnek fel a következő kérdések is:

- A kórházak erősen nyitott jellege miatt valójában tud érvényesülni a testi és lelki egészséghez továbbá a gyógyulást támogató, egészséges környezethez való jog?
- Az intézmények speciális célrendszeréből adódóan területükön sok a szenzitív, különleges adat (kórlapok, betegnyilvántartások, stb.) Nem a személyes adatok védelmének egyik alapvető követelménye lenne, hogy a jogosulatlan megismerés megakadályozása érdekében illetéktelenek számára a hozzáférést a lehető legjobban korlátozzuk?

Fentiekhez hasonló kérdések még szép számmal feltehetőek, de egy dolog biztos: a védelmi szakmának folyamatosan olyan alternatív és ellensúlyozó intézkedésként alkalmas megoldások kifejlesztésén és implementálásán kell dolgoznia, amellyel hatékonyan biztosítható ezen kiemelt fontosságú intézményrendszerünk védelme.

AZ ŐRSZEMÉLYZET KIBŐVÜLT FELADATRENDSZERE

A személy- és vagyonvédelmet személyesen ellátók fő tevékenységi körébe „klasszikusan” a kórházi objektum működési rendjének fenntartása, a betegek- látogatók és az ellátásukat biztosító személyzet biztonsága, a dolgozók és a szolgáltatást igénybe vevők értéktárgyainak védelme tartozik. Azonban napjainkban az őrszemélyzet feladatrendszere lényegesen kibővült, a megrendelők a szolgáltatási szerződésben egyre több követelményt állítanak, melynek oka sok esetben az, hogy a lehető legtöbb biztonsági jellegű feladat ellátását szeretnék részben vagy egészben „letudni” egy szolgáltatási szerződés keretén belül, függetlenül annak jellegétől és fajtájától. Már a kilencvenes évek végén világot látott, „Az európai biztonsági őri alapképzés kézikönyve” c. kiadvány [13] is kifejti, hogy az alapképzésben részesült biztonsági őr feladatainak részét képezheti - felelősségének határain belül – többek közt az egészségre és biztonságra ártalmas veszélyek elhárítása, illetve annak jelentése.[4]

Az egészségügyi szolgáltatás (és azon belül is kiemelten a kórházak) társadalomra gyakorolt hatása igen jelentős, ezzel összhangban pedig a védelmét ellátóknak egyes magánszektorbeli tevékenységektől eltérő szintű, emelt (szakmai és személyes) követelményeknek kell megfelelniük. Ennek egyik oka, hogy az egészségügyi ellátó hálózat, illetve annak egyes elemei deklaráltan a kritikus infrastruktúra részét képezik, magával vonva annak speciális védelmi szabályozását és alapelveit, melyet a védelmet ellátóknak el kell sajátítaniuk. Másrészt sok esetben a szolgáltatást igénybevevők személyes biztonsággal kapcsolatos prioritásában - amelynek biztosítására a „klasszikus” feladatellátás irányul - az esetleges anyagi veszteség jelentéktelen ahhoz az érzelmi, lelki és fizikai hátrányhoz képest, amely egy nem megfelelően védett környezetben érheti őket (még akkor is, ha adott esetben ezt ők maguk nem is ismerik fel), és ezt a tényt a szolgálat ellátásakor és a védelem megszervezésekor folyamatosan szem előtt kell tartani.

[4] Maga a jelenség nem új, a biztonsági őr képzés azonban nem feltétlenül követi minden esetben naprakészen a megbízói igényeket.

Harmadrészt, a működési sajátosságok okán a szolgálatot ellátó szinte közterületen végzi a munkáját, ahol a folyamatosan változó személyi kör és védelmi helyzet mellett meg kell küzdenie a szolgáltatást igénybe vevők személyes érzelmi és fizikai állapotából származó nehézségekkel, és emiatt az átlagostól eltérő (vagy magasabb szintű) társas és személyes kompetenciákkal, intézkedési kultúrával kell rendelkeznie. Végül, de nem utolsósorban a kórházak működési sajátosságai okán az emlegetett kibővült vagyonvédelmi feladatrendszer és annak biztonságos ellátása széles körű ismeretek kíván a biztonságtechnika több részterületéről. Az őrzés-védelmi feladatot az eredeti rendeltetéssel együtt, attól elválaszthatatlanul, szoros kölcsönhatásban kell végezni,[5] a szolgálatellátás nem működhet vákuumban az érintett intézmény területén, így a tevékenységet végző annak speciális veszélyforrásai által ugyanúgy érintett. Ez az oka annak, amiért kellő szakmai ismeretek szükségesek ahhoz, hogy a védelmet ellátó maga ne legyen a biztonsági események negatív hatásainak passzív elszenvedője, esetleg okozója. Ahhoz, hogy munkáját biztonsággal és megfelelő szakmai színvonalon tudja ellátni, kórház területén legalább alapvető ismeretekkel kell rendelkezni az általános munkavédelmi és tűzvédelmi oktatáson felül többek közt a sugárvédelem alapvető feladatairól,[6] az egészségügyben oly lényeges infekciókontroll okán az egyes területek speciális higiénés, továbbá az egészségügyi gépek, berendezések, a hulladékkezelés alapvető biztonsági szabályairól, stb.

Az egészségügyi intézményben a szolgáltatást igénybe vevők fizikai – érzelmi (pszichikai) helyzete sajátos, több értelemben véve is. Amellett, hogy nagyobb arányban fordulhatnak elő (esetleg még nem diagnosztizált) pszichés megbetegedésben szenvedők a munkavégzés hatókörében, a kórházi célrendszer okán a látogatói kör általában is lényegesen eltér egy más funkciójú objektumtól, hiszen a legtöbbször az intézménybe érkezők egészségükben károsodott emberek (vagy az ő hozzátartozóik, akik sokszor hasonló viselkedési mintákat követnek). Az akár súlyos betegségben szenvedők speciális fizikai, de legfőképpen érzelmi állapota a környezeti ingerek megfelelő befogadóképességének hiányán túl messzemenőleg kihat az egyén interperszonális kapcsolataira, az észlelésben és az érzékelésben problémákat okoz, továbbá konfliktustűrő - kezelő képességeit is jelentősen befolyásolhatja, azokra negatív hatással lehet.[7] Minden esetben szem előtt kell tartani, hogy egy nem megfelelően kivitelezett intézkedés nagyban ronthat a beteg érzelmi állapotán, adott esetben kiszámíthatatlan reakciókhoz, és az elhárítani kívánttól is fokozottabb agresszióhoz vezethet. Ennek megelőzésére az őrszemélyzet részéről is szükség van felismerni és hatékonyan kezelni ezeket a konfliktusszituációkat,[8] továbbá a megváltozott érzelmi és fizikai állapotra való tekintettel a vagyonőri intézkedések minőségét eljárás-szakmailag „de humane” modernizálni szükséges,

[5] Kevés más olyan terület van, ahol az objektumban végzett őrzés – védelmi tevékenység ennyire szoros kapcsolatban lenne intézmény fő tevékenységével.

[6] Az egészségügyben széles körben alkalmaznak különböző radioaktív izotópokat, közöttük olyanokat is, amelyek alkalmasak arra, hogy piszkos bomba alapanyagaként szolgáljanak. Éppen ezért fontos feladat ezen anyagok eltulajdonítási, szabotálási kísérletének detektálása, megszakítása, a fizikai hozzáférés megakadályozása, továbbá a velük kapcsolatos rendkívüli helyzetek kezelése. Ezen feladatokkal kapcsolatban a védelmet ellátókra is jelentős szerep hárul(hat).

[7] 2010-ben a Személy-Vagyonvédelmi és Magánnyomozói Szakmai Kamara és a Zrínyi Miklós Nemzetvédelmi Egyetem hallgatóinak közreműködésével ajánlás készült az Uzsoki utcai kórház vagyonvédelmi tervéhez. Ennek keretében készült kérdőíves felmérések tapasztalatai alapján a megkérdezett kórházi dolgozók közül verbális és nem verbális erőszakos cselekedeteknek több, mint nyolcvan százalékuk volt elszenvedője. Bántalmazásnak tíz százalékuk, verbális erőszaknak több mint hetven százalékuk volt kitéve. [14] Ezen felmérés eredménye egybecseng egyébként azon nemzetközi szakmai fórumok megállapításaival, amelyek az egészségügy veszélyeztetettségét vizsgálják és értékelik többek közt a munkavállalókat ért verbális erőszak szempontjából.

[8] A már említett ajánlás része volt a szerző munkája, mely részleteiben foglalkozik a kórházi szolgáltatást igénybe vevők védelmi tudatosságának fejlesztési lehetőségeivel. A kutatómunka során pszichológus és kommunikációs szakemberek bevonásával került sor a lehetséges módszerek vizsgálatára és ajánlások megfogalmazására.

amely csak megfelelő fejlesztéssel, képzéssel, oktatással érhető el. A „problémás" viselkedési mintákat felismerve, és az adott helyzetben a szükséges kompetenciát tudatosan előtérbe helyezve (pl. fontosabbá válik a meggyőzés, a kompromisszumkészség, mint adott esetben a határozottság, stb.) lehet egyik záloga annak, hogy a személy – és vagyonőr intézkedése a konfliktusszituációk hatékony és erőszakmentes megoldását biztosítsa.

Az őrszemélyzet gyakori rotációja (amely a vagyonvédelmi szakmában általánosan ismert jelenség) egy kórház esetében, ha lehet ilyet mondani, még nagyobb problémákat jelenthet az objektum és a benne tartózkodó személyek biztonságának szempontjából, mint általában. A már említett célirányos képzés hiányában a szolgálatot adók legtöbbször gyakorlati tapasztalatok alapján szerzik meg a kórházi feladatellátáshoz szükséges kompetenciákat, a mindennapi munka során sajátítják el az intézmények védelmi jellemzőiből származó specialitásokat és tanulják meg valamilyen szinten kezelni a betegek, látogatók, érzelmi és fizikai állapotából származó konfliktushelyzeteket. [6/p.164] A helyes cselekvéssor bizonyos helyzetekben nem is tudatos, hanem a gyakorlatban beivódott „használható" viselkedési minta alkalmazása.[9]

Általánosan elfogadott vélekedés, hogy az őrzés-védelmet megvalósító személyek feladatain és kötelességein túl minden ember felelősséggel tartozik saját testi épségéért, anyagi javainak védelméért, és az adott körülmények közt minden tőle joggal elvárható intézkedést meg kell tegyen azért, hogy ne váljon bűnelkövetés áldozatává. Kórházi környezetben sokszor a betegek (esetleg az értük aggódók) fizikai és pszichés állapotukból adódóan nem, vagy csak korlátozott mértékben képesek az ilyen jellegű öngondoskodásra. Márpedig a legtöbb cselekményt (főleg tulajdon ellen, de személy elleni sem ritka) a betegek sérelmére éppen ott követik el, ahol azok egy része (elsősorban az intézményi fekvőbeteg ellátás során) - időszakosan - részben, vagy egészében cselekvőképtelen. Az anyagi veszteségen vagy a testi épség károsodásán túl a sérelmükre elkövetett (bűn)cselekmény pszichés hatása megrendítheti a kórházba vetett bizalmukat, és az átélt trauma akár súlyosan is visszavetheti a gyógyulásukat. Fentiek tükrében a védelmet ellátók személyi biztonságukért, jogaik maradéktalan érvényesüléséért erkölcsi felelősséggel is tartoznak, és e különleges felelősség fennáll mind az operatív feladatokat végzők, mind a védelmet szervezők tekintetében, [6/p.162-163] mindez pedig magával vonja a fejlett etikai - erkölcsi érzék és humánus beállítódás szükségességét részükről.

A pszichés mellett meg kell említetni az egyén fizikai állapotából származó azon sajátosságokat is, amelyek szintén jelentősen kihatnak a szolgálatellátásra. A kórházak ezen szempontból is tartogatnak sajátos veszélyforrásokat, hiszen a már sokat emlegetett célrendszer okán az intézmény látogatói közt gyakrabban fordulhat elő olyan (akár komoly, pl. HIV), fertőző beteg, akivel szemben ha intézkedés szükséges, a vagyonőr testi erő alkalmazása során egy karmolás, vagy harapás révén komoly egészségkárosító kockázatnak lehet kitéve. Egy irányító – recepciós feladatkörben foglalkoztatott pedig fizikai kontaktus nélkül is nagyobb kockázatnak van kitéve cseppfertőzéssel terjedő betegségeknek (influenza, TBC, stb.) az egészségügyben, mint például egy átlagos banki objektumban. A vagyonőrök mentési feladataik során sokszor mozgásukban és/vagy cselekvőképességükben korlátozott személyekkel találkoznak, de nagyobb hangsúly helyeződik az elsősegélynyújtás/újraélesztési képességek megszerzésére és szinten tartására, hiszen kórházi környezetben a gyakorlati alkalmazásra nagyobb eséllyel van szükség.

[9] A tudatos alkalmazásához komoly szakmai és személyiségfejlesztés szükséges.

ÖSSZEFOGLALÁS, JAVASLATOK

A bevezetőben feltett kérdésre, hogy mely, az általános elméleti gyakorlati ismeretekhez képest eltérő jellegű vagy eltérő szintű tudásanyagot kell elsajátítania, illetve mely készségekkel és kompetenciákkal kell(ene) rendelkeznie egy olyan vagyonőrnek, aki feladatát kórházi (egyéb egészségügyi) intézményben látja el, a válasz:

Az általános szakmai, jogi, gyakorlati, és etikai ismereteken túl

- speciális ismeretekkel kell rendelkezzen a biztonságtechnika részterületeit illetően,
- tisztában kell lennie az alapvető és a betegjogok tartalmával és azok gyakorlati értelmezésével kórházi környezetben,
- ismernie és alkalmaznia kell a hatályos adatvédelmi szabályozás előírásait,
- az átlagostól eltérő jellegű elméleti és gyakorlati pszichológiai és eljárás – módszertani továbbá egészségügyi ismeretekre van szüksége.

Gyakorlatilag a feladatellátáshoz szükséges összes kompetencia (szakmai, személyes, társas, módszertani, stb.), komplex fejlesztésére kell, hogy sor kerüljön a biztonsági őr képzés során. A képzési anyag összeállítása maga is sokrétű szakértelmet igényel, segítségül kell hívni a jog, a pszichológia, a viselkedéstudomány szakértőit, biztonságtechnikai szakembereket, de akár orvos, orvostechnológus, kórház – higiénés, egyéb gyakorlati kórházi szakember bevonására is sor kerülhet. Az így összeállított és megszerzett ismeretek birtokában a feladatot végző, képzett szakemberek minőségi garanciát jelenthetnek arra vonatkozóan, hogy a szolgálatellátás kielégítő szakmai színvonala biztosított, megfelel a kórházi célrendszerből támasztott speciális elvárásoknak.[10]

Természetesen tisztában vagyok vele, hogy a minőségi szolgáltatásnak ára van. A napjainkban tapasztalható rendkívül nyomott vállalási árral összefüggésben nem tudok nem kitérni a megrendelő azon felelősségére, mely szerint neki kellene igényeket, többletkövetelményeket támasztania és ezáltal a szolgáltatói oldalon elkötelezettséget generálnia a minőségi szolgálatellátásra vonatkozóan. Általánosságban is elmondható, de a napjainkban zajló gazdasági válság miatt különösen igaz, hogy tömegesen végeznek biztonsági őr tanfolyamot olyan személyek, akiknek ez a szakma sok esetben kényszerpálya, emiatt kellő motiváció nélkül fogják ellátni feladatukat és nem is éreznek igényt a minőségibb szolgálatellátásra, a szakmai ismereteik fejlesztésére, bővítésére. A szakma felelőssége többek közt abban áll, hogy szigorítsanak a képzési követelményeken, és nyújtsanak valós életpályát ezen szakmát hivatásszerűen választóknak.[11] Ezek lehetnek az első lépések, hogy a védelmi szakma oldaláról is sikeresen hozzátegyünk valamicskét az állampolgárok testi–lelki egészségének megőrzéséhez, helyreállításához.

Felhasznált irodalom

[1] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól https://magyarorszag.hu Letöltés ideje: 2012. 09.15

[2] Dió Mihály, dr. Forgács Lajos: Egészségügyi-kórháztechnikai alapfogalmak (3. rész) In: Orvos és kórháztechnika XLV. évf. 3. szám p.4 ISSN 1585-7360

[3] Magyarország Alaptörvénye https://magyarorszag.hu Letöltés ideje: 2012.09.14

[10] Természetesen ezzel összhangban ezen ismeretek oktatására menedzserszinten is sort kell keríteni, többek közt a felsőfokú biztonságszervező/biztonságtechnikai mérnökképzés keretén belül.

[11] Nem nehéz napjainkban olyan hirdetéssel találkozni, amely szerint a tanfolyamot választók akár hat - hét (!) nap alatt szert tehetnek a tevékenység személyes végzéséhez szükséges bizonyítványra.

[4] 1997. évi CLIV. törvény az egészségügyről https://magyarorszag.hu Letöltés ideje: 2012.09.14

[5] Az állampolgári jogok országgyűlési biztosának OBH 2985/1997. hivatkozási számú jelentése

[6] Tiszolczi Balázs Gergely: Kórházi objektumok védelmének sajátosságai In: *Bolyai Szemle* 2012. XXI. évf. 1. szám p.151-168 ISSN**:** 1416-1443

[7] Az állampolgári jogok országgyűlési biztosának OBH 4152/2002. hivatkozási számú jelentése

[8] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról https://magyarorszag.hu Letöltés ideje: 2012.09.15

[9] Az Adatvédelmi Biztos 2002-es beszámolója http://www.naih.hu/files/Adatvedelmi-biztos-beszamoloja-2002.PDF p.158-159 Letöltés ideje: 2012.09.04

[10] A megfigyelés, adatgyűjtés céljából üzemeltetett képfelvevő, -rögzítő berendezésekkel kapcsolatos adatvédelmi biztosi ajánlás http://abi.atlatszo.hu/index.php?menu=aktualis/archivum/ajanlasok&dok=9278 Letöltés ideje: 2012.09.05

[11] 1997. évi LXXVIII. törvény az épített környezet alakításáról és védelméről https://magyarorszag.hu Letöltés ideje: 2012.09.14

[12] Az adatvédelmi biztos 2572/K/2007-3 ügyszámon kiadott állásfoglalása

[13] Spaninks, Louis; Quinn, Larry; Byrne, John: Az európai biztonsági őri alapképzés kézikönyve 1999 december http://www.coess.org/_Uploads/dbsAttachedFiles/European_vocational_training_manual_basic_guarding_HU.pdf Letöltés ideje: 2012.09.01

[14] Deák Gabriella: Közvélemény kutatás. Az Uzsoki utcai Kórház alkalmazottainak körében elkövetett személy-, és vagyonvédelmi bűncselekmények bemutatása. Személy és vagyonvédelmi oktatás szükségességének felmérése. In: A Személy-Vagyonvédelmi és Magánnyomozói Szakmai Kamara és a Zrínyi Miklós Nemzetvédelmi Egyetem hallgatóinak közreműködésével készült ajánlás az Uzsoki utcai kórház vagyonvédelmi tervéhez.(2010)

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Árvai László
laszlo.arvai@gmail.com

PILÓTA NÉLKÜLI REPÜLŐGÉPEK FÖLDI ÁLLOMÁSAINAK TERVEZÉSI KÉRDÉSEI

Absztrakt

A pilóta nélküli repülőgépek biztonságos és hatékony üzemeltetéséhez a repülőeszközön kívül számos egyéb kiegészítő rendszerre van szükség. Ezek egyike a földi állomás, amely még két újabb fontos alegységre tagolható. Egyrészt tartalmaz bizonyos hardver komponenseket, másrészt pedig az ezeken futó, illetve az ezeket működtető szoftvereket. A földi állomás szoftverének számos elvárásnak kell megfelelnie – a teljesség igénye nélkül – könnyen kezelhetőnek, rugalmasnak, biztonságosnak, hatékonynak kell lennie. Szükséges, hogy egy ilyen szoftver fejlesztésének az első lépése gondos tervező munka legyen, hiszen csak így biztosítható a lehető legtöbb kívánalom a lehető legmagasabb szinten történő teljesítése. Egy ilyen tervezési folyamatot mutat be az a cikk.

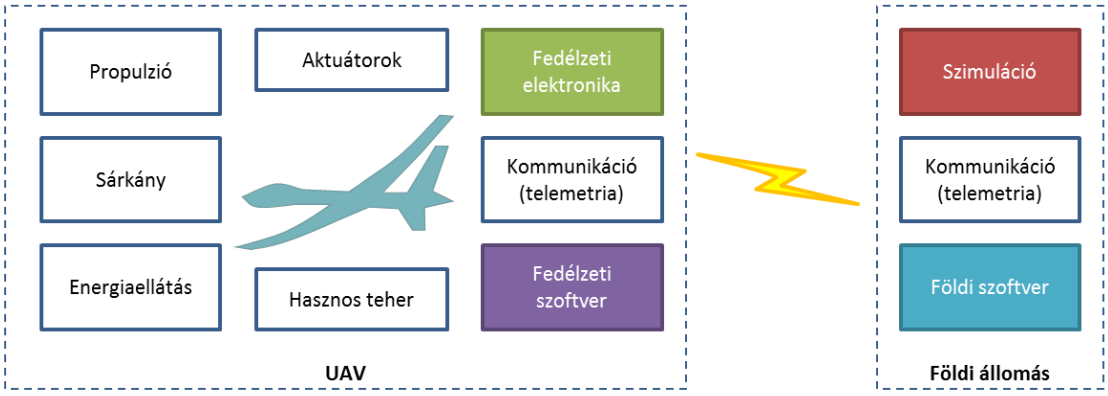
For the efficient and safe operation of any Unmanned Aerial Vehicle several auxiliary subsystems required than simply the aircraft itself. One of the required subsystems is the Ground Station. The Ground Station has at least two subsystems as well. It contains hardware components and software components running on it or operating the hardware components. There are several requirements for the ground station software - without mentioning all – it must be user friendly, flexible, safe and efficient. Therefore the first step of the development of the Ground Station Software must be a carefully executed design procedure otherwise the requirements can't be fulfilled at the highest level.

Kulcsszavak: *UAV, pilóta nélküli repülő eszköz, földi állomás, szoftvertervezés ~ UAV, software planning, ground station*

BEVEZETÉS

Egy pilóta nélküli repülőgép (UAV[1]) működéséhez számos rendszer harmonikus egységére van szükség. A legfontosabb összetevőket mutatja az 1. ábra.

A két legnagyobb rendszer egyike maga a repülőgép (vagy repülőeszköz) és az azon található fedélzeti rendszerek, a másik pedig a földi állomás (az egyéb, nem elektronikus rendszerek, mint például a földi kiszolgálás, logisztika, stb. tárgyalása már túlmutatna e cikk keretein, ezért csak a fontosabb elektronikus rendszereket tárgyaljuk). Az UAV és a földi állomás között természetesen vezeték nélküli kapcsolat áll fent, amely egyrészt szolgáltatja a telemetriás adatokat, másrészt lehetőség van a földi állomáson keresztül parancsokat adni, például módosítani a repülési pályáját. Természetesen a hasznos teher is igénybe veheti a kommunikációs csatornát (vagy rendelkezhet sajáttal is, amennyiben ez indokolt (például valós idejű video átvitel, mérési, megfigyelési adatok online sugárzása)).



1. ábra. Egy pilóta nélküli repülőgép fontosabb elemei

A földi állomás teszi lehetővé, hogy az operátor kommunikálhasson az esetleg már jelentős távolságban található repülőeszközzel, figyelemmel követhesse a működését, szükség esetén beavatkozhasson vagy akár át is vehesse az irányítást. Ezen kívül az UAV által gyűjtött adatok egy része vagy akár az egésze is megjeleníthető a földi állomáson, illetve a későbbi feldolgozásra szánt adatok tárolása, későbbi feldolgozása, megjelenítése is történhet ugyanitt.

Maga a földi állomás legalább két újabb alrendszerből áll. Áll egyrészt számos hardveregységből, másrészt az ezeken futó, illetve az ezeket üzemeltető szoftverekből. Csak ezen két rendszer hatékony együttműködése esetén végezhetők el azok a feladatok, amelyekkel egy földi állomásnak működése során meg kell birkóznia.

HELYBŐL FELSZÁLLÓ PILÓTA NÉLKÜLI REPÜLŐGÉP

A jelen cikkben ismertetendő UAV egy oktatási-kísérleti céllal fejlesztett berendezés. Ezért a földi állomással kapcsolatos követelmények is inkább ezt az irányt tükrözik, vagyis a megbízhatósági, robosztussági, mobilitási követelmények háttérbe kerülnek a rugalmasság, egyszerűség, alacsony költségek követelményeivel szemben.

A fejlesztési munka célja egy helyből felszállásra képes merevszárnyú, kísérleti repülőgép, illetve a működtetéséhez szükséges fedélzeti és földi összetevők prototípusának megalkotása. A feladat összetettsége miatt a munka két főbb folyamatra van osztva, melyek párhuzamosan futnak (2. ábra).

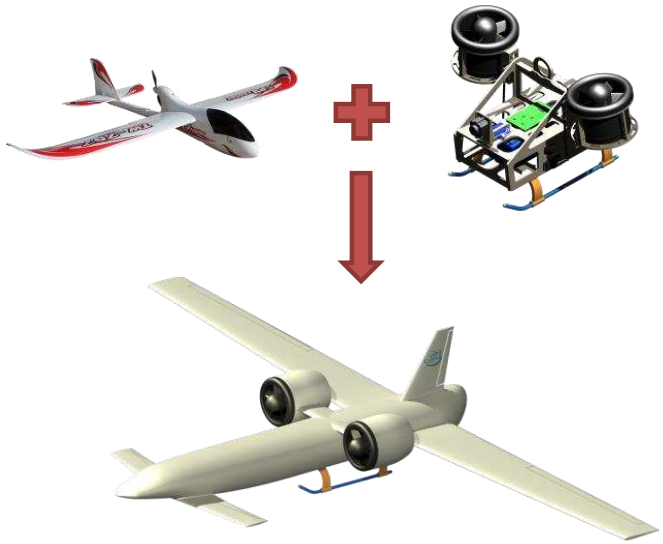
Egyrészt folyik a fedélzeti és földi összetevők fejlesztése egy hagyományosan fel- és leszálló, a kereskedelmi forgalomban készen kapható sárkányszerkezet segítségével. Ez a

[1] UAV - Unmanned Aerial Vehicle

gyakorlatban azt jelenti, hogy egy erre alkalmas repülőgépmodellt felszerelünk egy saját fejlesztésű, az automatikus repülést lehetővé tevő fedélzeti elektronikával, továbbá elkészítjük a működtetéséhez szükséges egyéb komponenseket (pl. földi állomás).

A fejlesztés másik iránya egy helyből felszállásra képes, egyedi tervezésű sárkányszerkezettel rendelkező, de még szárnyak nélküli repülőeszköz megalkotása. Ezen a fedélzeti elektronika továbbfejleszthető, illetve a helyből felszállás (függeszkedés) irányítástechnikai jellemzői vizsgálhatók.

Az utolsó lépés a két fejlesztési irány végén előállt eredmények (hardver, szoftver) egyesítése és egy végleges sárkányszerkezetbe integrálása, illetve az új rendszer tesztelése, hangolása.



2. ábra. Helyből felszálló pilóta nélküli repülőgép fejlesztési folyamata

Az előbbiekből következően a földi állomásnak képesnek kell lennie többféle, akár jelentősen eltérő repülőeszköz működtetésére és az ezekkel kapcsolatos fejlesztési feladatok támogatására.

FÖLDI ÁLLOMÁS TULAJDONSÁGAI, FELADATAI

A földi állomásnak számos feladatot kell ellátnia. Ezek jelen esetben két fő kategóriába oszthatók. Egyrészt képesnek kell lennie az UAV üzemeltetésére, másrészt pedig lehetőség szerint minél jobban támogatnia a kell a fejlesztési munkákat. Az üzemeltetéssel kapcsolatos fontosabb feladatok:

- Kommunikáció (telemetria, irányítás, hasznos teher)
- Adatok megjelenítése, vizualizálása
- Felhasználói, kezelői beavatkozások kezelése
- Hasznos teher működtetése
- Küldetéstervezés, útvonaltervezés és követés

Kommunikáció – a megfelelő hardverelemek (pl. rádió modem) felhasználásával kapcsolatot tart a fedélzeti rendszerekkel, akár több repülőeszközzel egyidejűleg. A kapcsolat kétirányú, a földi állomáshoz érkeznek a telemetriás adatok (fontosabb repülési adatok, működést leíró állapot információk), illetve a hasznos teherről származó adatok (pl. kép, hang). A repülőgép felé haladnak az irányítással kapcsolatos parancsok (pl. útvonal módosítás, kézi vezérlés), illetve a hasznos teher működtetésével kapcsolatos parancsok (pl. fedélzeti kamera beállításának módosítása).

Vizualizáció – a pilóta nélküli repülőgépről érkező adatokat könnyen áttekinthető formában megjeleníti. A megjelenítendő adatok lehetnek telemetriás és a hasznos tehertől származó adatok egyaránt. A megjelenítéshez felhasználhat helyi vagy távoli adatbázisokat (pl. térképek, időjárás adatok)

Kezelői beavatkozások – jelen esetben elvárás az UAV minél szélesebb körű automatikus működése, de ennek ellenére elkerülhetetlen, hogy az operator is be tudjon avatkozni a küldetésbe. A beavatkozás történhet magas szinten az automatikus működést nem befolyásolva (pl. útvonal módosítása) vagy történhet egészen alacsony szinten (pl. irányítás átvétele kézi üzemmódba).

Hasznos teher működtetése – amennyiben szükséges, a hasznos teher működtetését is célszerűen a földi állomás látja el. Ez a hasznos teher jellegétől függően lehet egészen egyszerű, de lehet bonyolult, összetett vezérlést kívánó feladat.

Útvonaltervezés – a földi állomásnak alkalmasnak kell lennie a küldetés megtervezésére, ami a tervezett repülési útvonal megtervezésével (térképes támogatással) és az egyes helyeken végrehajtandó feladatok megadásával történik. Természetesen már tervezéskor érdemes számolni az UAV hatótávolságával, domborzati viszonyokkal, időjárással, vészhelyzetekkel (pl. vészleszállóhely). A küldetést nyomon is kell követnie a már előzőekben említett telemetriás, vizualizációs modul segítségével.

Mivel egy kísérleti rendszerről van szó, azért nagyon fontos feladata a földi állomásnak a fejlesztési, tesztelési folyamat támogatása. Az ezzel kapcsolatos elvárások:

Rendszer paraméterek változtatása

- Rendszer monitorozás
- Szimulációs támogatás
- Rugalmasság, bővíthetőség

Rendszer paraméterek változtatása – lehetőséget kell biztosítania bizonyos fedélzeti rendszerparaméterek, szabályzási együtthatók változtatására, hangolására akár repülés közben is. Illetve ezek tárolására, gyors visszaállítására hibás beállítás esetén.

Rendszer monitorozás – feladata hasonló a már előzőekben említett vizualizációs funkcióhoz, azonban itt olyan belső paraméterek megjelenítéséről van szó, amelyek a repülőgép üzemeltetésekor nem bírnak különösebb jelentőséggel, de a fejlesztés, hibakeresés során fontos információkkal szolgálhatnak.

Szimulációs támogatás – a földi állomás felelős HIL[2]/SIL[3] szimulációs üzemmódban a szimulációs szoftver és az UAV közötti adatáramlásért. Ez a megoldás egyszerűbbé teszi a fedélzeti szoftver felépítését, hiszen az mindig csak a földi állomással kommunikál, a különböző szimulációs programokhoz tartozó egyedi illesztési módok a földi állomás szoftverében valósulnak meg.

Rugalmasság, bővíthetőség – a fejlesztési munka során sokszor szükség van olyan funkciókra is, amelyekre az üzemeltetés során nincs, vagy nem feltétlenül van szükség és ezek a funkciók a fejlesztési munka során folyamatosan változhatnak. Ezért fontos, hogy új funkciók (illetve a már létezők) módosítása gyorsan és könnyen elvégezhető legyen az egész rendszert érintő változások nélkül.

Több földi állomás elérhető nyílt forráskódban is. A teljesség igénye nélkül, néhány elterjedtebb, nyílt forráskódú rendszer: ArduPilot Mega Mission Planner [1], Paparazzi Ground Station [2], QGroundControl [3], HK Ground Control Station [4]. Kézenfekvőnek tűnik ezek közül valamelyik használata, de egyik sem annyira rugalmas és bővíthető, mint ami a kívánalmak között szerepel. Ezért célszerű egy saját tervezésű és fejlesztésű földi állomást készíteni. Ehhez első lépésben a felépítését kell megtervezni.

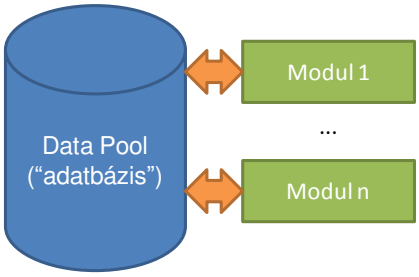
[2] HIL – Hardware In the Loop
[3] SIL – Software In the Loop

A FÖLDI ÁLLOMÁS FELÉPÍTÉSE

A földi állomás természetesen egyaránt tartalmaz hardver és szoftver elemeket is. A hardver elemek egyrészt egy IBM PC kompatibilis számítógépet tartalmaznak, illetve a hozzá csatlakoztatott egyéb kiegészítő elemeket. Ilyenek például a különböző kommunikációs interfészek, rádiós modemek vagy rádióvevők, antennakövető rendszerek, irány és helyzet meghatározó elemek, illetve egyéb kiegészítő egységek. A részletesebb ismertetésük – hely hiányában – nem része e cikknek, ezért a továbbiakban csak a földi állomás szoftverének felépítésével foglalkozunk.

A szoftver a rugalmas felépítés érdekében moduláris felépítésű. A modulokat egy keretrendszer fogja össze. A keretrendszer feladatai a következők:

- Modulok betöltése és futtatása. Minden modul külön DLL[4]-be kerül lefordításra, így futásidőben is szabadon be- és kivehetők a keretrendszerből.
- Képernyő felosztása a modulok között. A képernyőn minden modul számára saját terület jelölhető ki, az egyes elrendezések (layout) elmenthetők és tetszőleges időpontban visszatölthetők.
- Egységes konfigurációs felületet nyújtása a modulok részére, konfigurációk mentése, visszatöltése.
- Modulok közötti kommunikáció. A modulok közötti kommunikáció egy közös valós idejű adatbázison (data pool) keresztül történik. Ebben bármelyik modul helyezhet el adatokat (azok leírásával együtt), aktualizálhatja és szabadon elérheti őket.



3. ábra. Modulok közötti kommunikáció

A moduláris felépítéssel, illetve a modulok közötti kommunikáció előbb említett kialakításával elérhető, hogy egy modul megváltoztatása vagy egy új modul hozzáadása ne legyen hatással a teljes rendszerre. Másrészt előnye ennek a megoldásnak, hogy minden belső adat rendelkezésre áll egy helyen, így ez könnyen megjeleníthető, tárolható, elemezhető például diagnosztikai céllal.

A teljes földi állomás a keretrendszeren kívül számos modulból állhat. Ezek közül néhány fontosabb modul rövid ismertetésére kerül sor a következőkben.

KOMMUNIKÁCIÓS MODUL

A kommunikációs modul feladata a kétirányú adatkommunikációs kapcsolat fenntartása az UAV-al, lehetőség szerint repülés közben is. Ehhez természetesen valamilyen vezeték nélküli (pl. rádiós) adatátviteli egységre (modemre) van szükség az ehhez kapcsolódó antennákra (esetleg követő rendszerrel), illetve a megfelelő kommunikációs protokollokra. Ez utóbbi kivételével mindent a földi állomás hardvere tartalmaz, így ezek ismertetésétől most eltekintünk.

[4] DLL – Dynamic Link Library

A kommunikációs protokoll alsóbb rétegei (a média réteg az OSI értelmezés szerint) szintén a hardver (modem) szinten kerülnek megvalósításra. A kommunikációs modulban csak a felsőbb (csomóponti) rétegek kerülnek implementálásra.

A kommunikáció csomagokban történik, a csomagok adattartalmát pedig egy XML[5] fájl segítségével lehet meghatározni. Az XML fájlból egy megfelelő segédprogrammal egy C nyelvű az adott adatstruktúrát leíró deklarációkat tartalmazó fájl is előállítható, így a kommunikációs protokoll adattartalma a nélkül változtatható, hogy ez jelentős programozási munkával járna, illetve mivel a földi állomás kommunikációs moduljában ezek a konfigurációs fájlok cserélhetők, így könnyen állítható át a rendszer az egyik kommunikációs protokollról a másikra.

VIRTUÁLIS MŰSZERFAL MODUL

A virtuális műszerfal felelős a legfontosabb telemetriás adatok könnyen áttekinthető, értelmezhető megjelenítésért. Ehhez a hagyományos (és a repülésben elterjedt) műszerekhez hasonló megjelenítés szükséges, vagyis a már megszokott műszereket kell virtuálisan (a számítógép képernyőjén) megjeleníteni.

A rugalmasság, illetve a fejlesztés megkönnyítése érdekében nem érdemes minden műszerhez tartozó programot egyedileg elkészíteni. Sokkal egyszerűbb kialakítani egy olyan leíró nyelvet, aminek segítségével a műszerek megjelenése és működése közvetlenül leírható különösebb programozói tudás nélkül. Mivel a XML igen elterjedt különböző adatstruktúrák leírására célszerű egy XML alapú leírónyelvet létrehozni, amelynek segítésével szinte tetszőleges virtuális műszer létrehozható. A következő ábrán (4. ábra) egy sebességmérő műszerhez tartozó XML kód látható.

```
<?xml version="1.0"?>
<dashboard>
    <!-- ** Variables ** -->
    <variables>
      <variable Name="Airspeed" Min="0" Max="80"/>
    </variables>

    <!-- ** Mappers ** -->
    <mappers>
      <linear Name="Airspeed_Angle" Variable="Airspeed" Min="-160" Max="160"/>
    </mappers>

    <!-- ** Transformation ** -->
    <transformations>
        <!-- Airspeed transformation -->
        <transformation Name="Airspeed_Transformation">
          <rotate Angle="Airspeed_Angle" OriginLeft="0" OriginTop="-11"/>
        </transformation>
     </transformations>

    <!-- ** Instruments ** -->
    <instruments>
      <!-- Airspeed Indicator -->
      <instrument Left="5" Top="5">
        <bitmap Source="airspeed_background.png"/>
        <line Transformation="Airspeed_Transformation" Left="89" Top="100" Width="0" Height="-80" PenColor="White" PenWidth="3"/>
      </instrument>
    </instruments>
</dashboard>
```

4. ábra. Sebességmérő műszer XML kódja

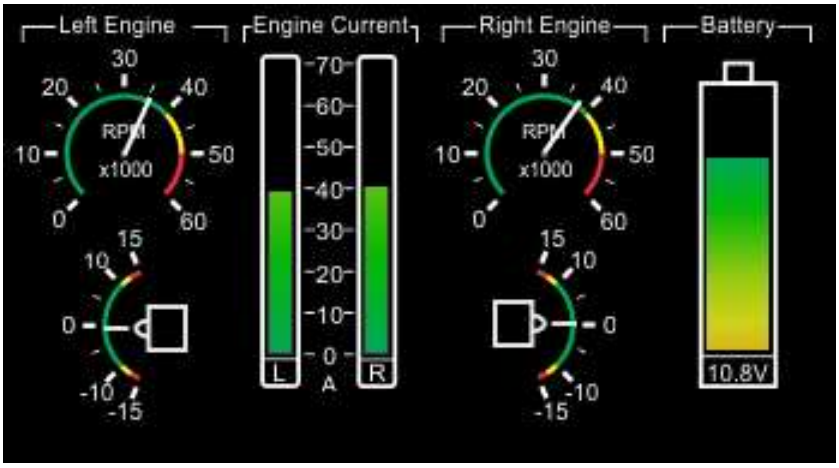
Terjedelmi okokból kifolyólag, a részletes ismertetést mellőzve, látható, hogy a kódban néhány sor megírásával egy működő és fontosabb paramétereit tekintve egyszerűen változtatható műszer hozható létre. Természetesen nem csak egy, hanem több műszer is definiálható, így létrehozható egy teljes virtuális műszerfal (5. ábra).

[5] XML – Extensible Markup Language

5. ábra. Virtuális műszerfal

Ezen a virtuális műszerfalon a 'szokásos' műszerek láthatók, (lég)sebességmérő, műhorizont, magasságmérő, elfordulás- és dőlésmérő, iránytű és függőleges sebességmérő.

Lehetőség van természetesen a szokásos kinézetű műszerek mellett modernebb, 'glass cookpit' jellegű műszerek definiálására is, ahogy ez a következő ábrán (6. ábra) látható.



6. ábra. Motor ellenőrző műszerek

Ezek a műszerek például a cikkben szereplő helyből felszálló repülőgép motor ellenőrző műszerei lehetnek. Látható a fordulatszám, hajtómű elfordítási szög, felvett áramok és az akkumulátor töltöttségét (kapocsfeszültségét) jelző műszer.

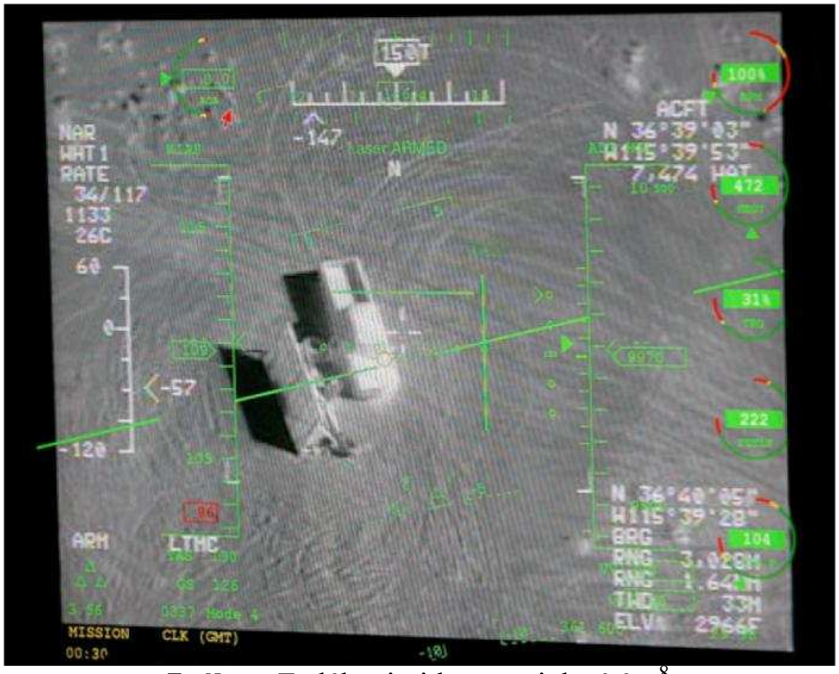
VIDEO MODUL

A video modul feladata a fedélzeti kamera képének fogadása, megjelenítése, rögzítése.A megjelenítéshez célszerű a képen elhelyezni a legfontosabb telemetriás adatokat, hasonlóan a repülőgépek HUD[6]-jához (6. ábra), így az amúgy is korlátozott méretű képernyő hatékonyabban használható ki. Az itt megjelenítendő adatokat a virtuális műszerfalhoz hasonlóan egy XML fájl segítségével lehet leírni.

Természetesen szükséges lehet a video rögzítése a későbbi visszajátszás érdekében. A rögzített videóba a HUD képe nem kerül bele, mert a HUD megjelenítéséhez szükséges telemetriás adatok egyébként is rendelkezésre állnak, illetve később a fedélzeti adatrögzítőből

[6] HUD – Head Up Display

is kinyerhetők. Azért, hogy a videojelfolyamot a telemetriás adatokkal szinkronban lehessen kezelni, a fedélzeti videó továbbító rendszer az egyébként nem használt hangcsatorán FSK[7] modulációval elhelyez egy időbélyeget, mely a videó jelfolyam részeként rögzítésre kerül. Így később bármikor újra felépíthető a HUD vagy a video mellett szinkronizáltan megtekinthetők a telemetriás adatok.



7. ábra. Fedélzeti video megjelenítése[8]

A 7. ábra egy lehetséges video megjelenítést mutat. Az ábrán látható a fedélzeti kamera képe és az arra ráhelyezett HUD szerű adatkijelzés.

TÉRKÉP, ÚTVONALTERVEZŐ MODUL

Nagyon fontos eleme a teljes rendszernek a GIS alapokon nyugvó útvonaltervező és követő modul.

Minden küldetés első lépése a tervezés. Definiálni kell az egyes célterületeket, az ott végrehajtandó feladatokat és meg kell tervezni a célterületek közötti útvonalat is. Eközben természetesen figyelemmel kell lenni a földfelszín magasságára (UAV repülési magassága), az útvonal hosszára (UAV hatótávolsága), számolni kell a le és felszállóhelyekkel (vészhelyzet esetére is), esetleg az időjárásra és alternatív útvonalakra is. Természetesen az így megtervezett útvonalak elmenthetők és később újra felhasználhatók, módosíthatók. Szintén a modul feladata a küldetés nyomonkövetése, a valós idejű vagy tárolt telemetriás adatok alapján az UAV megjelenítése térképeken vagy akár 3D-s virtuális térben.

DIAGNOSZTIKAI MODUL

Az UAV fejlesztése (de akár a karbantartása esetén) is hasznos segítséget nyújthat egy olyan modul, ami a fedélzeti repülésvezérlő elektronika bizonyos belső változónak a pillanatnyi értékét vagy ennek bizonyos (pl. idő szerinti) függését ábrázolja. Ennek segítségével a rendszer belső működése is figyelemmel kísérhető, az esetleges hibák, meghibásodások könnyebben felderíthetők. A 8. ábra egy ilyen lehetséges megjelenítése mutat.

[7] FSK – Frequency Shift Keying
[8] http://uihfes.files.wordpress.com/2010/03/hud.png

8. ábra. Diagnosztikai modul[9]

Az ábrán egyaránt szerepelnek numerikus értékek, illetve grafikonon megjelenített paraméterek.

Azért, hogy ez a kijelzés is könnyen módosítható, változtatható legyen a megjelenítendő adatok, diagramok a már szokásos XML fájl segítségével definiálhatók.

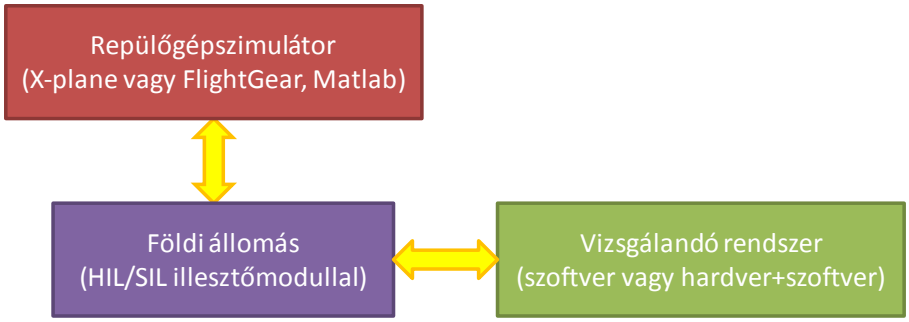
Eddig még nem került említésre, de az XML jellegű leírásnak van egy további előnye. Akár többféle megjelenítés is megtervezhető előre és ezek egyetlen mozdulattal (egy másik XML fájl betöltésével) cserélhetők, akár működés közben is.

HIL MODULOK

A HIL/SIL[10] modulok feladata a földi állomás illesztése a különböző szimulációs szoftverekhez.

A HIL/SIL szimulációk lényege a teljes szoftver (SIL) vagy hardver és szoftver együttesen (HIL) rendszer (beleértve a fedélzeti szoftvereket is) minél nagyobb részének tesztelése, tényleges repülés nélkül. A repülőgép csak egy virtuális térben repül egy szimulációs szoftverben, viszont a szimuláció pontosan azokat a beavatkozó jeleket kapja, amit a tényleges repülőgép kormányszervei kapnának, illetve (a szimuláció pontosságától függően) a valóságos repülőgéppel azonos válaszokat ad a beavatkozó jelekre.

A szimuláció során használt adatfolyamot a következő ábra (9. ábra) mutatja.



9. ábra. HIL/SIL szimuláció adatfolyama

A szimulátor bár közvetlenül kommunikálhatna a fedélzeti rendszerekkel, de ez nem minden esetben valósítható meg egyszerűn a fedélzeti (beágyazott) rendszerek korlátozott erőforrásai miatt. Célszerűbb kiegészíteni a telemetria-vezérlést megvalósító protokollt, amely

[9] http://wiki.ardupilot-mega.googlecode.com/git/images/ArduPilotMegaImages/QGC_Engineer.png
[10] HIL – Hardware Int he Loop, SIL – Software Int he Loop

egyébként is létezik a földi állomás és a repülőgép között. Így a különböző szimulációs programokhoz történő illesztés a földi állomásban történik, ahol jóval nagyobb erőforrások állnak rendelkezésre.

ÖSSZEFOGLALÁS

A földi állomás szoftvere egy rendkívül összetett rendszer, számos kívánalomnak kell megfelelnie, mint például a könnyű kezelhetőség, rugalmasság, bővíthetőség, könnyű karbantarthatóság. Ezen kívánalmak mindegyike csak úgy teljesíthető, ha az implementálást gondos tervezési munka előzi meg. A teljes rendszer modulokra bontásával, az egyes modulok minél általánosabb felépítésével és XML fájlok által történő testreszabásával, illetve a modulok közötti valós idejű, adatbázis alapú kommunikáció segítségével olyan rendszer alakítható ki, amely hosszú távon szolgálhat szinte tetszőleges pilóta nélküli repülőgép földi állomásaként.

Felhasznált irodalom

[1] ArduPilot Mega Mission Planner (Letöltve: 2013. január 12.) http://www.ardupilot.co.uk/

[2] Paparazzi Ground Control Station (Letöltve: 2013. január 10.) http://paparazzi.enac.fr/wiki/GCS

[3] QGroundControl (Letöltve: 2013. január 10.) http://qgroundcontrol.org/

[4] HK Ground Control Station (Letöltve: 2013. január 10.) http://code.google.com/p/happykillmore-gcs/

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Gyarmati József
gyarmati.jozsef@uni-nke.hu

KRITIKUS INFRASTUKTÚRA MODELLEZÉSE DÖNTÉSELMÉLET ÉS JÁTÉKELMÉLET SEGÍTSÉGÉVEL[1]

Absztrakt

A cikk kritikus infrastruktúra modellezésére alkalmas módszereket mutat be. A matematikai modellek alkalmazása gyakorlati példákon keresztül kerülnek bemutatásra. A példák döntéselmélet és játékelmélet segítségével vannak megoldva.

This paper shows eight models which are applicable for modeling critical infrastructure. Solving the problems decision theory and game theory was used. The paper shows the mathematical model and shows practical examples as well.

Kulcsszavak: *kritikus infrastruktúra, modellezés, játékelmélet, döntéselmélet ~ critical infrastructure, modeling, game theory, decision theory*

[1] A tanulmány a TÁMOP-4.2.1.B-11/2/KMR-2011-0001 számú Kritikus infrastruktúra védelmi kutatások című pályázat „Közlekedési kritikus infrastruktúra védelem” kiemelt kutatási terület támogatásával készült

BEVEZETÉS

A tanulmány célja olyan modellek összegyűjtése, amelyek segítségével matematikailag modellezhetővé válik a kritikus infrastruktúra védelme. A modellezés elsősorban azon esetekre vonatkozik, ahol a támadó, illetve a védett értéken rongáló nem intelligens, vagyis nem valamilyen természeti erő. A modellezés alapvető célja ennek megfelelően a védett rendszert támadó és az azt védeni próbáló üzemeltető cselekvéseinek leírása, valamint az egyes cselekvési változatokkal járó következmények, károk értékének előrejelzése.

1. DÖNTÉSELMÉLETI MEGKÖZELÍTÉS

Legyen egy védett objektum, amelyet az üzemeltető az optimális költségen kíván működtetni és legyen egy támadó, amely minél nagyobb kárt akar okozni. Kérdés: milyen mértékű erőforrást szánjon az üzemeltető a védelem kiépítésére és milyen mértékűt a támadó a legnagyobb kár okozás érdekében?

Definíciók

A döntéselméleti modell általános leírását az (1) egyenlet mutatja.

$$\begin{array}{ccccccc} & S_1 & S_2 & \dots & S_n & P(T_i) \\ T_1 & K_{11} & K_{12} & \dots & K_{1n} & P(T_1) \\ T_2 & K_{21} & K_{22} & \dots & K_{2n} & P(T_2) \\ \vdots & \vdots & \vdots & K_{ij} & \vdots & \vdots \\ T_m & K_{m1} & K_{m2} & \dots & K_{mn} & P(T_m) \end{array} \qquad (1)$$

$$\text{és } \sum_{i=1}^{m} P(T_i) = 1,\ i = 1 \dots m,\ j = 1 \dots n.$$

Ahol:

E: védett érték [Ft]

A támadásnak kitett objektum, rendszer, stb., pénzben kifejezett értéken.

S: védelmi szint [%]

Hány százalékkal képes a biztonsági rendszer csökkenteni a támadás hatását.

V: védelmi költség [Ft]

V = f(S, E)

Az adott védelmi szint eléréshez szükséges anyagi erőforrások pénzben kifejezve.

T: támadás [%]

Hány százalékban rombolja a támadó a védett értéket.

C: kár [Ft]

A védett értékben közvetlenül keletkező kár, valamint a védett érték károsodása miatt keletkező közvetett kár.

C = f(E, S, T)

K: összköltség [Ft]

K = C + V

$P(T_i)$ [-]

Adott T_i mértékű támadás bekövetkezésének a valószínűsége.

D_i Döntési kritérium. [-]

Azon szabály, amely alapján az üzemeltető (döntéshozó) választ az alternatívák közül.

1.1. Modell

A védelmi költség a védelmi szint lineáris függvénye:

$$V = m\,E\,S, \tag{2}$$

Ahol m iránytangens az arányossági tényező és $m \in \mathbf{R}^+$. Kifejezi, hogy a védelmi rendszer költsége 100%-os védelem esetén hányad része a védett értéknek.

A kár csak a védett értékben keletkezik közvetett hatások nincsenek. A kár ennek megfelelően a védelmi szint és a támadás lineáris függvénye:

$$C = E\,T\,(100\%\text{-}S) \tag{3}$$

A következmény értékét a (2) és a (3) egyenletekből a következő szerint kell számítani:

$$K_{ij}(T) = C_{ij} + V_{ij} = E{\cdot}T_i{\cdot}(100\%\text{-}S_j) + m{\cdot}E{\cdot}S_j. \tag{4}$$

A támadás bekövetkezéséről, annak várható nagyságáról a rendszer üzemeltetője részéről nem áll rendelkezésre semmilyen információ. A támadás nagysága és a védelmi szint nagysága között nincs összefüggés. (Azon eseteket ahol ez nem áll fenn játékelmélet segítségével lehet modellezni.)

A modell megoldása egy példán keresztül kerül bemutatásra. Legyen E = 100 [mFT], és m = 0,5.

		Védelmi szint			
		25,00%	50,00%	75,00%	100,00%
Támadás	25,00%	31,25	37,5	43,75	50
	50,00%	50	50	50	50
	75,00%	68,75	62,5	56,25	50
	100,00%	87,5	75	62,5	50
Maxi–max	W_j	31,25	37,5	43,75	50
Mini–max	w_j	87,5	75	62,5	50

1. táblázat. Az 1.1. modell döntési táblázata

A modellt a döntéselméletbe alkalmazott rendezés szerint döntési táblázatban mutatja be az 1. táblázat. A döntéshozó jelen esetben a rendszer üzemeltetője, a cselekvési változatait pedig az 1. táblázat oszlopai mutatják. A döntéshozónak a lehetséges védelmi szintek között kell választania. A kiválasztott cselevési változattól –a döntési modell feltételei szerint– függetlenül események következnek be, ez jelen esetben a bekövetkező támadás nagysága. A kiválasztott cselekvési változat, vagyis a rendszer üzemeltetője által meghatározott védelmi szint és a bekövetkező támadás nagysága együttes hatására létrejön a következmény, ami esetünkben a (4) egyenletekből van számítva.

Az üzemeltető számos stratégia szerint választhatja ki a cselekvési változatát. Elsőként tekintsük az un. maxi–max döntési elvet Szentpéteri (1980:36) szerint. Ez az elv egy teljes mértékben optimista döntéshozó gondolkodását írja el. Az optimizmus jelen esetben nem a döntéshozó személyes tulajdonságából fakad, hanem a körülmények csekélyebb mértékű támadásra engednek következtetni. A döntéshozó személyes jellemvonásait már csak azért sem célszerű figyelembe venni, mert a vizsgált helyzet un, csoportos döntési probléma. Nem egy személy üzemelteti a rendszert, hanem egy számos taggal rendelkező szervezet. A végső döntéseket a legtöbb esetben egy személy hozza meg ugyan, de a döntés meghozatala előtt

számos más személy véleménye kerül meghallgatásra, vagyis a döntésben több személy értékrendje információja és egyéb személyes attitűdje is szerepel.

A maxi–max elv esetén a döntéshozó feltételezi, hogy bárhogyan is dönt minden esetben a számára legkedvezőbb esemény, jelen esetben legkisebb mértékű támadás következik be. Például ha nem alakít ki védelmet evvel csökkentve a saját költségeit, akkor támadás sem lesz, ha teljes védelmet alakít ki, akkor a támadás is maximális mértékű lesz. A cselekvési változat kiválasztásához az 1. táblázat oszlopaiban meg kell keresni a maximális bevételt, jelen esetben a minimális kiadást:

$$W_j = \min_i\{K_{ij}\} \tag{5}$$

és az így képezett sorból kell kiválasztani a legkedvezőbb értéket, vagyis a maximális bevételt, esetünkben a minimális kiadást:

$$D_1^{\text{opt}} = \min_j\{W_j\} \tag{6}$$

Esetünkben ez az (5) egyenlet szerinti {31,25; 37,5; 43,75; 50} értékekből kiválasztott legkisebb, amit az 1. táblázatban pirossal jelölt érték mutat, mely szerint a legalacsonyabb védelmi szintet kell kialakítani. Figyelembe véve, hogy a védelmi költség lineáris függvény szerint lett képezve, a legkedvezőbb alternatíva, ha a rendszer üzemeltetője egyáltalán nem alakít ki védelmet.

A pesszimista döntéshozó arra számít, hogy minden lehetséges cselekvési változatához képest a legkedvezőtlenebb következményt indikáló esemény fog bekövetkezni. Az előző példát erre a döntési elvre érvényesítve, ha a rendszer üzemeltetője nem alakít ki védelmet, akkor maximális erejű támadás fog bekövetkezni. A cselekvési változat kiválasztásához most oszloponként a legkedvezőtlenebb következményt kell kiválasztani, vagyis a maximális költséget:

$$w_j = \max_i\{K_{ij}\} \tag{7}$$

és az így képzett sorból a legkisebbet:

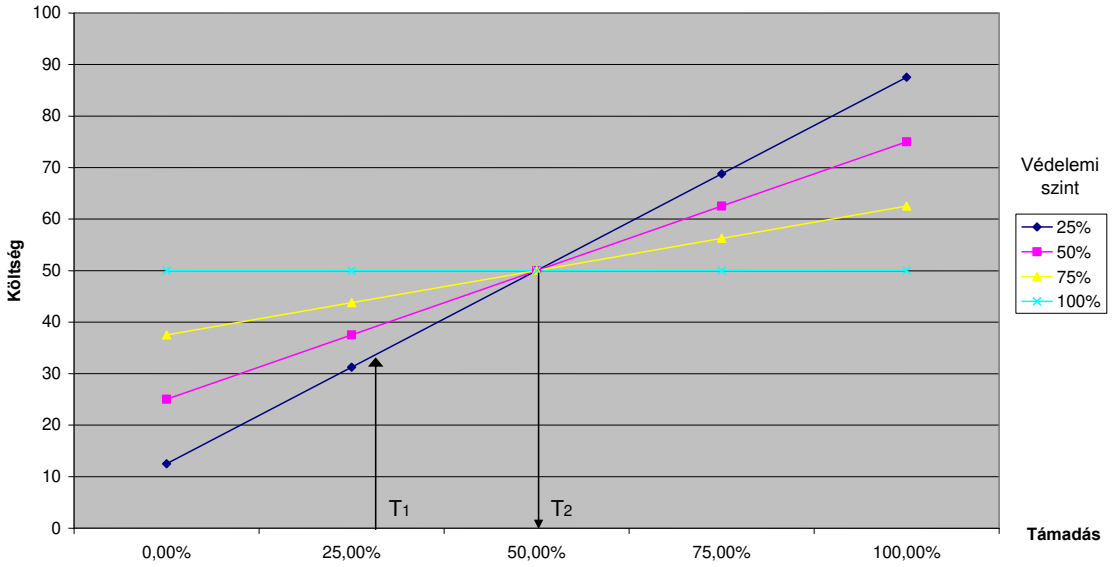
$$D_1^{\text{pesz}} = \min_j\{w_j\}. \tag{8}$$

A döntéselméletben ezt mini–max elvnek nevezik. Az 1. táblázatban kék színnel lett jelölve az így kiválasztott alternatíva.

A két döntési elv szerint a teljesen optimista nem alakít ki védelmet a teljesen pesszimista pedig maximális védelmet alakít ki. Természetesen ezen elvek szerint kiválasztott cselekvési változatokat szélsőségnek kell tekinteni, hiszen teljes mértékben optimista, illetve pesszimista döntéshozó gyakorlatilag nem létezik. Ezen jellemzők finomabb árnyalására alkalmazzák a döntéselméletben az un. Hurwitz kritériumot (Szentpéteri, 1980:37), amely egy $0 \le \alpha \le 1$szám segítségével állítja be az optimizmus mértékét és $\alpha = 1$, ha a döntéshozó teljes mértékben optimista. Jelen esetben ehhez egy nagyon hasonló megközelítést alkalmazunk, avval a különbséggel, hogy a döntéshozónak a veszélyeztetettség mértékétől függően a támadás nagyságát kell előre megjósolnia. A védelmi szinteket diszkrét értéknek és a támadás mértékét folytonosnak tekintve, az egyes védelmi szintekhez a (4) egyenlet szerint definiálható a következő függvény:

$$K_j(T) = C_j + V_j = E{\cdot}T{\cdot}(100\%\text{-}S_j) + m{\cdot}E{\cdot}S_j, \tag{9}$$

ahol T mint a támadás mértéke folytonosnak tekinthető, és az S_j a j-edik védelmi szint nagysága. Ennek megfelelően a lehetséges védelmi szintek számának megfelelő számú, vagyis j darab függvény képezhető. A függvényeket az 1. ábra mutatja.



1. ábra. Az 1.1. modell általános megoldása

A döntéshozónak arra a kérdésre kell válaszolni miszerint: „Milyen mértékben várható támadás?”; vagy „Milyen mértékű a veszélyeztetettség?”. A támadás várható nagysága által meghatározott helyen (1. ábra $T_1 = 30\%$) a legkisebb költségű cselekvési változat görbéjét kell választani, jelen esetben ez a minimális 25%-os védelmi szinthez tartozó görbe. Az 1. ábrából jól látható, hogy amennyiben $T > 50\%$ vagyis inkább vagyunk pesszimisták, akkor maximális védelem, ellenkező esetben minimális védelem szükséges. Általánosan:

$$D_1^{\text{ált}} = \min\{K_j(T)\}. \tag{10}$$

A (10) egyenlet szerinti döntési elv magába foglalja az előző két elvet is, ezért ez a modell mindhárom döntési elvet magába foglaló megoldásának is tekinthető.

1.2. Modell

A védelmi költség a védelmi szint lineáris függvénye:

$$V = m\,E\,S, \tag{11}$$

ahol m iránytangens az arányossági tényező és $m \in \mathbf{R}^+$. Kifejezi, hogy a védelmi rendszer költsége 100%-os védelem esetén hányad része a védett értéknek.

A kár csak a védett értékben keletkezik közvetett hatások nincsenek. A kár ennek megfelelően a védelmi szint és a támadás lineáris függvénye:

$$C = E\,T\,(100\%\text{-}S) \tag{12}$$

A támadás bekövetkezéséről információ áll rendelkezésre a $P(T_i)$ diszkrét valószínűségeloszlás formájában az (1) egyenlet szerint, de ez független a védelmi szinttől.

Az egyes események bekövetkezési valószínűségének ismeretében egyszerűen számítható minden cselekvési változat un. várható pénzértéke, ha a kiválasztott cselekvési változathoz tartozó minden következményértéket szorozzuk a hozzá tartozó valószínűséggel és a szorzatokat összegezzük:

$$M(K_j) = \Sigma_i K_{ij} P(T_i) \tag{13}$$

A legkedvezőbb alternatíva, amelynek a várható összköltsége a legkisebb, vagyis a várható érték sorából a legkisebb értéket kell választani. Képlettel megfogalmazva:

$$D_2{}^d = \min\{M(K_j)\}. \tag{14}$$

A modell megoldása példán keresztül: legyen E = 100 [mFT], és m = 0,5.

A valószínűségek $P(T_i)$ és $T_i \in \{25\%, 50\%, 75\%, 100\%\}$ ismeretében a döntési táblát a 2. táblázat mutatja.

			Védelmi szint			
		25,00%	50,00%	75,00%	100,00%	$P(T_i)$
Támadás	25,00%	31,25	37,5	43,75	50	0,1
	50,00%	50	50	50	50	0,4
	75,00%	68,75	62,5	56,25	50	0,3
	100,00%	87,5	75	62,5	50	0,2
	$M(K_i)$	61,25	57,5	53,75	50	
	$M_f(K_i)$	37,5	41,6	45,8	50	

2. táblázat. Az 1.2. modell döntési táblázata

Az eredmény 50 (pirossal kiemelve) és a kiválasztott alternatíva a maximális 100%-os védelem.

Amennyiben a támadás nagysága folytonos eloszlású, akkor a várható értéket a következő egyenlettel számíthatjuk Szentpéteri (1980:59) szerint:

$$M_f(K_j) = \int_0^1 K_j(T) f(T) dT, \tag{15}$$

ahol $f(T)$ az eloszlás sűrűségfüggvénye. Legyen az eloszlás sűrűségfüggvénye:

$$f(T) = c - m_T T \tag{16}$$

alakú lineáris függvény, ahol $m_T \in \mathbf{R}^-$, vagyis a sűrűségfüggvény szigorúan monoton csökkenő [0,1] vizsgált intervallumon belül és $\int_0^1 f(T) dT = 1$.

A (15) egyenletet a (9) és a (16) felhasználásával megoldva valamint behelyettesítve a 1.2. modell konstansait, az egyes védelmi szintekhez tartozó várható következmény értékeket a 2. táblázat utolsó sora mutatja. Csökkenő védelmi szinthez itt csökkenő összköltség tartozik, ami a választott eloszlás és a hozzá tartozó paraméter értékének tudható be.

1.3. Modell

A védelmi költség a védelmi szint négyzetes függvénye:

$$V = m_v E S^2, \tag{17}$$

ahol m_v arányossági tényező, és $m_v \in \mathbf{R}^+$.

A kár jelen esetben nem csak a védett értékben keletkezik, közvetett hatások is vannak, melyek négyzetesen arányosak a támadás mértékével:

$$C = m_T E (100\%-S)T^2 \quad (18)$$

ahol m_T arányossági tényező, és $m_T \in \mathbf{R}^+$.

A *j*-edik cselekvési változathoz tartozó összköltségek:

$$K_j(T) = m_v E S^2_j + m_T E (100\%-S_j)T^2. \quad (19)$$

A cselekvési változat kiválasztásához felhasználható az 1.1. modellnél bevezetett (6) és (8) egyenlet szerinti döntési kritérium. Az 1.1. modell (10) egyenlete szerinti elvet alkalmazva a döntési probléma itt is általánosítható:

$$D_3 = \min \{K_j(T)\} \quad (20)$$

ahol $0\% \leq T \leq 100\%$ és $S_j \in \{25\%, 50\%, 75\%, 100\%\}$.

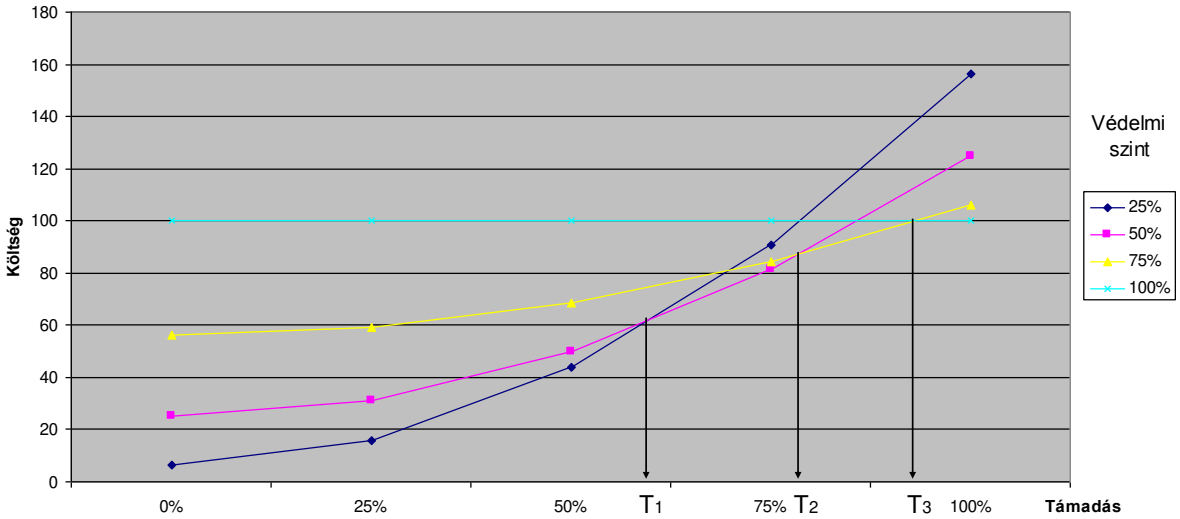
Egy példán keresztül bemutatva: legyen $m_v = 1$ és $m_T = 2$ és E = 100 mFT.

		Védelem			
		25,00%	50,00%	75,00%	100,00%
Támadás	0%	6,25	25	56,25	100
	25,00%	15,625	31,25	59,375	100
	50,00%	43,75	50	68,75	100
	75,00%	90,625	81,25	84,375	100
	100,00%	156,25	125	106,25	100
	W_j	6,25	25	56,25	100
	w_j	156,25	125	106,25	100

3. táblázat. Az 1.3. modell döntési táblázata

Az értékeket behelyettesítve az (19) egyenletbe a 3. táblázatot kapjuk.

A (6) és a (8) szerinti tisztán optimista és a tisztán pesszimista döntési kritérium alapján a döntéshozó rendre a minimális illetve a maximális védelmi szintet választja, amit a 3. táblázatban piros illetve kék szín jelöl. A megoldás általánosításához az értékeket behelyettesítve a (11) egyenletbe a 2. ábra szerinti $K_j(T)$ függvények adódnak.



2. ábra. Az 1.3. modell általános megoldása

A cselekvési változat kiválasztásához, vagyis a védelmi szint nagyságának a meghatározásához a (20) szerint a minimális értékű $K_j\ (T)$ függvényt kell megkeresni. A 2. ábrán jól látható, hogy a támadás nagyságának a függvényében változik a minimális értékeket tartalmazó függvény és a 0-100% támadási intervallumon belül mind a négy lehetséges védelmi szinthez kapcsolódó függvény minimumként jelenik meg. A négy függvény három metszéspontját ($T_1\ T_2\ T_3$) kell megkeresni, ahhoz hogy a védelmi szintet egyértelműen hozzá lehessen rendelni a támadás várható szintjéhez. A T_1 értéket a $K_{25\%}\ (T)= K_{50\%}\ (T)$, a T_2 értéket a $K_{50\%}\ (T)= K_{75\%}\ (T)$, a T_3 értéket pedig a $K_{75\%}\ (T)= K_{100\%}\ (T)$ egyenlet megoldásával. Az egyenleteket megoldva a

$$T_1 = 61\%,\ T_2 = 79\%,\ T_3 = 94\%,$$

értékek adódnak. Vagyis, ha a támadás elvárt mértéke $T < 61\%$ akkor 25%-os védelmet célszerű kialakítani, ha $61\% \le T < 79\%$ akkor 50%-os védelmet célszerű kialakítani, ha $79\% \le T < 94\%$ akkor 75%-os védelmet célszerű kialakítani, ha pedig $T > 94\%$ akkor 100%-os védelmet célszerű kialakítani.

1.4. Modell

A védelmi költség a védelmi szint négyzetes függvénye:

$$V = m_v\, E\, S^2, \tag{21}$$

ahol m_v arányossági tényező, és $m_v \in \mathbf{R}^+$.

A kár jelen esetben nem csak a védett értékben keletkezik, közvetett hatások is vannak, melyek négyzetesen arányosak a támadás mértékével:

$$C = m_T\, E\, (100\%-S) T^2 \tag{22}$$

ahol m_T arányossági tényező, $m_T \in \mathbf{R}^+$. és

$$K_{ij}(T) = C_{ij} + V_{ij} = m_T\, E\, (100\%-S_j)\, T_i^2 + m_v \cdot E \cdot S_j^2\ , \tag{23}$$

A támadás bekövetkezéséről információ áll rendelkezésre. Ismert a $P(T_i)$ diszkrét valószínűségeloszlás, ahol $T_i \in \{25\%, 50\%, 75\%, 100\%\}$. A modell megoldása a 1.2. modellnél leírtakkal egyezik meg eltérés csak a következményértékek számításában van.

$$M(K_j) = \Sigma_i K_{ij} P(T_i) \tag{24}$$

$$D_4 = \min\{M(K_j)\}. \tag{25}$$

A példán keresztüli bemutatáshoz felhasználva a 3. modell adatait és az 1.2. modell valószínűségeloszlását a 4. táblázat szerinti eredményekhez jutunk.

			Védelmi szint			
		25,00%	50,00%	75,00%	100,00%	$P(T_i)$
Támadás	25,00%	6,25	25	56,25	100	0,1
	50,00%	15,625	31,25	59,375	100	0,4
	75,00%	43,75	50	68,75	100	0,3
	100,00%	90,625	81,25	84,375	100	0,2
	$M(K_j)$	38,13	46,25	66,88	100	

4. táblázat. Az 1.4. modell döntési táblázata

A 4. táblázat szerint a legkisebb védelmi szint kiépítése látszik a legcélszerűbbnek, összevetve ez a 2. táblázat hasonló döntési modelljével megállapítható, hogy jelen esetben az ott megfigyelt kimenettel szemben teljesen ellenkező döntés meghozatala látszik célszerűnek. Ebből a megfigyelésből csak annyi következtetést célszerű levonni, miszerint az egyes védett objektumok jellege, a keletkező kár nagysága és a képzés formája a döntést akár teljes mértékben megváltoztathatja.

2. JÁTÉKELMÉLETI MEGKÖZELÍTÉS

Definíciók

Legyen A_1, A_2,… A_n védett objektum. A rendszer üzemeltetője korlátozott erőforrásokkal rendelkezik, amely csak az egyik objektum védelmét teszi lehetővé. A rendszert támadó szintén korlátozott erőforrásokkal rendelkezik, amely szintén csak egy objektum támadását teszi lehetővé. A támadó kiválaszt egy objektumot, amelyet megkísérel rongálni, és az üzemeltető is kiválaszt és védelemmel ellát egy objektumot. A két választás együttes hatására valamelyik objektumban valamilyen szintű kár keletkezik. A modell un. kifizetési táblázatát az 5. táblázat mutatja, ahol p_{ij} jelenti az i-edik, és egyben támadott objektumban keletkező kárt, ha az üzemeltető a j-edik objektumot védi és $i, j = 1,\ldots,n$, **x** és **y** vektorok tartalmazzák azon valószínűségeket, amellyel a támadó kiválasztja célpontját, illetve az üzemeltető kiválasztja a védett objektumot. A modellből egyértelműen következik, hogy p_{ij} ott éri el a minimumot, ha $i = j$.

		Üzemeltető			
		A_1	A_2	…	A_n	**x**
Támadó	A_1	p_{11}	p_{12}	…	p_{1n}	x_1
	A_2	p_{21}	p_{22}	…	p_{2n}	x_2
	A_n	p_{n1}	p_{n2}	…	p_{nn}	x_n
	y	y_1	y_2		y_n	

5. táblázat. Általános játékelméleti modell

2.1. Modell

A kifizetési tábla legyen a 6. táblázat szerinti. A táblázatból látható, hogy nincsenek az egyes alternatívákhoz rendelve valószínűségértékek. Mindkét fél rendelkezik a 6. táblázat információjával és mindkét félről feltételezhető, hogy racionálisan cselekszik, vagyis a Támadó maximálni–, az Üzemeltető pedig minimálni szeretné a kárt, továbbá mindketten ismerik az ellenfelük ezen célját.

		Üzemeltető		
		A_1	A_2	A_3
Támadó	A_1	1	3	3
	A_2	4	2	4
	A_3	8	8	4

6. táblázat. A 2.1 modell kifizetési táblázata

A 6. táblázat fődiagonálisa tartalmazza a soronkénti legkisebb elemet, ami azt mutatja, hogy akkor keletkezik a legkisebb kár, ha a támadó azt az objektumot támadja, amelyet az Üzemeltető védelemmel is ellát. A fődiagonálison kívüli elemek soronként azonosak, ami abból adódik, ha a támadó egy objektumot támad, de az üzemeltető nem azt védi, akkor már teljesen mindegy, hogy melyik objektum van ellátva védelemmel ugyanakkora kár keletkezik a támadott helyen. A modell így feltételezi az objektumok és a védelmi rendszerek függetlenségét.

A kifizetési táblázat a keletkezett kárt mutatja ennek megfelelően a támadó maximálni, míg az üzemeltető minimálni szeretne. Amennyiben a támadó oldaláról közelítünk észrevehető, hogy az A_3 objektum támadásához tartozó értékek {8, 8, 4} rendre nagyobban az A_1-hez {1, 3, 3} tartozókhoz képest. A támadó függetlenül az üzemeltető döntésétől, minden esetben nagyobb kárt okoz, ha az A_3 –at támadja. Az A_3 dominálja az A_1-et, tehát az A_1 a támadó cselekvési változataiból kizárható. A kifizetési táblázat a 7. táblázat szerint módosul.

Támadó \ Üzemeltető	A_1	A_2	A_3
A_2	4	2	4
A_3	8	8	**4**

7. táblázat. A 2.1. modell módosított kifizetési táblázata

Az üzemeltető viszont ugyanevvel az információval rendelkezik, vagyis Ő is látja, hogy a támadó A_1-et semmiképpen nem fogja támadni ezért a 7. táblázat szerinti kifizetési táblát vizsgálja, amelyből az első sor már törölve van. Ha az üzemeltető 7. táblázat szerinti A_3 objektumot védi, akkor rendre 4–4-et veszíthet, míg ha A_1-et akkor 4–8-at, vagyis a támadótól függetlenül jobban jár, ha az A_3-at védi. A kifizetési táblázatból, ennek megfelelően az első oszlop törölhető (7. táblázat zöld keret). A tovább redukált kifizetési táblázatban a támadó részéről már A_3 dominálja A_2-t vagyis A_2 sora törölhető (7. táblázat kék keret). A végére az üzemeltető részéről marad A_3 illetve A_2 objektum védelme az első esetbe 4-et a második esetben viszont 8-at fizethet, tehát célszerűen az A_3 objektum védelmét választja.

A megoldást jelen esetben minkét fél domináns stratégiák alapján választották, feltételezve, hogy mindkét fél racionális, ami jelen esetben annyi jelent, hogy a támadó maximálni akarja az okozott kárt, míg az üzemeltető ugyanezt minimálni szeretné.

2.2. Modell

Legyen a kifizetési táblázat a 8. táblázat szerint. Összevetve ezt az 5. táblázattal megállapítható, hogy a fődiagonálishoz tartozó elemek soronként a legkisebbek, de a fődiagonálison kívüli elemek soronként nem egyenlők. A védett rendszerek és védelmi berendezések nem függetlenek. Az üzemeltető és a támadó továbbra is racionális, vagyis a maximális kárt illetve a minimális költséget keresik.

Támadó \ Üzemeltető	A_1	A_2	A_3	min
A_1	1	2	6	1
A_2	6	**4**	5	**4**
A_3	7	2	1	1
max	7	**4**	5	

8. táblázat. A 2.2. modell kifizetési táblázata

A 8. táblázat alapján megállapítható, hogy sem a támadónak sem pedig a védőnek nincs domináns stratégiája. A modell az 1. modellnél bemutatott szerint nem egyszerűsíthető. A két fél jelen esetben választhat úgy, hogy maximálja a minimális bevételét. A támadó esetében ez a cselekvési változatonkénti minimálisan okozható kár maximálásával érhető el. A támadó soronként kiválasztja a minimumot és az így képzett oszlopból kiválasztja a maximális elemet (**4**).

Az üzemeltető minimálni szeretné a cselekvési változatonkénti maximális kiadását. Ezt úgy éri el, hogy oszloponként kiválasztja a maximális elemet és az így képzett sorból kiválasztja a legkisebbet (**4**).

A 8. táblázatban megfigyelhető, hogy a játékosok a másik fél döntésétől függetlenül nem tudnak javítani a saját helyzetükön. Az üzemeltető nem tudja csökkenteni a kárát, ha az A_1-et választja akkor 6-ra növekszik a költsége, ha A_3-at akkor 5-re. A támadó hasonló helyzetben van, ha megváltoztatja bármilyen irányban az eredeti döntését akkor az okozott kárt fogja csökkenteni 2-re.

A megoldás mindkét esetben az A_2 kiválasztása, a soronkénti minimumok maximuma és az oszloponkénti maximum minimuma megegyezik (**4**), a játékelméletben ezt a pontot nyeregpontnak nevezik, a **4**-et pedig a játék értékének.

2.3. Modell

Legyen a kifizetési táblázat a 9. táblázat szerinti. Alkalmazva előző modellnél bevezetett mini-max stratégiát, minkét félnek az A_3 kiválasztása látszik optimálisnak. A táblázatban viszont megfigyelhetjük, hogy soronkénti minimumok maximuma (**4**) és az oszloponkénti maximum minimuma (**5**) nem egyezik meg, nincs nyeregpont. A játékosok a stratégiájuk változtatásával javíthatnak a pozíciójukon.

Támadó \ Üzemeltető	A_1	A_2	A_3	min
A_1	1	3	3	1
A_2	5	2	5	2
A_3	8	8	4	**4**
max	8	8	**5**	

9. táblázat. A 2.3. modell kifizetési táblázata

A támadó felismerheti, hogy A_2-re módosítva növelheti az okozott kárt 4-ről 5-re, ezt viszont az üzemeltető is látja és módosít A_3-ról A_2-re így csökkentve a kiadását 5-ről 2-re. A támadó viszont módosít A_2-ről A_3-ra 8-ra növelve a kárt, az üzemeltető pedig módosít szintén A_3-re így csökkentve a kárt 4-re, és ezzel vissza is értünk a kiinduló pontra. Feltételezve mindkét fél racionalitását mindkét fél rájön arra, hogy a mini-max stratégia itt nem vezet megoldáshoz.

A legjobb megoldás ebben az esetben, ha mind a két fél a másiktól a lehető legjobban rejtve véletlenszerűen választ az érintett, jelen esetben az A_2 és az A_3 stratégiák közül. Abban az esetben, ha a döntési helyzet egymást követően gyakran fordul elő, akkor ügyelni kell arra, hogy az egymást követő döntésekben ne legyen fellelhető olyan minta, ami a másik fél felé információval szolgálhat.

Módosítja a modell megoldását, ha a támadó nem intelligens például valamilyen természeti katasztrófa ellen védekezünk, ebben az esetben az üzemeltető a mini-max kritérium segítségével kiválasztja a védett objektumot és csak annak tartja fenn a védelmét, amivel minimálhatja a maximális veszteségét.

2.4. Modell

Legyen a kifizetési táblázat a 10. táblázat szerinti. A táblázat alapján megállapítható, hogy a játéknak nincs értéke.

Üzemeltető

Támadó	A_1	A_2	A_3	min
A_1	1	5	5	1
A_2	6	2	6	2
A_3	7	7	3	**4**
max	8	8	**5**	

10. táblázat. A 2.4. modell kifizetési táblázata

A soronkénti minimumok maximuma, vagyis az alsó érték nem egyezik meg az oszloponkénti maximumok minimumával, vagyis a felső értékkel. A megoldás ebben az esetben az, hogy véletlenszerűen választunk az egyes stratégiák közül. Kérdésként viszont felmerülhet, hogy létezik-e olyan eloszlása **x** és **y** vektoroknak (5. táblázat) amellyel a játékosok minimálhatják maximális kiadásaikat. A feladat a (26) (27) szerinti lineáris programozási feladat segítségével oldható meg, a levezetést Hiller (1994:302) részletesen bemutatja.

A Támadó által maximalizálandó:

$$\mathbf{p}_i\,\mathbf{x} - \mathbf{x}_{n+1} \geq \mathbf{0} \qquad (26)$$

$$\max\{x_{n+1}\}$$

Az Üzemeltető által minimalizálandó:

$$\mathbf{p}_i^T\,\mathbf{y} - \mathbf{y}_{n+1} \geq \mathbf{0} \qquad (27)$$

$$\min\{y_{n+1}\}$$

ahol $\mathbf{p}_i$ a $\mathbf{P} = [p_{ij}]$ mátrix oszlopvektorai, $\mathbf{p}_i^T$ pedig **P** sorvektorainak transzponáltja, és $x_1 + x_2 +,\ldots,+x_n = 0$, $y_1 + y_2 +,\ldots,+y_n = 0$. $\mathbf{x_{n+1}}$ és $\mathbf{y_{n+1}}$ pedig x_{n+1} y_{n+1} változókból álló *n*-elemű vektor.

A 10. táblázat konstansait felhasználva a megoldás:

$$\mathbf{x}^T\,[0;\ 0{,}77;\ 0{,}23]$$

$$\mathbf{y}^T\,[0{,}08;\ 0{,}34;\ 0{,}58]$$

3. KÖVETKEZTETÉS

A felsorolt modellek alapján megállapítható:

- a támadó és a üzemeltető cselekvése döntéselmélet és játékelmélet segítségével modellezhető;
- számos modell és a esetenként a modellek számos megoldása áll a rendelkezésre;
- a modellek pontossága, vagyis az alkalmazhatóság megállapításához további vizsgálatok szükségesek.

Felhasznált irodalom

[1] Hiller, F. S., Lieberman, G. J. Bevezetés az operációkutatásba LSI Oktatóközpont, Budapest 1994, ISBN 963 577 1347

[2] Szentpéteri, Sz. Gazdasági döntések bizonytalanság esetén, Közgazdasági és Jogi Könyvkiadó Budapest 1980 ISBN 963 220 944 3

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Hornyacsek Júlia
hornyacsek.julia@uni-nke.hu

A KATASZTRÓFA-KÁRTERÜLET FELDERÍTÉSÉNEK ELMÉLETI ÉS GYAKORLATI KÉRDÉSEI

Absztrakt

A hatékony kárfelszámolás alapfeltétele, hogy a megjelenő mentőerők összehangoltan, a kialakult helyzetnek legmegfelelőbb módszerekkel tevékenykedjenek, és önmaguk is biztonságban végezhessék a feladataikat. Mindezek megvalósítása csak akkor lehetséges, ha a kialakult helyzet és a kárterületek felderítése hiteles, korrekt, mindenre kiterjedő, mert a mentést irányító vezetők elsősorban a felderítési adatok alapján hozzák meg a mentési feladatok végrehajtásával kapcsolatos döntéseiket. Ebben a cikkben a szerző arra keresi a választ, hogy napjaink katasztrófái során mi a kárfelderítés rendeltetése, milyen módszereket, elveket kell alkalmazni a mentőerők, a lakosság és az anyagi javak védelme érdekében a felderítő munkában, továbbá milyen összefüggés van a mentés érdekében kialakítandó védelmi képességek és a katasztrófa felderítés célja és alaprendeltetése között.

The prerequisite of effective recovery is that the rescue forces arriving at the site act in a coordinated way, using the most appropriate methods, and that they can carry out their tasks in safety. It is only possible to implement it if the detection of an incident site is accurate and credible, covering all aspects, since deployment control officials make their decisions on the rescue operations primarily based on detection data. In this article, the author seeks answers to the questions, what methods and principles should be used during the detection of disasters nowadays, what the function of incident site detection is in order to protect the members of the rescue forces, the population and property; in addition, what the interaction between the protection capacities to be created for the sake of rescue and the goals and basic functions of incident site detection is.

Kulcsszavak: *kárterület, kárfelderítés, szakfelderítés, detektálás, védelmi szint, védelmi képesség, felderítő erők, műszaki felderítés ~ incident site, incident site detection, specialized reconnaissance/detection, protection level, protection capacity, detection forces, technical detection/reconnaissance*

BEVEZETŐ

Napjainkban egyre gyakrabban jelennek meg tudósítások, amelyek olyan katasztrófa-helyzetekről számolnak be, amelyek intenzitása, jellege, lefolyása eltér a klasszikus, korábban kialakult katasztrófáktól és a következmények felszámolásának módozataitól. Ezek az esetek más- és mentési formákat követelnek a védelmi szervektől. Jó példa erre a kolontári esemény, vagy a 2010. évi borsodi árvíz, de a 2013. évi márciusi rendkívüli időjárási helyzet is, ami napokra megbénította az autópályák és a települések közlekedését, nehezítette az ellátásukat, és komoly kihívás elé állította a mentőerőket. Vélhetően ezeknek a jelenségeknek is tulajdonítható, hogy az elmúlt években mind a szakemberek, mind a tudományos kutatók fontosnak tartják a kialakult kárterületek jellemzőinek és a mentés során végrehajtandó feladatok vizsgálatát.

A gyakorlatban felmerült problémákat, azok kezelési módjait több konferencián [1] és folyóiratcikkben [2-3] feldolgozták, ezzel kapcsolatban szakma-módszertani anyagok készültek, és könyvek kerültek kiadásra a katasztrófa-kárterületen kialakult jelenségekről, a károk felszámolására irányuló feladatokról, valamint az ehhez szükséges képességekről [4].

Ezek elemzése kapcsán megállapítható, hogy a védelmi szféra szakemberei és a témával foglalkozó tudományos kutatók kiemelt jelentőséget tulajdonítanak a hatékony parancsnoki/védelmi vezetői munkának, valamint a kárfelderítésnek, mint a védelmi vezetők döntéseit megalapozó folyamatok legfontosabb elemének [5][6].

Ebben a cikkben megvizsgálom a felderítés helyét és szerepét a katasztrófák felszámolásában, és a döntési folyamatok meghozatalában. Rendszerezem a felderítés fajtáit, módszereit, eszközeit, megvizsgálom a felderítés és a tudományos elmélet és gyakorlat kapcsolatát, valamint a védelmi képességekkel való összefüggéseit.

1. A KATASZTRÓFA-KÁRTERÜLET FELDERÍTÉSÉNEK FOGALMA, FORMÁI, FAJTÁI, RENDELTETÉSE

A katasztrófa-kárterületen összetett kárelhárítási- és kárfelszámolási tevékenység folyik, amelyet jól érzékeltet a kárelhárítási feladatok fogalmi meghatározása:

„A kárelhárítási feladatok a katasztrófák elleni védekezés mentési időszakában végrehajtandó azonnali beavatkozásokat, operatív intézkedéseket magába foglaló része, olyan rendszabályok és tevékenységek összessége, melyek katasztrófák és más veszélyek esetén biztosítják az azonnali élet- és vagyonmentést, továbbá a káros hatások továbbterjedésének megakadályozását, a következményeinek mérséklését vagy kiküszöbölését, valamint a súlyos környezeti károk kialakulásának megakadályozását” [7].

A kárelhárítás alapvető feladata tehát, hogy megakadályozza a helyzet eszkalálódását, újabb károk keletkezését, és hatékonyan számolja a fel a kialakult károkat. Mindezek végrehajtására több alapvető feladatot kell ellátni.

A kárterületen az elsődleges teendő az életmentés, a tűzoltás és a lakosságvédelmi feladatok ellátása úgy, mint: a riasztás, tájékoztatás, kitelepítés, kimenekítés, befogadás, áldozatokkal való feladatok végzése stb. Ezt követi a létfenntartáshoz szükséges anyagi javak (különösen víz-, élelmiszer-, takarmány- és gyógyszerkészletek-, állatállomány stb.) és a kulturális értékek védelme. A mentés során fontos szerepe van a különböző szakfeladatok végrehajtásának is, mint a műszaki mentés-, az egészségügyi-, a vegyi-, biológiai-, radiológiai jellegű feladatok. Szintén fontos az érintettek folyamatos tájékoztatása a katasztrófa sújtotta területen, valamint a mentési folyamat minden oldalú logisztikai biztosítása, továbbá az alapvető életfeltételek megteremtése. Ezeket a feladatokat az 1. sz. ábra összegzi.

1. ábra. A kárelhárítás feladatai katasztrófák során.
Készítette: Dr. Hornyacsek Júlia, Forrás: [8]

A fenti feladatok végrehajtásának módját és formáját a parancsnoki/védelmi vezetői döntések határozzák meg, amelyek alapját a kárterület folyamatos felderítése során szerzett adatok és az azokból levont következtetések képezik.

A védekezés vezetőinek felelőssége, hogy a döntéseiket megfelelő helyzetértékelés alapján hozzák meg, és azok szakmailag megalapozottak legyenek, továbbá, hogy a mentőerők biztonságban végezhessék a munkájukat. A fentieken túl, bonyolult, elhúzódó esetekben, illetve ha a káresemény jellege, intenzitása szükségessé teszi, javaslatot tesznek a különleges jogrend bevezetésére is [9].

A fentiek alapján kijelenthető, hogy a katasztrófa-kárterület felderítésének fontos szerepe van a védekezés gyors és eredményes végrehajtásában. A következő alfejezetben bemutatom, hogy mi a kárterület-felderítésnek, milyen fajtái és módszerei vannak.

1.1 A kárterület-felderítés fogalma, alapvető csoportosítása

A kárterület-felderítés fogalmát a gyakorlatban „kárfelderítés” fogalmaként is használják, de a kettő nem ugyanaz. A kettő között az a különbség, hogy míg a kárfelderítés „csak” a konkrét károk megállapítására vonatkozik, addig a kárterület-felderítés ezeken túl, a kárterület további jellemzőinek megállapítását is magába foglalja. Ebből következik, hogy a kárfelderítés a kárterület-felderítésének része. A kár- és a kárterület felderítésének fogalma az alábbiakban adható meg:

A kárfelderítés „mindazon végrehajtott adatszerző- és elemző tevékenységek összessége, melyek a rendelkezésre álló erőforrások hatékony és gyors alkalmazásának feltételeit teremtik meg”[11].

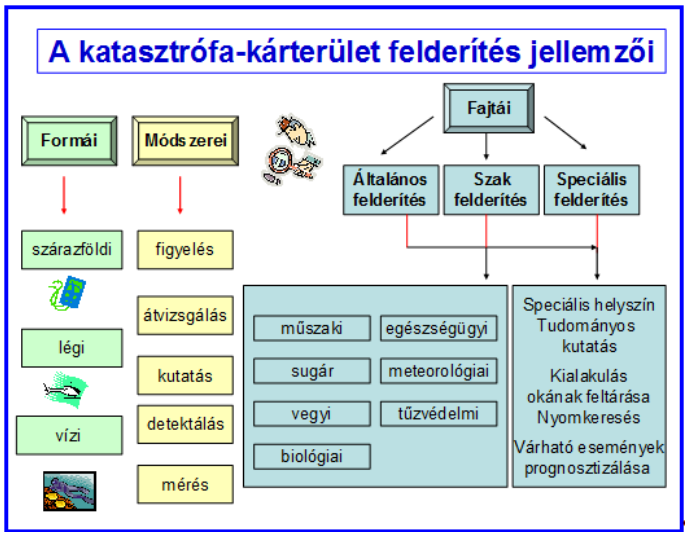
A kárterület-felderítés olyan tervező-, szervező-, végrehajtási- és elemező tevékenységek összessége, amely a károk felderítésén túl, információt szolgáltat a kárterület egyéb jellemzőiről, a kialakult helyzetről, a védekezés lehetséges formájáról, módjáról, és az események várható alakulásáról.

A védekezésért felelős vezető ezen információk alapján tud döntést hozni a védekezéshez szükséges erőforrásokról, a végrehajtandó feladatokról és azok prioritásáról, valamint a mentőerők biztonságos beavatkozásáról.

A kárterület-felderítés egyrészt tehát folyamatos adatgyűjtés- és elemzés az adott kárterületen kialakult helyzetről, másrészt segítséget nyújt a mentőerők számára feladataik

végrehajtásához. Végrehajtás formáját tekintve *szárazföldi-*, *légi-* és *vízi* felderítést különböztetünk meg [12].

Fajtáját tekintve, *általános-*, *szak-* és *speciális* felderítésről beszélhetünk. A felderítési feladatok végrehajtásának módszerét tekintve, lehet *figyelés*, *átvizsgálás*, *keresés-kutatás*, továbbá *detektálás* és *mérés* [13] [14]. E módszerek a kárterületen rendszerint nem elkülönülve, hanem egymás mellett, vagy egymásra épülve kerülnek alkalmazásra. A katasztrófa-kárterület felderítési munkáinak összefoglaló jellemzőit a 2. sz. ábra mutatja be.



2. ábra. A katasztrófa-kárterület felderítés jellemzői
Készítette: Dr. Hornyacsek Júlia, Forrás: [15]

1.2 A kárterület-felderítés fajtái, és azok alaprendeltetése

Az ábrából is látható, hogy a kárfelderítésnek három alapvető fajtája az általános, a szak- és a speciális felderítés.

Az általános felderítés az első általános adatokat szolgáltatja a kialakult katasztrófa-helyzetről, a kárterület méretéről, a károk jellegéről és nagyságáról, az utak járhatóságáról, a tűz-helyzetről, valamint a végrehajtandó mentési feladatokról, és az ahhoz szükséges erőkről.

A szakfelderítés az általános felderítés adatainak kiegészítésére, pontosítására irányul. Részletes, konkrét adatokat szolgáltat az egészségügyi-, műszaki (óvóhelyi-, közmű stb.), vegyi-, sugár-, biológiai-, állat- és növényvédelmi-, meteorológiai-, valamint tűzvédelmi szakmai területekről és azok kárterületen kialakult jellemzőiről.

A speciális felderítésről egyrészt akkor beszélünk, ha a káresemény olyan környezetben és helyszínen következett be, amely különleges felderítési eljárást és tudást igényel. Ilyenkor alkalmazhatunk barlangi-, hegyi-, kutyás mentő-, lavinamentő- vagy a tűzszerész mentőcsoportot, illetve AMAR, VFSZ, MoLaRi stb. jelzőrendszereket).[1]

Adódhatnak továbbá olyan esetek, amikor a felderítés célja nem, vagy nem csak a mentéshez való adatgyűjtés, hanem egyéb célok megvalósítása is. Ilyen például, a kárterületen folytatott tudományos kutatás, a helyzet kialakulása okainak felderítése, esetleg nyomkeresés- és biztosítás a rendőri szervek munkájához.

Napjaink katasztrófa-eseményei bizonyították, hogy a különböző tudományos módszereknek és technikai eszközöknek rendkívül fontos szerepe van a felderítés területén, illetve a szerzett adatok elemzése és értékelése szempontjából. A következő alfejezetben megvizsgálom a felderítés és a tudományos módszerek és technikai fejlesztések kapcsolatát.

1 AMAR (Automata mérő- és adatszolgáltató rendszer), VFSZ (Vegyi Felderítő Szolgálat, napjainkban ezek Mobil Laborok, formájában működnek), MoLaRi (Monitoring és lakossági riasztó rendszer)

1.3 A felderítés és a tudományos módszerek, technikai fejlesztések kapcsolata

A tudomány és a felderítés kapcsolatát három területen célszerű vizsgálni:

Az *egyik területe* a felderítés technikai eszközei, elemző értékelő berendezései. Amennyiben a felderítőket korszerű eszközökkel látjuk el, az általuk szerzett adatok sokkal pontosabbak és megbízhatóbbak, gyorsabb és biztonságosabb a mintavételezés módja is. Modern laboratóriumi eszközökkel, a kárterületről szerzett minták elemzése alapján olyan információkhoz juthatunk, amelyek hatékony segítséget nyújtanak a különböző szakmai döntések meghozatalához.

A másik területe a különböző tudományos módszerek és eljárások alkalmazása. A felderítők által megszerzett adatok elemzése és feldolgozása után, a mentési- és kárelhárítási feladatok végrehajtásához nagy segítséget nyújtanak a kémia, a biokémia, a biológia, a fizika, a humán- és állategészségtan, az informatika, a kommunikáció-tudományok, a pszichológia, a műszaki tudományok stb. területén meglévő tudományos eredmények.

A harmadik terület a kárterületen végzett tudományos kutatások és mérések. A katasztrófa kialakulásának okaira, körülményeire, valamint nem várt helyzetek kialakulására vonatkozó prognózisok, hipotézisek készítéséhez igénybe lehet venni kárterületen végzett tudományos kutatásokat és azok eredményeit, illetve egy adott esemény kárterülete is szolgálhat kutatások hipotéziseinek igazolásához vagy elvetéséhez adatokkal

Mindinkább előtérbe kerülnek azok a nézetek, hogy a felderítés pontosságát tudományos fejlesztésekkel kell segíteni. Jól érzékelteti ezt a tendenciát, hogy az Európai Unió több tagállama is jelentős összegeket különített el olyan kutatásokra, amelyek a felderítés eszközeinek fejlesztését, új eszközök kialakítását szolgálják. Németországban a *Kutatás a civil biztonság érdekében* címmel az állami stratégia részeként, *Hightech Strategie* programot hirdettek, és ennek kapcsán, jelentős fejlesztéseket végeztek a veszélyes anyagokkal szembeni védelem, a könnyebb anyaggyűjtés, valamint a biztosabb detektálás érdekében [16]. Ennek eredményeként több olyan készülékek kifejlesztésére került sor, amelyet jól lehet alkalmazni a felderítések alkalmával. Ilyenek például az ivóvíz-szennyezést vizsgáló detektorok, a chips-alapú állati fertőzéseket detektáló rendszerek. Kifejlesztettek például toxikus proteineket detektáló műszereket, miniatürizált laborokat a helyszíni talaj-, és élelmiszer vizsgálatokhoz, point-of car diagnosztikával működő hő-, optikai-, és elektromos adatolvasókat, száloptikás szenzorokat, továbbá a próbavétel, elemzés idejét csökkentő mikro-szenzorokat a veszélyes anyagok azonosításához, osztályzásához.

Jelentős fejlesztések történtek a kémiai anyagokat a levegőben felismerő és analizáló gáz-kromatográfok, a gázfelhő átvitelére alkalmas videofelvételt készítő készülékek, a szelektív megvilágító- és infravörös képek analizálását végző multi-spektrális készülékek vonatkozásában is. Egyre nagyobb hangsúlyt fektetnek a robbanásokat követő gázfázis elemzésére, valamint a nehezen megközelíthető területek, omlásból eredő üregek vizsgálatára, valamint minden más lehetséges eszközre, műszerre, ami a felderítés és a mentőerők védelmét szolgálják. Új utakat jelent a személyek és eszközök fertőzöttségének vizsgálatára alkalmas intelligens személyi scanner-ek kifejlesztése és gyártása, amelyek vizualizálják a szennyeződést, és lehetővé teszik a távolsági adatrögzítést, a szennyező anyag beazonosítását, valamint a szükséges mentesítő anyagok gyors meghatározását. Ezek nélkülözhetetlen elemei lesznek a jövő kárterület-felderítési tevékenységének.

Hazai viszonylatban is több területen áttörés érzékelhető a felderítő-eszközök fejlesztésében, alkalmazásában. Akadályozó tényezőként jelenik meg azonban, hogy az elmúlt évtizedekben a védelmi szféra is forráshiánnyal küzd, melynek következtében óhatatlanul is a mentésre, és nem a felderítésre, és a felderítési eszközökre helyeződött a hangsúly és a mobilizálható pénzeszközök.

2. A KATASZTRÓFA-KÁRTERÜLET FELDERÍTÉSÉNEK FELADATCSOPORTJAI ÉS AZOK BELSŐ TARTALMA

A fentiekben áttekintettük a felderítés, formáit, fajtáit, módszereit, tudománnyal való kapcsolatát. Ebben a fejezetben megvizsgálom a felderítés feladatcsoportjait, a végrehajtás folyamatát és azok belső tartalmát. A felderítési feladatok 4 alapvető csoportra oszthatóak:

1. a felderítés tervezése;
2. a felderítés végrehajtása, adatgyűjtés, adatrögzítés;
3. a felderítési adatok összegzése, értékelése, hitelességének ellenőrzése, valamint a szükséges korrekciók végrehajtása.

A fenti feladatcsoportok egymással szorosan összefüggnek, egymásra épülnek. Ha ezeket a végrehajtás oldaláról vizsgáljuk, felfoghatóak a végrehajtás folyamataként is.

2.1 A felderítés tervezése, annak fő területei, követelményei

Tervezés nélkül a felderítési feladatokat nem lehet szakszerűen végrehajtani. Egy katasztrófa bekövetkezése esetén nincs arra idő, hogy munkálatok közben tervezzék és szervezzék magának a felderítésnek a folyamatát, biztosítsák a feltételeket, képezzék ki az állományt, és alkalmassá tegyék őket a felderítés végrehajtására. Ezeket a feladatokat már a felkészülés időszakában végre kell hajtani, és a szükséges feladatokat a felderítési tervben kell rögzíteni. (Témánk szempontjából nem az egyszerű, viszonylag könnyen kezelhető katasztrófa-esetekről van szó, hiszen ott más a felderítés tervezése, hanem azokról az esetekről, amelyeknek összetett, nagy kiterjedésű a kárterülete, és elhúzódó mentés várható.)

Vizsgáljuk meg a nagykiterjedésű, összetett kárterület felderítése tervezésének folyamatát és annak feladat-tartalmát!

1. Első feladat a felderítés tervezésében a célok, és a felderítendő terület kijelölése, a felderítés fajtájának, formájának, módszereinek kiválasztása, a végrehajtandó felderítési feladatok időbeni tervezése.
2. Következő feladat a felderítő erők és azok nagyságának, munkarendjének meghatározása.
3. A következő lépés a kiemelt felderítendő adatok és szempontok kijelölése, valamint a felderítés eszközeinek, adathordozóinak kiválasztása, valamint a felderítési adatok továbbításának és a jelentés rendjének meghatározása.

A felderítés folyamatának összefoglalását és a tervezés fő területeit a 3. sz. ábra mutatja be.

3. ábra. A felderítés folyamata, a felderítés tervezés fő területei
Készítette: Dr. Hornyacsek Júlia

A gyakorlatban a felderítés megtervezése és megszervezése minden esetben a rendelkezésre álló időtől függ. Amennyiben kevés idő áll a döntéshozó rendelkezésére, a felderítés megtervezhető és elrendelhető szóban is, a felderítési térkép gyors áttekintésével. Elhúzódó mentés, vagy összetett kárterület estén, követelmény, hogy a felderítési feladatok tervezését és elrendelését írásos formában hajtsák végre.

A felderítéssel és annak tervezésével szemben követelmények fogalmazhatóak meg. A felderítés tervezésével és a tervezés eredményeként kialakított felderítési tervvel szembeni alapvető követelmények a következők:

1. a terv legyen világos, érthető, könnyen kezelhető,
2. alkalmazkodjon a kialakult helyzet sajátosságaihoz, a rendelkezésre álló erőkhöz, eszközökhöz,
3. A tervbe foglalt felderítési módszereket úgy kell megválasztani, hogy a tevékenység legyen rugalmas, kövesse az esetleges változásokat, az események eszkalálódásával kialakult új helyzetet,
4. a terv legyen alkalmas a felderítő erők erőkifejtésének összehangolására, illetve tartalmazzon garanciákat a felderítő erők biztonságára,
5. a felderítési tervhez készüljön térkép grafikus formában, a szükséges táblázatos és szöveges kiegészítésekkel, és a mindenki által ismert egységes jelekkel, rövidítésekkel, hogy mindenki értse, azonos módon értelmezze a feladatokat.

A felderítés-tervezési folyamat fontos eszköze a felderítő térkép (lehet papír alapú vagy digitális), amely tartalmazza a felderítő egységek elhelyezkedését a kárterületen, az eszközök eloszlását, a tervezett tevékenységet és a felderítési irányokat. Tartalmazza továbbá a veszélyeztetett települések és területek várható rombolódási-zóna határát, a tiltott útvonalakat, a mentő erők elhelyezését és az odavezető útvonalakat, a mentési-mentesítési tevékenység határait, a kitelepítési útvonalakat, az együttműködők lehetséges menetvonalait [14].[2]

Tartalmazhat ezen túlmenően más olyan adatot, megjegyzést, ami a helyzet specialitásaiból adódik. A felderítés tervezésére rendszerint kevés idő áll rendelkezésre, az életmentés érdekében a mentési munkák már akár előtte, vagy ezzel párhuzamosan folynak, így a tervezésnél a mentőerőktől, lakosságtól spontán befutó adatokat is figyelembe kell venni.

2.2. Az általános- és szakfelderítési feladatainak végrehajtása és módszerei

A felderítési terv elkészülését követően kezdődik meg a felderítés végrehajtása, amely rendszerint az általános felderítéssel indul, majd szükség esetén szakfelderítéssel folytatódik. Vizsgáljuk meg ezek tartalmát!

Az általános felderítés feladatai, és azok végrehajtása

Ennek során a cél általános, alapvető adatok gyűjtése kárterületről. Első lépésként a felderítők megkapják a feladatot, a védelmi vezető megtartja az eligazítást, kiosztja a terveket, szóban vagy írásban kijelöli a felderítési területet, a felderítő párokat, és meghatározza a betartandó biztonsági szabályokat.

A felderítők értelmezik a feladatot, felkészülnek rá, majd kivonulnak a kárterületre, ahol először szemrevételezést tartanak, majd megkezdik a kárterületen az elsődleges adatgyűjtést és azokat rögzítik. Másodlagos adatoknak kell tekinteni azokat, amelyeket nem a felderítők nyernek, hanem a kárterületen tartózkodók és szemtanúk közölnek a felderítőkkel. Ezeket az elsődleges és másodlagos felderítési adatokat előzetesen értékelik, következtetéseket vonnak le belőlük, és az adatokat is továbbítják a védelmi vezető felé. Szükség esetén a vezető utasítására eltérhetnek a tervben meghatározott felderítési útvonaltól bizonyos adatok visszaellenőrzése és újak megszerzése céljából.

[2] 15. oldal

A feladat végrehajtását követően elkészítik a felderítéssel kapcsolatos jelentésüket, majd megkezdik a csoport kivonását a kárterületről. A kárterület határán elvégzik a szükséges mentesítést, jelentik a feladat-végrehajtás során tapasztaltakat, majd összegzett jelentést készítenek.

A szakfelderítés feladatai, és azok végrehajtása

A veszélyeztetett terület értékelése azonban csak sok szempont figyelembevételével válhat teljessé. Az általános helyzetfelmérés kapcsán szerzett felderítési adatok mindössze az azonnali beavatkozás, és a közvetlen fenyegetettség felszámolásához elegendő információt nyújtanak. Szükség lehet tehát szakfelderítési adatokra. A szakfelderítés során speciális eszközökkel, műszerekkel, módszerekkel részletesebb adatokat nyernek. Ennek végrehajtása az adott témában szerzett szakértelmet, és sokszor többéves gyakorlatot igényel. A szakfelderítésnek több típusa is van, így a feladatok is szerteágazóak. Vizsgáljuk meg ezeket!

A műszaki felderítés során műszaki adatokat szereznek az épületek, utak, hidak, közművek, tárgyak, eszközök állapotáról, a rombolódásuk fokáról, jellegéről, a szükséges mentő- és helyreállítási munkákról, az ahhoz szükséges erőkről, eszközökről. Az épületek vizsgálata során elemzik a romtorlaszok határait, a romosodás módját, a romok alóli mentés lehetőségeit, vizsgálják a bennük rekedtek lehetséges számát, és az élet-esélyeiket.

A vegyi- és sugárfelderítés során felderítő eszközökkel és járművekkel gyűjtenek adatot a kárterület nagyságáról, vegyi- vagy sugár-szennyezettségéről, a szükségessé váló mentő-mentesítő eszközökről, a lakosság-, a természet- és az anyagi javak érintettségéről. Az érintett körzetben a felderítés tehát a radioaktív és/vagy kémiai szennyező anyagok által kiváltott veszélyeztetettség mértékére vonatkozó információk begyűjtésére irányul, megállapítja a sugárszinteket, a veszélyes anyagok típusát, jellegét, hatását.

A biológiai felderítés során levegőből, talajból, növényekből, állatokból vett minták gyűjtésével és vizsgálatával határozzák meg a terület biológiai jellemzőit, károsodását, illetve a kárterület nagyságát. Vizsgálatuk kiterjed a terep-, a vízforrások, az alapvető élelmiszer- és állatállomány esetleges fertőzöttségének, elfajulásainak, pusztulása mértékének megállapítására is. A kárterület nagyságának, jellemzőinek lehetséges zárási, mentesítési pontjainak meghatározásához is ennek kapcsán gyűjtenek adatokat.

Az egészségügyi felderítés az egészségügyi-, járványügyi állapotról gyűjt adatokat. Adatot szolgáltat a mortalitás és a morbiditás értékeléséhez, a terjedés prognosztizálásához, a mentési feladatokhoz. Célja a bevezetendő egészségügyi preventív rendszabályok és teendők meghatározásának előkészítése is.

A tűzvédelmi felderítés a tűzhelyzetet vizsgálja, értékeli annak terjedési irányát, az általa való fenyegetettséget, elemzi a tűzoltáshoz szükséges víznyerő helyeket. Vizsgálja a tűz által érintett települések, személyek számát, a veszélyeztetett ökológiai tényezőket, és az adott tűzesemény esetleges hatását a fő mentési irányokra és a mentőerőre.

A meteorológiai felderítés során elemzik a hőmérsékleti és széladatokat, a talajmenti levegő adatait, a felhőzet-terjedési adatokat stb. Vizsgálják az időjárási jellemzőinek (csapadék, hőmérsékleti viszonyok, légkör állapota, hidrometeorológiai helyzet) hatását az adott területre, a mentésre, és a helyreállításra.

A katasztrófa jellegéből adódóan, vagy előre látható, hogy szakfelderítésre lesz szükség, vagy csak az általános felderítés során derül ki, hogy ahhoz, hogy a vezetői döntéshez minden adat rendelkezésre álljon, egy vagy több szakfelderítést is el kell végezni. A fenti feladatok gyakran nem elkülönülten jelentkeznek, hanem szükség lehet arra, hogy az egyik szakfelderítési forma mellett egy másikat is elvégezzenek, például a vegyi felderítés folyamán a tűzfelderítés végrehajtására is sor kerül.

A szakfelderítés végrehajtása hasonló az általános felderítéséhez, így a következő mozzanatokból áll:

1. Feladat átvétele, értelmezése,
2. Felkészülés a feladat végzésére (tájékozódás, módszerek, eszközök megválasztása, védőfelszerelés felvétele stb.),
3. Kárterületre vonulás, szemrevételezés,
4. A tervszerű felderítés, adatgyűjtés végrehajtása annak megfelelően, amilyen szakfeladatot ellátnak,
5. Az elsődleges adatok összevetése a másodlagos adatokkal,
6. Kapcsolattartás a védelmi vezetővel és más felderítő csoportokkal,
7. Rész-jelentések elkészítése,
8. Újabb adatok gyűjtése, illetve az előzők visszaellenőrzése, szükség szerinti módosítások, korrekciók végrehajtása,
9. A feladat végrehajtását követően, a csoport kivonása a kárterületről,
10. Mentesítés végzése (személy-, eszköz- és járműmentesítés),
11. Összegzett jelentések készítése.

A fenti folyamaton belüli feladatok minden katasztrófánál eltérőek, az adott eseménytől függ, hogy milyen módszerrel hajtják végre.

A felderítés végrehajtásának alapvető módszerei

A felderítés módszerének megválasztása több tényezőtől függ, így a rendelkezésre álló felderítő szervezetek típusától, nagyságától, szakértelmétől, képességeitől is. A kárterületen a felderítési feladatokat végrehajtó szervezetek létszáma, szakmai összetétele szorosan összefügg a kárterület jellemzőivel. Felderítésre minimum 2 fő részvételével kerülhet sor.

A felderítő szervezetek fajtái létszámuktól és szerepüktől függően, az alábbiak lehetnek:

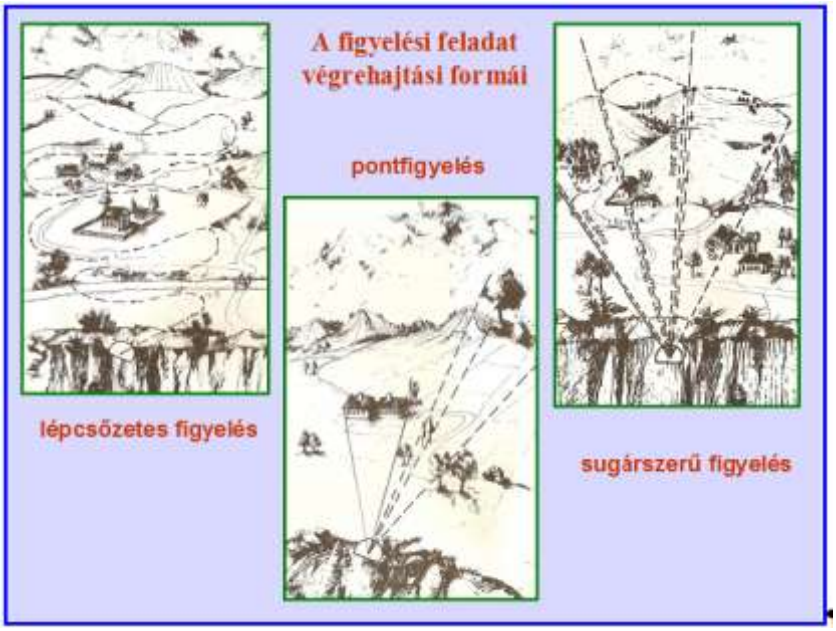
- a figyelők,
- rejtett figyelők,
- felderítő járőrök,
- figyelő rajok (őrsök),
- felderítő csoportok,
- esetenként mentés-vezetői felderítő járőrök/munkacsoportok.

A fent bemutatott szervezetek a következő módszerekkel dolgoznak:

- figyelés,
- járőrözés,
- ellenőrzés,
- átvizsgálás, kutatás,
- mintavétel,
- Utóellenőrzés.

Vizsgáljuk meg ezek lényegét!

Megfigyelés. A felderítő munkája, legyen az általános vagy szakfelderítés, rendszerint a figyeléssel kezdődik, melynek során az adott jelenség alapvető változóit, azok területre való hatását, és annak következményeit figyelik meg. A figyelés végrehajtását tekintve lehet egy adott állapot egyszeri szemrevételezése, de lehet pontfigyelés-, sugárszerű- és lépcsőzetes figyelés. Ezeket elsősorban korábban háborús helyzetben alkalmazták nagy területekre kiterjedően, de katasztrófák esetén is szükséges lehet, például erdőtüzek, árvizek, állatok vonulása stb. esetén. (Lásd 4. sz. ábra.)



4. ábra. A figyelési feladatok végrehajtásának formái Készítette: Dr. Hornyacsek Júlia, forrás: [17]

Járőrözés. A felderítés másik módszere a járőrözés, amikor a járőrök a terep kijelölt részén meghatározott rendben haladva feltérképezik a helyzetet, megállapításokat tesznek, adatokat rögzítenek. Ilyen például árvíz esetén a gátak suvadásának, állapotának vizsgálata stb.

Ellenőrzés. A felderítők végezhetnek ellenőrzést, amikor bizonyos jellemzők állapotának azonosítását hajtják végre, majd ezt ismétlik meg ciklikusan, illetve a felderítési adatok változását ellenőrzik.

Átvizsgálás. Szükség lehet a terület átvizsgálására, erők, eszközök felkutatásra, keresésére is, melynek során a területet kereső négyzetekre osztják és aprólékosan átvizsgálják. Ilyen eset lehet a földrengések során az épületek átvizsgálása statikai szempontból, vagy a romok alá temetett területeken élőlények kutatásához adatgyűjtés (romhatárok, romosodás módja, üregekben rekedtek életesélyeinek prognosztizálása stb.)

Utóellenőrzés. A védelmi vezetés döntéseihez szükség lehet utóellenőrzésre is. „Ennek során a felderítő egy *jellemző* aktuális végállapotát rögzíti.” [18] Ezt összevetik a korábbi adatokkal, és következtetnek a helyzet romlására, stagnálására vagy javulására.

Mintavétel. Egy további felderítési tevékenység a mintavétel, ami „olyan eljárás, mellyel a felderítés folyamán, az anyag egy meghatározott részét, egy adott módszerrel eltávolítják, annak helyszínen nem detektálható jellemzőinek későbbi megállapíthatósága végett.”[18] A felderítési bármelyik formájában lehetnek adatgyűjtési- és adatrögzítési feladatok, ezért vizsgáljuk meg ezeket!

2.3 Adatgyűjtési- és adatrögzítési tevékenység és annak jellemzői

A felderítéskor fontos feladat az adatgyűjtés. Ennek során az adott területről, jelenségről beszedhető, számszerűsíthető adatokat vagy jellemzőket gyűjtik össze, előzetes elemzést végeznek, azokat értékelik (helyben vagy laborokban), majd az eredményeket továbbítják a döntéshozóknak. Az adatgyűjtés az adat jellegéből adódóan, lehet audio-, vizuális- és audiovizuális.

Hordozóját tekintve lehet papír alapú vagy digitális. A nyert adatokat minden esetben *felderítési naplóban* kell rögzíteni, illetve *a felderítési adatok nyilvántartó könyvében*. Ezeknek napjainkra kialakult az elektronikus formája is, és a továbbítása rendszerint számítógépes rendszeren történik.

Az adatgyűjtés önmaga is egy folyamat, melynek főbb mozzanatai a következők:

- Az adatkör és változóinak meghatározása,
- Az adatgyűjtés módjának (analóg, digitális) eldöntése,
- Az adatgyűjtés formájának (képi-, audio-, vizuális-, audiovizuális) eldöntése,
- Az adatgyűjtés és mintavétel végrehajtása,
- Az adatok rögzítése (napló), archiválása, elsődleges értékelése,
- Az adatok előzetes összehasonlítása,
- Az adatok továbbítása.

Vannak olyan adatok, amelyek helyben nyerhetők, de vannak, amelyek az eset jellegéből adódóan, nem nyerhetők ki a területen, ezért a vizsgálni kívánt mintákat el kell szállítani a kárterületen kívülre, és ott kell elvégezni a vele kapcsolatos vizsgálatokat. Ebben az esetben gondoskodni kell arról, hogy a minták szállítás során ne sérüljenek.

Az adatgyűjtés folyamata attól is függ, hogy milyen jellegű adatra van szükség. Gyakran elegendő csak a szemrevételezéssel értelmezni a jelenségeket, illetve képi-, audio- vagy audiovizuális módon rögzíteni, de lehet olyan jellegű az esemény, hogy szükséges a vizsgálandó jelenségről mérhető, számszerűsíthető adatokat méréssel nyerni. Az előbbire példa, amikor a nyúlgátak állapotáról, az esetleges gátsuvadásról az álló-, vagy mozgókép-rögzítéssel nyert adatok is elegendőek. Utóbbira példa, egy terület vegyi szennyeződésének mérőműszerekkel való vizsgálata, és a nyert adatok statisztikai, matematikai értékelése.

Összetett kárterületen a mintavétel végrehajtásához gyakran van szükség arra, hogy műszaki feladatok ellátása útján tegyék szabaddá, hozzáférhetővé a területet a mintanyeréshez.

Adatrögzítés. Az adatgyűjtést követően fontos mozzanat, a rögzítés, archiválás, mely a későbbi kategorizálást, tipizálást, az értékelést segíti, de a visszakereshetőséget is ez biztosítja. Erre egyaránt alkalmasak a papír alapú rögzítők, illetve az elektronikus adattárolók. A digitális adathordozók, mint a CD-k, DVD-k, külső tárolók jól alkalmazhatóak, de sérülékenységük miatt már újabb, biztonságosabb megoldások alakultak ki. Napjainkra modern adat- és video-archiváló rendszerekkel tudják tárolni, kategorizálni a kárterületek, káresemények adatait.

A felderítés során szükségessé válhat az új adatok korábbi eseményekkel, adat-értékekkel való összehasonlítása, ehhez már modern szabadon használható adatkategorizáló programok állnak rendelkezésre: mint például ACDSee, FastStone Image Viewer, Picasa, IrfanView vagy az XnView stb.

A nemzetközi szervezetek katasztrófák során mindenki számára elérhető információs portálokat működtetnek, azon tárolják és teszik közzé az adatokat. Ezeknek vannak a szakemberek számára elérhető, kódolt felületei is, amelyen a kárfelderítési adatokat találják különböző csoportosításokban. [19][3]

Az adatgyűjtés minden típusának, módjának teljes vertikumú bemutatására nincs lehetőség, ezért itt az egyik leggyakrabban használt módszert, a *képrögzítést*, mint a katasztrófák kárterületén viszonylag könnyen alkalmazható típust vizsgálom!

A képrögzítés, mint adatrögzítési forma

A képrögzítés az egyik legfontosabb adatgyűjtési eljárás. Ennek analóg és digitális változata is használatos. Lehet álló- és mozgóképrögzítés. Az állókép rögzítése végezhető telefon, mp3 lejátszó, pantop, laptop, netbook, tablet és a hagyományos illetve a nagysebességű fényképezőgépek segítségével. Ezek előnye, hogy viszonylag gyorsan, könnyen készíthetőek, mivel azonban statikusak, csak egy adott állapotot rögzítenek. A másik formája a mozgóképes

[3] 35-40. oldal

képrögzítés. Előnye, hogy nem csak egy adott pillanatot, hanem egy folyamatot is rögzíteni tudnak. Nézzünk néhány példát és speciális alkalmazást a katasztrófák során való képrögzítésre!

1. A képrögzítés legegyszerűbb változatát a normál fényképezőgépek nagyfelbontású fajtáival való rögzítés jelenti.
2. A 480 alatti és a 700 nanométer feletti sugárzástartományba eső tárgyakat, amelyet már szabad szemmel nem érzékelünk, infravörös képrögzítővel készítik.
3. Összetett, nagy kiterjedésű katasztrófáknál, olyan helyeken, ahol a felderítés veszélyeztetné a felderítők életét, pilóta nélküli repülőgéppel végeznek képrögzítést.
4. Nagy kiterjedésű erdőtüzeknél, ahol a valósidejű felvételek készítése a cél, termikus WASP (Wildfire Airborne Sensor Program) és a WASP-Lite érzékelőkkel rögzítenek képeket.
5. A nehezített terepen való képrögzítést gyakran Wifi rendszeren működő sisakkamerák, az ütés- és vízálló kamerák segítségével végzik, mint például a Pentax Optio WG-2 kamera, amely 16MP-es CMOS szenzorral, 1080p (30fps) videó-rögzítéssel, 5x optikai zoommal működik.
6. Speciális helyzetek esetén, amikor az egész teret kell látni, de képesnek kell lenni a kárterület egy adott részének kiélesítésére, jól használhatóak a Lytro (light-field) fényképezőgépek.
7. Üregek, omladékok mögötti adatok gyűjtésére, az élőlények felkutatására a száloptikás cső- és csatornavizsgáló-kamera, valamint a hajlékony, monitorral ellátott endoszkóp-kamerák állnak rendelkezésre a képrögzítéshez. [19][4]

Az adatgyűjtés és adatrögzítés tehát hagyományos és modern módszerekkel is folyik. A begyűjtött, esetenként jelentős számú adatot rendszerezni, összesíteni kell, áttekinthető, relációkat és tendenciákat is mutató adatbázist kell belőlük készíteni a vezetői döntésekhez. Vizsgáljuk meg ennek folyamatát!

2.3 Az adatok összesítése, elemzése, értékelése és a kialakult helyzet megítélése

Az adatok beszerzését a felderítők a kárhelyszínen hajtják végre, amelyet az előzetes értékelés után továbbítanak a döntést hozó szerv elemző-értékelő munkacsoportjai felé. A munkacsoportok elvégzik az adatok összesítését, végrehajtják az adatok ellenőrzését, a szükséges korrekciókat, majd ezekből következtetéseket vonnak le a vezetői döntés meghozatalához. Ez a tevékenység az alábbi lépésekből tevődik össze:

- az adatok összegzése és tartalmának megismerése,
- hitelességük és sürgősségi értékük megítélése, szükséges korrekciók végrehajtása,
- az adatok osztályozása, rendszerezése tartalmuk vagy a felderített objektum szerint,
- az adatok analízise, matematikai, statisztikai, mentés-módszertani értékelése, összehasonlítása más adatokkal,
- az adatokból következtetések levonása, a mentés feladatainak, a szükséges erőknek, eszközöknek meghatározásához, és javaslattétel a vezetői döntéshez.

Az adatok értékelésének, feldolgozásának egyik legfontosabb módszere az analízis, amely történhet összehasonlítással, statisztikai értékeléssel, matematikai számításokkal. Ennek során gyakran korábbi, hasonló esetekben mért adatok összevetésével vonnak le következtetéseket, és prognosztizálnak helyzeteket. Ilyen például a vízállások összevetése egy adott

[4] 41-43. oldal

folyószakaszon a korábbi adatokkal, vagy hasonló gátszerkezettel rendelkező folyókkal, de ilyen a talajmozgások mérési adatainak, gátak suvadási mutatóinak az összehasonlítása is.

A statisztikai elemzésekkel átlagot, az átlagtól való eltérést, arányokat és a változók jellemző értékeit, illetve a törvényszerűségeket tudják kimutatni. Ilyen például a járványok idején a megbetegedések számának, szóródásának vizsgálata, a terjedés mértékének, irányának rögzítése, és az ezekből leszűrhető prognózisok felállítása.

Matematikai számításokkal tudnak a szakemberek következtetni például a vegyi- vagy sugárzó anyag terjedésére, feleződésére, hígulására.

A kárterületen kialakult helyzet értékelésekor a felderítési adatokból több fontos kérdésre is választ kell kapni annak érdekében, hogy a legmegfelelőbb döntést lehessen hozni a további teendőkre. Ezek a kérdések a következőek:

- Mi váltotta ki a helyzetet?
- Milyen károk keletkeztek, és azok milyen következményekkel járnak?
- Mit, kiket és milyen mértékben érintett és érint a veszély?
- A kárterületen milyen jelenségek érzékelhetőek?
- Milyen további következmények várhatóak?
- Milyen spontán mentési reakciók indultak meg, ezek milyen eredménnyel jártak?
- Beavatkozás nélkül milyen kimenetele lenne az esetnek?
- A lehetséges megoldásoknak milyen előnyei, milyen hátrányai lehetnek?
- Mik a halaszthatatlan teendők, és azoknak mi a prioritása?
- Mik a további teendők, és azokat milyen sorrendben kell végezni?
- Milyen erők bevonása válik szükségessé?
- A mentőerők mely irányokban és milyen mélységben tudják végezni az elsődleges és másodlagos teendőiket?
- Milyen logisztikai támogatást kell nyújtani a mentőerők részére? [20]

A helyzet-megítélést követő lépés a döntéshozatal, valamint az együttműködők tájékoztatása, a feladatok kiosztása. A kárterületen a mentés irányításához mindvégig folyamatos felderítést kell végrehajtani, melynek érdekében szükséges a felderítő egységek pihentetése, váltása. Ennek előfeltétele tartalék felderítő egységek létrehozása és teljes készenlétbe helyezése.

3. A FELDERÍTÉSKOR ALKALMAZOTT ESZKÖZÖK TÍPUSAI, A MŰSZAKI SZAKFELDERÍTÉS ESZKÖZEI

A fentiekben áttekintettük a felderítés célját, fajtáit, módszereit, folyamatát. Mindezeket a felderítők meghatározott eszközökkel végzik. Ezeknek széles a skálája, a cikk terjedelme nem teszi lehetővé a teljes vertikum bemutatását, így csak a fontosabb eszköz-kategóriákat tekintem át. Vizsgáljuk meg a végrehajtásához szükséges eszközök főbb kategóriáit!

A felderítési tevékenység összetett feladat, ezért a felderítő erőknek mindehhez alapeszköz-készlettel és az adott eseménynek megfelelő szakfelderítő készlettel, továbbá speciális készletekkel is rendelkezniük kell. Bizonyos eszközök nem szállíthatóak kézzel, vagy nem működtethetőek önmagukban, ezeknek hordozó járművei is vannak. Ezek attól függően, hogy vízen, levegőben, szárazföldön folyik a felderítés, lehetnek vízi-, szárazföldi- vagy légi járművek. Az 5. sz. ábra tartalmaz néhány felderítő eszközt, és hordozó járművet.

Az eszközöket csoportosíthatjuk aszerint, hogy egyéni felderítő-, vagy a szakfelderítést szolgáló, az adott szakterület adatainak gyűjtését segítő eszközök.

5. ábra. Szakfelderítő eszközök és hordozók Készítette: Dr. Hornyacsek Júlia, forrás: [21-24]

A felderítő eszközök főbb kategóriái:

- A helyszín megközelítését szolgáló eszközök,
- Az adatok gyűjtését szolgáló eszközök,
- Az adatok rögzítését szolgáló eszközök,
- Az adatok elemzését, elsődleges értékelését segítő eszközök,
- Az adatok továbbításra való átalakítását, továbbítását segítő eszközök,
- A felderítés határait, eredményeit jelölő eszközök.
- Egyéb, speciális rendeltetésű eszközök.

Mind az általános, mind a szak- és speciális felderítések során a fenti eszköz-csoportokban található felszereléseket, berendezéseket és eszközöket viszik magukkal a végrehajtók. Vannak olyan eszközök és felszerelések, amelyekkel minden felderítőnek rendelkeznie kell. Ezek elsősorban a saját biztonságukat, a mintához való hozzájutást, az adatgyűjtést, valamint a veszélyes területek megjelölését szolgálják.

Az alábbiakban vizsgáljuk meg a szak- és speciális felderítés lehetséges eszközeit!

A szakfelderítő eszközök annyi félék, ahány felderítés-típus van, ezek mindegyikét nem vizsgálhatjuk e cikk keretében, ezért a szakfelderítések közül az egyik legfontosabb, és minden kárterületen előforduló típus, *a műszaki felderítés* eszközeit elemzem.

Műszaki szakfelderítő eszközök

A szakfelderítés eszközei mindig az adott káreseménytől, a kárterület jellemzőitől függenek. A műszaki szakfelderítő tevékenység az épületek, utak, hidak, kritikus infrastruktúra elemek állapotának, sérülési mértékének felderítésére irányul, kiterjed a műszaki mentőerők alkalmazási lehetőségeinek feltérképezésére, létszámuk meghatározásához adatgyűjtésre, az elérhetőségi útvonalak összeírására, a szükséges eszközökre való javaslattételre. A kárterület összetettsége miatt, saját biztonságuk érdekében előfordulhat, hogy képesnek kell lenniük további veszélyeztető tényezők felderítésére. A felszerelésüknek emiatt túl kell mutatnia a műszaki eszközökön.

Néhány nagyobb katasztrófa-eseményt, annak kárterületét és felderítő munkáját vizsgálva[5] állítottam össze azokat az eszköz-kategóriákat, amelyek egy műszaki jellegű kárterület felderítéséhez, adatainak begyűjtéséhez szükségesek. Ezeket az alábbiakban összegzem:

A kutatást, feltárást, megközelítést segítő, műszaki jellemzőket mérő eszközök

- azok az okmányok, leírások, adatbázisok, amelyek az adott kárterületről, az előrevonási útvonal műtárgyairól, közműhálózatáról, tájékozódást adnak,
- ásók, lapátok, vésők, speciális kulcskészletek, világító eszközök, tájékozódási eszközök,
- világító eszközök, mérőszalagok,
- oszlop-mászóvas, feszültségmérő műszerek, sérült elektromos kábelek keresésére, mérésére,
- robbanó anyagok felderítéséhez szükséges eszközök,
- közmű- kulcskészletek, a fémvágó fűrészek,
- elektromos lehallgató készülékek a földben, falban elhelyezett vezetékek, csövek, fémek felkutatásához, infra-érzékelők,
- foszforbronz hálóból vagy egyéb anyaggal és technikával készült fémruha a nagyfeszültségű (áram alatt levő) vezetékek felderítésére,
- sztetoszkóp, és más lehallgató készülékek az épületek beomlott üregek feltárásához,
- a távolságok és magasságok egyidejű mérésén alapuló felderítéshez tachométerek,
- a szilárdság-vizsgálatokhoz a Schmidt-féle rugós kalapács, betonoszkóp és a rétegvastagság-mérő pachiometer, továbbá száloptikás üregvizsgálók.

A felderítéssel összefüggő területek, objektumok megjelölésére és jelzésére szolgáló eszközök

A felderített területeken a veszélyes épületek, különböző veszélyforrások megjelölésére, valamint több felderítő szerv együttes működése során a már felderített területek jelzésére, továbbá a duplikációk elkerülése érdekében, különböző jelzőtáblákat és jelölési módokat használnak. Az erre alkalmas eszközök közül a legfontosabbak az alábbiak:

- speciális kréták, tollak, festékek,
- jelzőtáblák, határoló szalagok és oszlopok,
- tiltó táblák, jelzőfények, jelzőcsíkok,
- veszélyesterület-jelző, és a felderített terület határát jelző szalagok,
- „leszúrható táblák, zászlók, műanyag szalag, jelzőbóják az elhatárolási, jelölési feladatok végrehajtásához, valamint leszúrható fémtüskék, pálcák.” [25]

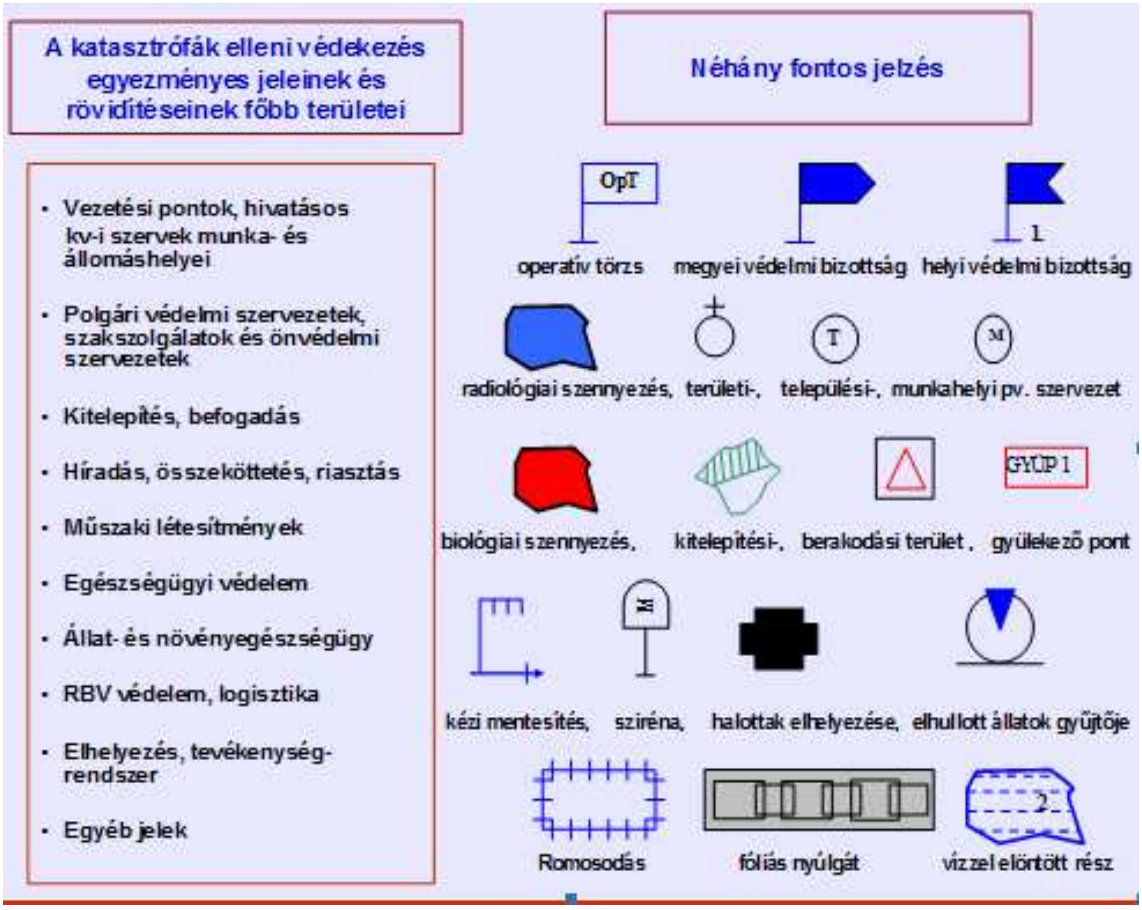
A felderítés során az egyik legfontosabb eszköz a térkép, és a térkép használatának egységes értelmezését szolgáló jelek és jelzések. Ezeket a térképen használatos jeleket és jelzéseket hazánkban a hivatásos központi katasztrófavédelmi szerv (BM OKF) főigazgatója által kiadott Katasztrófavédelmi műveleti szabályzat tartalmazza [26]. Lásd 6. sz. ábra.

[5] Hazai árvizek: 2000., 2001., 2006., 2010.; földrengés: Gyömrő, 2006., Oroszlány: 2011.; buszbaleset Siófok: 2003; vonatbaleset: 2006. Monorierdő; Pirotechnikai gyár robbanása: 2006. Balatonfűzfő; repülő-szerencsétlenség: 2006. Hejce; vörösiszap katasztrófa: 2010. Kolontár; földrengés: L’Aquila, 2009.; Földrengés, cunami, atomerőmű robbanás: Japán, Fukushima 2011.

Az adatok rögzítését, előzetes értékelését és továbbítását szolgáló eszközök

- speciális fényképezőgépek, hőkamerák,
- közműhálózat-térképek a sérülési adatok rögzítéséhez,
- térinformatikai eszközök, szoftverek,
- informatikai eszközök, a mobil számítógépek,
- műszaki adattárak- és értékelő szoftverek,
- híradó eszközök (mobil telefonok, rádiók stb.).

A műszaki szakfelderítés eszközeinek bemutatása koránt sem teljes, de jól érzékelteti, hogy egy kárterületen, ahol rendszerint összetett hatásokkal találkozunk, igen széles a skálája az adatok gyűjtését, tárolását, előzetes elemzését segítő, illetve azoknak az eszközöknek, amelyek kárterületen lévő különböző veszélyforrások, veszélyes épületszerkezetek és területek megjelölésére elhatárolására szolgálnak.



6. ábra. Egyezményes jelek főbb területei. Készítette: Dr. H. Júlia, forrás: [26]

Az előző fejezetekben és alfejezetekben bemutattam, a vezetői döntéseket és a mentési feladatok végrehajtásának formáját, módját alapvetően meghatározó „kárterület-felderítés", fajtáit, módszereit, eszközeit, feladatait és azok végrehajtásának folyamatát. A témával kapcsolatos irodalmi kutatásaim mellett megvizsgáltam és elemeztem a kárterület felderítésének helyét, szerepét és fontosságát, megtörtén katasztrófák esetén, a mentési feladatok végrehajtásának megszervezése, és a szükséges mentési képességek kialakítása során.

A kutatási eredmények egyértelműen bebizonyították és alátámasztották azt a hipotézisemet, mely szerint, ha közvetve is, de a „kárterület felderítés" alapvetően befolyásolja a mentési feladatok végrehajtásának módszerét, a mentő erők szakmai összetételét, képességét és ez által a mentés sikerét és hatékonyságát. Ennek oka, hogy a

mentésért felelős vezető a helyes mentési módszerek megválasztására a mentő erők összetételére képességeinek kialakítására, valamint a mentés feladatok megkezdésére vonatkozó döntéseit a felderítési adatok, valamint az abból levont következtetések, megállapítások alapján hozza meg. Éppen ezért, rendkívül fontos, hogy a kárterület felderítésének feladatai időben és szakszerűen legyenek végrehajtva, a felderítési adatok legyenek hitelesek és pontosak és az abból levont vezetői döntést segítő következtetetések megalapozottak.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Napjaink hazai és nemzetközi katasztrófái ráirányították a figyelmet a kárterület-jellemzők felderítésének kérdésére. A kárterületen kialakult helyzet elemzése, értékelése a parancsnoki/védelemvezetői munka alapvető eleme, melynek célja a mentési feladatokkal és a kárfelszámolással kapcsolatos döntések meghozatala.

A katasztrófa-kárterület felderítése különböző, egymásra épülő feladatokból és munkafolyamatokból áll, amely a felderítés tervezésével kezdődik, a végrehajtás megszervezésével, a felderítési adatok gyűjtésével, szükség szerint előzetes helyszíni elemzéssel, mintavételezéssel, valamint az elemző értékelő munkacsoportokhoz történő továbbítással folytatódik. Ezt követően kerül sor az összegyűjtött adatok rendszerezésére, hitelességének ellenőrzésére, a prioritások megállapítására, valamint elemzésére, értékelésére, melynek célja a kárterület jellemzőinek, veszélyforrásainak, a kialakult és várható helyzet megismerése, a károk nagyságának megállapítása, és mindazon információk megszerzése, amelyek a mentési feladatok megszervezéséhez, végrehajtásához, a mentési képességek kialakításához, valamint a mentési feltételek megteremtéséhez szükségesek. Végezetül, az így kapott adatok és információk alapján a mentésért felelős vezető meghozza a mentési feladatok megkezdésével és végrehajtásával kapcsolatos döntéseit, és elrendeli az adatok továbbítását a jogszabályban meghatározott a társszervekhez, hivatalokhoz, mentőerőkhöz és együttműködő szervekhez, szervezetekhez.

A felderítés végrehajtásának formáját tekintve, megkülönböztetünk légi-, szárazföldi és/vagy vízi felderítési módokat. A felderítés fajtáit vizsgálva beszélünk általános felderítésről, szakfelderítésről és speciális felderítésről. A felderítési feladatokat végrehajtók köre széles, főként figyelők, rejtett figyelők, járőrök, mintavételezők, elemzők, elemzőcsoportok végzik.

A felderítés eredményes és sikeres végrehajtása nagyban függ a felderítési tervek pontosságától, a végrehajtás körültekintő megszervezéstől, valamint a felderítők rendelkezésére álló, általuk használt felderítő eszközök minőségétől. A felderítés eszközeinek kiválasztása, a nyert adatok regisztrálásának, valamint a részértékelések továbbításának meghatározása is fontos feladat. A felderítők feladataik végrehajtása során az egyéni védőfelszerelésük mellett különböző általános-, speciális- és szakfelderítő eszközöket, berendezéseket használnak. Példaként bemutattam a műszaki szakfelderítést, melynek eszközei széles skálán mozognak, az egyszerű feltárást, keresést, kutatást, anyagvételezést segítő szerszámoktól, a modern adatgyűjtési eszközökön és a rögzítést, értékelést megkönnyítő készülékeken át, a területjelölő, adatrögzítő anyagokig mindenre szükség lehet. A felderítés fontos eszköze még napjainkban is a felderítési napló és a felderítési térkép, amelyeken az eredményeket egyezményes jelekkel rögzítik, és a mentésben közreműködők részére közzé adják.

A felderítési adatok elemzését és értékelését végző munkacsoportok gyakran alkalmaznak olyan tudományos eljárásokat, módszereket, amelyek segítenek a pontosabb és megalapozottabb következtetések és döntések meghozatalában. Nem ritka, hogy napjainkban

az adatértékelés összehasonlító elemzésekkel, statisztikai feldolgozással, matematikai számításokkal történik. Elterjedt módszer, hogy a helyszíni mérések adatait, a minták alapján, labormérési eredményekkel hasonlítják össze, így ellenőrzik azok pontosságát, hitelességét.

Összességében megállapítható, hogy a kárterület felderítésének eredményessége, a felderítési adatok hitelessége alapvetően befolyásolja a mentési feladatok végrehajtásának sikerét. Ennek oka, hogy a mentésért felelős vezető a mentési módszerek helyes megválasztására a mentő erők összetételére, képességeinek kialakítására, a feltételek biztosítására, valamint a mentés végrehajtására vonatkozó döntéseit, a felderítési adatok alapján hozza meg.

Felhasznált irodalom

[1] Konferenciák: http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_tudomany_konferencia Letöltés: 2013. 03.15.

[2] Laczik Balázs: Speciális műszaki technikai eszközök alkalmazási lehetőségei kárelhárítási és kárfelszámolási feladatok végrehajtása során, a katasztrófák sújtotta kárterületen. Műszaki Katonai Közlöny, XXI. évfolyam, 1-4. szám, 2011. 213-228. oldal

[3] Dr. Tóth Rudolf: A lakosságvédelem aktualitása, helye, szerepe napjaink új kihívásainak tükrében. Polgári védelmi Szemle, 2009. 2. szám, 55-75. oldal

[4] Dr. Hornyacsek Júlia: A települési védelmi képességek a katasztrófa-kihívások tükrében, a települések katasztrófa-elhárítási feladatai, a végrehajtáshoz szükséges helyi védelmi képesség alapvető területei, azok kialakításának folyamata. "Biztonságunk érdekében" Oktatási- és Tanácsadó Tudományos Egyesület Budapest, 2011. ISBN: 978-963-08-2606-8

[5] „Veszélyes és mérgező anyagok felderítésének, semlegesítésének és a következmények felszámolásának egészségügyi és katasztrófavédelmi feladatai”2012. http://www.bm-tt.hu/cuccok/letolt/mtuun2012/docs/mtu02/nov6_7_program.pdf Letöltés: 2013. 03.15.

[6] Szakmai Tudományos Műhely - robotrepülőgépek az Óbudai Egyetemen. http://events.uni-obuda.hu/en/node/1699 Letöltés: 2013. 03.15.

[7] Dr. Szabó Sándor – Dr. Tóth Rudolf: A kárelhárítási és kárfelszámolási feladatok értelmezése a katasztrófavédelem területén. VIth International Symposium on Defence Technology, 6-7 May 2010 Budapest, Hungary Konferencia kiadvány 7-8. oldal, ISSN 1416-1443

[8] Dr. Hornyacsek Júlia: A települési védelmi képességek a katasztrófa-kihívások tükrében, a települések katasztrófa-elhárítási feladatai, a végrehajtáshoz szükséges helyi védelmi képesség alapvető területei, azok kialakításának folyamata. "Biztonságunk érdekében" Oktatási- és Tanácsadó Tudományos Egyesület Budapest, 2011. 64. oldal ISBN: 978-963-08-2606-8

[9] Alaptörvény 53. cikk (1-4)

[10] Laczik Balázs: Speciális műszaki technikai eszközök alkalmazási lehetőségei kárelhárítási és kár-felszámolási feladatok végrehajtása során, a katasztrófák sújtotta kárterületen. Műszaki katonai Közlöny, XXI. évfolyam, 1-4. szám 2011. 213. oldal

[11] Dr. Földi László-Körmendy Norbert: Katasztrófaveszély felderítés 1. Általános felderítési feladatok. 1. oldal http://www.zmne.hu/tanszekek/vegyi/docs/fiatkut/pdf/korm_04_03.pdf Letöltés: 2013. 03.15.

[12] Szerző nélkül: A polgári védelmi felderítő szervek alkalmazása. Tansegédlet, BM PVOP, 1986. 5. oldal

[13] Dr. Földi László-Körmendy Norbert: Katasztrófaveszély felderítés 1. Általános felderítési feladatok. http://www.zmne.hu/tanszekek/vegyi/docs/fiatkut/pdf/korm_04_03.pdf 2-3. oldal Letöltés: 2013. 03.15.

[14] Szerző nélkül: Polgári védelmi felderítés. Budapest, 1981. BM PVOP. 5-7. oldal

[15] Szerző nélkül: Segédlet a polgári védelem felderítési feladatai végrehajtásához. BM PVOP, Budapest, 1971. Zrínyi Nyomda, 7-18. oldal

[16] Forschung für die zivile Sicherheit. Detektion von Gefahrstoffen. Bundesministerium für Bildung und Forschung (BMBF) Referat Sicherheitsforschung. Bonn, Berlin, 2008.

[17] Szerző nélkül: A polgári védelmi felderítő szervek alkalmazása. Tansegédlet, BM PVOP, 1986. 12-14. oldal

[18] Körmendy Norbert- Dr. Földi László Katasztrófaveszély felderítés 2. Szakfelderítési feladatok 2. 2. oldal, http://www.zmne.hu/tanszekek/vegyi/docs/fiatkut/pdf/korm_04_04.pdf Letöltés: 2013. 03.15.

[19] Murai László: Az álló- és mozgóképrögzítés a katasztrófavédelem területén, technikák, elvei, módszerei, a gyakorlatban történő megvalósítás lehetséges formái. ITDK dolgozat, NKE, 2012. 35-43. oldal

[20] Richtlinie für das Führen im Katastropheneinsatz. Bundesministerium für Inneres, Abteilung II/4, Wien 2004. http://www.bmi.gv.at/cms/BMI_Service/Richtlinie_fuer_das_Fuehren_im_Katastropheneinsatz.pdf Letöltés: 2013. 03.15.

[21] [Letöltés: 2013. 03.16.
a) vízi sugárfelderítő rendszer
http://www.gammatech.hu/?mnuGrp=mnuProducts&module=products&lang=hun&group=teruletszerint_jarmufedelzeti&menupath=-teruletszerint_jarmufedelzeti&csoport=Járműfedélzet
b) Járműfedélzeti ABV felderítés
http://www.gammatech.hu/?mnuGrp=mnuProducts&module=products&lang=hun&group=teruletszerint_jarmufedelzeti&menupath=-teruletszerint_jarmufedelzeti&csoport=Járműfedélzeti
c) Mobil sugárkapu
http://www.gammatech.hu/?mnuGrp=&module=products&lang=hun&group=teruletszerint_hulladekkezeles_sugarfelderito&product=bns94m&termek=BNS

[22] Agrometeorológiai állomás
http://www.gammatech.hu 2013. 03.15

[23] Kommunikációs, vezérlő és adatgyűjtő modul
http://www.gammatech.hu/?mnuGrp=mnuProducts&module=products&lang=hun&group=custom&product=ucip&termek=µCIP-01 2013. 03.15

[24] Sugárszint mérő: http://www.gammatech.hu/?mnuGrp=&module=products&lang=hun&group=teruletszerint_hulladekkezeles_sugarfelderito&product=bns92s&termek=BNS-92S 2013. 03. 15.

[25] Szerző nélkül: A polgári védelmi felderítő szervek alkalmazása. Tansegédlet, BM PVOP, 1986. 5. oldal

[26] Katasztrófavédelmi Műveleti Szabályzat. Budapest, 2011. BM OKF, 2. sz. függelék 113-119. oldal

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Komjáthy László
komjathy.laszlo@uni-nke.hu

MAGYARORSZÁG TŰZVÉDELME A HATÁRMENTI TELEPÜLÉSEK TŰZVÉDELME

Absztrakt

Magyarország biztonságpolitikájának egyik fő célkitűzése a polgári, emberi jogok teljes érvényesülésének, valamint Magyarország területén élők élet-, vagyon- és szociális biztonságának a szavatolása. Ebből kiindulva a tűzvédelem az ország biztonsági rendszerének nélkülözhetetlen és elválaszthatatlan része.
A hazánkban bekövetkezett bármely, komoly erő és eszköz azonnali bevetését igénylő eseményekhez elsődlegesen riasztható, megfelelő technikai felszereltséggel és szakmai felkészültséggel rendelkező szervezetek a katasztrófavédelem tűzoltó egységei. Fő tevékenységük nemcsak a tűzesetek felszámolása, melyet az is bizonyít, hogy napjainkban a beavatkozásukat igénylő események kb. 1/3-át a műszaki mentési feladatok teszik ki. Elsődleges szerepük pedig katasztrófa helyzetek felszámolásában is megkérdőjelezhetetlen.

One of the main goals of Hungarian safety politics is the complete realization of human and citizens' rights as well as assuring life, property and the social safety of Hungary's inhabitants. This makes fire protection an indispensable and inseparable part of the country's safety system.
In the case of a serious incident that requires the immediate intervention of an adequately equipped organization with well-trained individuals, firemen are among the first to be alerted in the country. The argument that their activities are not limited to merely putting out fires is supported by the fact that approximately one third of their interventions involve technical rescue. Furthermore, firemen play a huge role in preventing and mitigating catastrophic events.

Kulcsszavak: *tűzoltóság, tűzoltók, biztonság, segítségnyújtás ~ fire fighting, firemen, safety, help*

A tűzoltóságok számára a közeljövő egyik legnagyobb kihívását a veszélyes anyagok közúti szállítása jelenti, az abban rejlő komplex bizonytalansági tényezők, így elsősorban a veszélyforrás mobilitása következtében. A veszélyes anyagok szállításának kockázata a mintegy 31 ezer km-es hazai közúthálózat nehezen behatárolható részén és az emellett elhelyezkedő érzékeny pontokon (települések, veszélyes üzemek, telephelyek stb.) jelentkezhetnek elsősorban. Magyarország földrajzi elhelyezkedéséből kiindulva, a rendelkezésre álló szakmai tapasztalatok, elemzések, a meglévő információbázisok alapján az országon belül keletkező és az országhatáron átnyúló lehetséges veszélyeztető hatások, kockázati tényezők jelentős mértékben ismertek. Ennek ellenére szükségszerű feladatként fogalmazódik meg a kockázatelemzések és előrejelzések hatásfokának növelése, a veszélyes szállítmányok nyomon követése, valamint célszerű megvizsgálni a Magyar Honvédség vegyi felderítőegységével történő szorosabb együttműködés lehetőségét is.[1]
A statisztikai adatok szerint a hazai tűzoltói beavatkozást igénylő események kb. 1/4-e-1/3-a műszaki mentési tevékenységet jelent, melyek döntő többsége I-es vagy I-es kiemelt riasztási fokozat elrendelését indokolja. A legtöbb esetben ez víz- és viharkárok felszámolását, közúti baleseteknél történő beavatkozást takar.

Tovább vizsgálva a statisztikákat, szembetűnő az is, hogy a tűzesetek több mint fele szabadban keletkezik, mely esetek kb. 50 % - át avar, nádas, szemét és gaztűz eredményezi. A fenti események felszámolása általában nem igényel túlzottan magas színtű technikai és szakmai felkészültséget. A hivatásos tűzoltó parancsnokságok, az önkormányzati tűzoltóságok leterheltségét és működési költségeit jelentősen csökkentené, ha ezeket a feladatokat például az önkéntes tűzoltóságok látnák el [2].

Ahhoz, hogy hazánk tűzvédelmének helyzetét értsük, lépjünk kicsit vissza az időben. A helyi önkormányzatokról szóló 1990. évi LXV. Törvény[3] nem sorolta a kötelezően ellátandó feladatok közé a települések tűzvédelmét, s ennek ellátására nem biztosított normatív támogatást. Ezt a problémát úgy korrigálta az 1991. évi XX-as, az úgynevezett hatásköri törvény[4], hogy a hivatásos önkormányzati tűzoltóságok székhelye szerinti települési önkormányzatok kötelező közszolgáltatási feladataként határozta meg a tűzoltást és a műszaki mentést. E feladatokat nemcsak saját településükön, hanem a kijelölt működési körzetükben is el kellett látniuk. Ezt a szabályozást vette át az 1996. évi XXXI. Törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról

Magyarországon a tűzoltást és a műszaki mentést a részükre kijelölt elsődleges működési körzetben a jelenleg működő 105 hivatásos tűzoltóság látja el, normatív úton biztosított költségvetési támogatással. Az elmúlt közel húsz év vonulási adatait elemezve feltűnő az esetszámok folyamatos emelkedése: Míg 1994-ben 34.005 esetben történt riasztás, addig ez a szám 2004-re 51.793-ra nőtt, ami 2010. első fél évében már 55.289, 2011.ugyanezen időszakában viszont csak 34.099 riasztást jelentett tűzoltáshoz és műszaki mentéshez[5]! Ez közel 70 %-os emelkedés, melyet szinte változatlan létszámú beavatkozói állománnyal hajtottak végre az egységek. A leterheltség csökkentésének és a működési terület hatékonyabb tűzvédelmének biztosítása érdekében a fejlesztés egyik lehetőségét a hivatásos beavatkozói létszám emelésében, új állomások és őrsök létesítésében látom.

A hivatásos tűzoltóságok 20-25 km-es körzetben kellene, hogy ellássák feladatukat, hogy az előírt 25 perces vonulási időt be tudják tartani[6]. Az ország településszerkezete, népsűrűsége, közlekedési viszonyai mintegy 200-220 állandóan riasztható tűzoltóság működtetését indokolná. Természetesen a feladatellátás függvényében továbbra is támogatásra javasolom a vonulási területtel rendelkező önkormányzati tűzoltóságokat, a tűzoltásban és műszaki mentésben közreműködő önkéntes tűzoltó egyesületeket, fontosnak ítélve a tűzoltás, illetve a mentés mielőbbi megkezdését, kisebb eseteknél annak felszámolását.

Szükséges lenne a mentő tűzvédelmi szempontból nem megfelelően ellátott térségekben, az ún. fehér foltokon központi céltámogatással elősegíteni az önkormányzati tűzoltósággal nem rendelkező megyékben, településszámtól függően legalább két kihelyezett őrs, valamint 15-20 önkéntes tűzoltó egyesület megalakulását. Főleg, ha ehhez helyi kezdeményezés is járul, hiszen az 1996-os év közepétől kísérleti jelleggel, 1998–tól pedig jogszabállyal kijelölt területen működő önkéntes tűzoltóságok – ez évtől önkormányzati tűzoltóságok- teljesítették az éves vonulások mintegy 10 százalékát.

A lakosság számához viszonyított tűzelőfordulás aránya az Európai Uniós. országokkal összehasonlítva elszomorító képet mutat, például közel kétszerese az osztrákokénak. Okai között az emberi tájékozatlanság, a gondosság hiánya, illetve a tulajdonosi szemlélet lassú elterjedése a legfőbb ok. A Magyarországon élő lakossághoz a tűzoltó erők mérhető átlagos vonulási ideje az Európai Unió tagállamait tekintve az utolsók között van. A vonulási idő a jelzéstől a kárhelyre történő kiérkezésig eltelt időből áll. A riasztási idő csökkentésére a lehetőség korlátozott, elsősorban a vonulási idő, illetve a vonulási távolság csökkentése jelenthet lényeges javulást. Hazánkban a tűzoltóságok egy tűzesethez átlagosan 34 km-t vonulnak, ami 36 percet jelent. Ez a hosszú vonulási idő azért van, mert az ország közel 3100 települését kötelezetten 105 hivatásos és 68 önkormányzati, azaz összesen 173 tűzoltóság védi. Ehhez képest a nyugati és északi államokban legfeljebb 8-10 illetve 12 perces átlag vonulási idők vannak.

A rendkívül nagy elmaradásunk oka elsősorban az 1948-90 között működő rendszer volt, ahol 1/5–ére csökkent a tűzoltásra képes tűzoltóságok száma. 1948-ban közel 2.000 különböző típusú tűzoltóság volt, ma nem éri el ennek az egytizedét sem. A jelenlegi helyzet másik oka az 1990 és 96 közötti időszak következménye, ahol a tűzvédelemmel a rendszerváltás folyamatában sem az állam, sem az önkormányzatok nem tudtak alapvetően pozitív irányú változást előidézni. A helyi önkormányzatokról szóló 1990. évi LXV törvény 8. §-a a tűzvédelemről való gondoskodást az önkormányzatok választható feladatává, majd az 1991. évi XX. törvény a gondoskodást csak a hivatásos tűzoltóságokkal rendelkező önkormányzatoknak tette kötelező feladatává. Ez azt eredményezte, hogy a tűzoltásra képes önkéntes tűzoltó egyesületek száma rohamosan csökkent, mert sem az önkormányzat, sem az állam, sem a hatályos jogszabályok nem támogatták az egyesületek működését és fejlődését. Emiatt a tűzoltás hatékonysága a kisebb településeken tovább romlott.

1996 áprilisában az Országgyűlés elfogadta a tűz elleni védekezésről és a műszaki mentésről szóló 1996. évi. XXXI. sz. törvényt. Ez a jogszabály hivatásos tűzoltóságokat elvileg átadta az önkormányzatoknak, viszont az irányítási és finanszírozási rendszer nem alakult át a vártnak megfelelően. E törvény tette lehetővé a köztestületként működő önkéntes tűzoltóságok létrehozását. 1996. júliusában kísérleti jelleggel 26 ilyen tűzoltóság kezdte meg működését az ún. „fehér foltokon”. 1998. január 1-jétől már a belügyminiszter által kijelölt működési körzetben többségében önállóan látták el a tűzoltási és műszaki mentési feladatokat. 1999-ben az összes beavatkozás 10 százalékát már a köztestületi tűzoltóságok teljesítették. Számuk 2002. januártól 39-re emelkedett. 2004. januártól már 46 ilyen tűzoltóság működött.

Jelenleg Magyarországon 105 hivatásos tűzoltó parancsnokság van. A parancsnokságok Műveletirányítási Terveiből kiolvasható, hogy mely települések azok, amelyek jelenleg 25 perces vonulási időn túl érhetők csak el. Ezek közül a települések közül kell kiválasztani a kihelyezett őrs állomáshelyét úgy, hogy körzetközpontként működve felügyelje a körzetében megalakuló önkéntes egységeket is. Az eddigi működési terület ellátását javítva, fizikailag közelebb kerül a tűzoltóság a védeni kívánt lakossághoz, viszont pénzügyi többletet az elhelyezésen túl nem jelent.

Megállapodás abban szükséges, hogy az új őrs elhelyezését (2 szerállásos szociális helyiséggel rendelkező épület) a befogadó önkormányzat biztosítja-e. Erre célszerű kistérségi

forrás pályáztatása. Az ellátatlan területen meg kell vizsgálni azt is, hogy az ellátás költséghatékonysága milyen megoldással a legkedvezőbb.

Borsod-Abaúj-Zemplén megyében – az egyik legnagyobb területű és településszámú megye - kilenc hivatásos tűzoltó parancsnokság működik. Működési területükön (Encs 78, Kazincbarcika 46, Mezőkövesd 30, Miskolc 35, Ózd 29, Sátoraljaújhely 45, Szendrő 36, Szerencs 32, Tiszaújváros 29) összesen 36o település tűzvédelméért felelősek, amelyekből 177 település csak átlagosan 24 perc alatt érhető el, azaz ellátatlan településeknek minősülnek[7]. Csak az encsi hivatásos tűzoltó parancsnokság működési területén található 78 településből 34 olyan helység van, ami 25 percen kívül érhető csak el[8], az alábbi táblázatban látható. A plusz kettő perc a jelzéstől az indulásig terjedő idő.

Település neve	Távolság htp-től km	Vonulási idő perc
Abaújlak	20	25+2
Abaújszolnok	20	24+2
Abaújvár	34	37+2
Büttös	26	34+2
Csenyéte	21	27+2
Alsódobsza	31	37+2
Felsődobsza	22	27+2
Felsővadász	26	34+2
Gadna	22	28+2
Gagybátor	23	32+2
Gagyvendégi	20	25+2
Gönc	28	29+2
Göncruszka	22	28+2
Hejce	23	29+2
Hernádkércs	20	24+2
Homrogd	32	36+2
Kány	35	40+2
Kéked	38	40+2
Keresztéte	31	41+2
Krasznokvajda	25	34+2
Kupa	31	39+2
Mogyoróska	25	34+2
Monaj	28	34+2
Nagykinizs	21	25+2
Nyésta	24	29+2
Pamlény	31	42+2
Pányok	38	44+2
Perecse	28	34+2
Regéc	27	36+2
Selyeb	25	30+2
Szászfa	28	38+2
Tornyosnémeti	28	27+2
Telkibánya	40	48+2
Zsujta	29	30+2

1. táblázat. Az encsi Hivatásos Tűzoltó Parancsnokság működési területéhez tartozó, 25 percen túl elérhető települések. (saját gyűjtés)

Sátoraljaújhely Hivatásos Tűzoltó Parancsnokság működési területéhez tartozó 45 település közül 34 helység minősül ellátatlannak,[8] melyek az alábbi táblázatban láthatók:

Település	Távolság (km)	Elérhetőség + riasztás (perc)
Bodrogolaszi	20	23+2
Bózsva	20	25+2
Cigánd	36	45+2
Erdőbénye	33	35+2
Erdőhorváti	30	35+2
Filkeháza	19	24+2
Fűzér	25	32+2
Fűzérkajata	22	28+2
Fűzérkomlós	24	29+2
Fűzérradvány	16	23+2
Györgytarló	33	37+2
Háromhuta	39	43+2
Hollóháza	28	36+2
Karcsa	19	25+2
Kenézlő	31	41+2
Kishuta	20	26+2
Kisrozvágy	31	37+2
Komlóska	35	39+2
Nagyhuta	23	30+2
Nagyrozvágy	29	34+2
Nyíri	24	30+2
Olaszliszka	28	29+2
Pácin	22	26+2
Pusztafalu	26	31+2
Ricse	37	46+2
Sárazsadány	21	25+2
Tiszacsermely	28	36+2
Tiszakarád	27	35+2
Tolcsva	26	28+2
Vágáshuta	23	29+2
Vámosújfalu	23	39+2
Viss	34	46+2
Zalkod	37	50+2
Zemplénagárd	45	60+2

2. táblázat. Sátoraljaújhely HTP ellátatlannak minősülő települései (saját gyűjtés)

Az ózdi Hivatásos Tűzoltó Parancsnokság működési körzetéhez 29 település tartozik. Ezek közül 11 minősül ellátatlannak, azaz csak 25 perc elteltével érnek ki a tűzeset helyszínére az ózdi tűzoltó egységek. Mindhárom tűzoltóság estében ugyanaz volt a rendező elv: a google maps segítségével, a domborzati viszonyokat is figyelembe véve a számítógép határozta meg a kiérkezési időt. Ehhez társul még minden település esetében a kettő perc riasztási idő, amit a 3. számú táblázatba foglaltam össze.

Bükkmogyorósd	16	25+2
Csokvaomány	18	29+2
Domaháza	17	23+2
Gömörszőlős	25	32+2
Kelemér	23	27+2
Lénárddaróc	16	24+2
Nekézseny	19	28+2
Sajómercse	18	25+2
Sajóvelezd	19	24+2
Szentdomonkos	25	31+2
Uppony	17	23+2

3. táblázat. Ózd működési körzetének 25 percen kívül eső települései (saját gyűjtés)

A megyében működő önkormányzati tűzoltóság nincs, így itt őrsök kihelyezésével lehetne a leghamarabb eredményt elérni (pl. Gönc, Tokaj). A B-A-Z megyei települések tűzvédelmét ellátó egységek (Encs, Sátoraljaújhely, Ózd) esetében célszerű lenne vizsgálni a kétoldalú nemzetközi együttműködés lehetőségét is. A tűzoltás, műszaki mentés területén törekedni kellene arra, hogy a határokon átnyúló, kétoldalú segítségnyújtásra történő együttműködésben az érdekelt felek, nevezetesen az adott térség hivatásos tűzoltóságai a megyei igazgatóságok segítségével kössenek kölcsönös segítségnyújtásra együttműködést. Így az általam vizsgált szlovák-magyar határ felé magyar oldalról Sátoraljaújhely, Encs, Szendrő, Kazincbarcika, Ózd, Salgótarján, Balassagyarmat, Vác, Esztergom, Nyergesújfalu, Komárom, Győr, Mosonmagyaróvár hivatásos tűzoltóságai, valamint a körzetükben lévő önkormányzati tűzoltóságok létesíthetnének napi kapcsolatot a határ másik oldalán lévő települések Královský Chlmec, Caňa, Moldava nad Bodvou, Tornaľa, Filakovo, Lučenec, Veľký Krtiš, Sahy, Sturovo, Komárno, Veľký Meder, Dunajská Streda, Samorin tűzoltó egységeivel.

Sátoraljaújhely tűzoltósága például a határ szlovák oldalán 21 településre érne oda 25 percen belül. Královský Chlmec tűzoltósága pedig a Bodrogköz településeinek tudna segítséget nyújtani. Mindkét fél szakmai tapasztalataira, emberi kapcsolataira serkentőleg hatna az együttműködés. Megvalósulhatna a határok nélküli tűzvédelem. A határon túli segítségnyújtást a Műveletirányítási Tervek készítésénél is figyelembe kellene venni. A kétoldalú egyezményeket ki kellene terjeszteni a tűzesetek és katasztrófák megelőzését érintő tapasztalatok cseréjére is.

Ehhez nyújthat segítséget a Nemzetközi Visegrádi Alap, melynek célkitűzései között szerepel a határokon átívelő kapcsolatok szorgalmazásával a Visegrádi Négyek országai közötti regionális együttműködés[11]. Szorgalmazni kell a tűzesetek tapasztalatainak cseréjét, új tűzoltás technikai és tűzoltás-taktikai megoldások, fejlesztések eredményének hasznosítását. Ennek egyik lehetséges formája a külföldi szakirodalom magyarországi szélesebb körű elterjesztése, illetve a hazai szakirodalom külföldi propagálása, valamint ezekben a témákban nemzetközi konferenciák szervezése. A Kormány politikájával összhangban a tűzvédelem területén is fejleszteni szükséges a regionális és területi kapcsolatokat, amelyek igénye nemcsak szlovák relációban jelentkezik.

Felhasznált irodalom

[1] Földi László: A Magyar Honvédség tevékenysége a vegyi katasztrófák elleni védelem összefüggés rendszerében. PhD értekezés. ZMNE, 2003, 69. oldal.

[2] Az 1996.évi XXI.törvény alapján az önkéntes tűzoltóságok csak a hivatásosak segítségnyújtói lehetnek

[3] 1990. évi LXV. törvény a helyi önkormányzatokról

[4] 1991. évi XX. törvény a helyi önkormányzatok és szerveik, a köztársasági megbízottak, valamint egyes centrális alárendeltségű szervek feladat- és hatásköreiről

[5] Forrás: http://www.katasztrofavedelem.hu/statisztika/201106/

[6] A mentő tűzvédelem rendszere. Fülep Zoltán tű. alezredes, Országos Tűzoltósági Főfelügyelőség, Tűzoltósági főosztályvezető előadása 4.dia. www.katasztrofavedelem.hu/letoltes/tuzvedelem/eloadas/2/fulep_zoltan_eloadas.pdf

[7] www.lotosz.hu/tuzvedelemkorszerusites, saját gyűjtés.

[8] Saját gyűjtés a Térkép24.hu és a 43/2012 Főigazgatói Intézkedés 1. számú melléklete alapján. A +2 a riasztási időt jelenti.

[9] Saját gyűjtés a 43/2012 Főigazgatói Intézkedés 1. számú melléklete alapján

[10] Lubica Bátová: medzinárodná spolupráca HaZZ a hasicskych jednotiek Slovenskej republiky s hasicskymi zbormi a ostatnymi záchrannymi zlozkami susednych státov pri zdolávaní mimoriadnych údalostí. FIRECO 2005, konferencia anyag.

[11] Fire Ingeneering Monography. Zvolen, 2002, 25. Oldal

A cikk a TÁMOP-4.2.1.B-11/2/KMR-0001 Kritikus infrastruktúra védelmi kutatások projekt támogatásával készült.

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Kozák Attila
kozaka24@gmail.com

SZABOLCS-SZATMÁR-BEREG MEGYE TŰZVÉDELMI LEFEDETTSÉGE

Absztrakt

Az Országgyűlés 2011. szeptember 19-én elfogadta a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvényt, amely egységes elvek mentén szervezi meg a hivatásos katasztrófavédelmi szervezetrendszert, mint a közbiztonság fenntartásának egyik elemét. A katasztrófavédelem jelenlegi jogszabályi környezetének átfogó módosításával, a minősített időszakok rendszerének megújításával, a bekövetkezett katasztrófa esetén irányadó rendkívüli intézkedések megteremtésével, az állam szerepvállalásának növelésével fokozható a lakosság életének, vagyonának biztonsága, valamint biztosítható az ország működőképességének folyamatos fenntartása.[1]

On 19 September 2011 the Parliament adapted Act no. CXXVIII of 2011 on disaster relief and the amendment of certain related acts. This law organises the official disaster protection organisational system based upon standardised principles, which is one of the elements of maintaining public security. The security of the population's life and property can be enhanced and the continuous maintenance of the country's functioning can be provided by the overall modification of the current legislative environment of disaster relief and the reformation of the system of qualified periods, in the case of any disasters taking place, the creation of the normative extraordinary actions and the increasing of state role.[1]

Kulcsszavak: *katasztrófavédelem, lefedettség, védekezés, irányítás, törvény, intézkedés ~ disaster relief, coverage, protection, management, act, action*

A SZABÁLYOZÁS FŐBB IRÁNYAI AZ ALÁBBIAK SZERINT ÖSSZEGEZHETŐ:

1.A veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védelem erősítése (pl. az engedélyezési eljárások kiterjesztése, a veszélyes áruszállítással kapcsolatos hatósági hatáskörök átalakítása).

2.A polgári védelem szerepének erősítése (a polgári védelmi szervezetek alkalmazásának fejlesztése a polgári védelmi hatósági és szakhatósági jogkörök bővítésével)

3.A veszélyhelyzeti szabályozás megújítása, a katasztrófaveszélyre, valamint a veszélyhelyzetre vonatkozó irányítási szabályok lefektetése. Ennek eredményeként javul a védekezés, a kárelhárítás hatékonysága és a veszélyhelyzet kihirdetése elkerülhetővé válhat azzal, hogy a kormány a veszélyhelyzeti szabályozás egyes elemeit indokolt esetben, elsősorban a helyreállítás és az újjáépítés zavartalan lebonyolítása érdekében a katasztrófakárosító hatása által érintett területen bevezetheti.

4.A tűzvédelem egységes irányításának biztosítása (a hivatásos önkormányzati tűzoltóságok állami kézbe vonása, egységes állami tűzoltóság létrehozása). Az önkormányzatok terheinek

csökkentése érdekében a katasztrófavédelmi törvénycsomag a hivatásos tűzoltóságokat ismét állami irányítás alá vonja, ezzel javul hazánk mentő-tűzvédelmi lefedettsége, illetve, hogy a

katasztrófavédelem közelebb kerüljön a lakossághoz, Magyarország lakossága az ország minden pontján azonos védelemben részesüljön.

Dolgozatomban az utóbbiról ejtenék bővebben szót. A tűzvédelem egységes irányításának biztosítása (egységes állami tűzoltóság létrehozása) a tűz elleni védekezés biztosítása – mint a rendvédelmi feladatok része – történetileg az állam által ellátott legelső funkciók egyike. Alapvető fontosságú annak biztosítása, hogy az állam területén élő lakosság valamennyi tagja számára – lakóhelyétől függetlenül – e szolgáltatás magas színvonalon hozzáférhető legyen, ezért a törvény célul tűzi ki a tűzvédelmi szervezetrendszer elaprózódásából adódó területi kiegyensúlyozatlanságok megszüntetését.

Az új törvény alapján a jelenleg az önkormányzatok irányítása alatt álló, helyi érdekektől befolyásolt, és a helyi anyagi lehetőségek függvényében változó hatékonysággal működő hivatásos tűzoltóságok megszűnnek, a feladatellátásért viselt felelősség, és ezzel együtt a feladatellátást szolgáló összes eszköz és szervezet is az államra száll.

A korábbi szervezet helyébe lépő, centralizáltan felépülő állami tűzoltóság működtetése során a központi irányítás létrejötte a tűzoltási és műszaki mentési tevékenységgel összefüggő szakmai követelmények egységes elvek mentén történő érvényesítését és számon kérhetőségét, az erőforrások átlátható módon történő allokációját eredményezi.

A meglévő kapacitások jobb hatásfokú kihasználása, területi elosztásának centrális megszervezése, az erő- és eszközállomány optimális tervezése és mozgatása hatékonyabb, területileg egységes színvonalú tűzvédelmet eredményez, és a források ésszerű felhasználását teszi lehetővé.

1. ORSZÁGOS TŰZVÉDELEM – MŰKÖDÉSI TERÜLETEK, AZ ÚJ EGYSÉG, A KATASZTRÓFAVÉDELMI ŐRS

1.1 Jogszabályi változás – Az új katasztrófavédelmi törvény

A fent ismertetett változtatásokat a katasztrófavédelem rendszerében nemcsak a jogszabályi változások, hanem a tapasztalatok is szükségessé tették. A változásokat az Országos Katasztrófavédelmi Igazgatóság főigazgatója, Bakondi György tű. altábornagy egy 2012 januárjában, a BM Országos Katasztrófavédelmi Főigazgatóság által szervezett, az önkéntes tűzoltó egyesületek első országos találkozóján tartott beszédében foglalta össze.[1]

Bakondi György a megújult katasztrófavédelem rendszerét egy új időszak kezdetének nevezi amely a szándékok szerint perspektívákat vázol fel az önkéntes szervezetek számára. „Ez azért nagyon fontos – szögezi le a főigazgató - mert az önkéntes egyesületek rendkívüli értéket képviselnek a tűzvédelem rendszerében, azok tagjai ugyanis szabadidejükben igyekeznek a bajbajutottak segítségére lenni. A katasztrófavédelem vezetésének eltökélt szándéka, megtalálni annak a módját, hogyan lehet az önkéntes egyesületek súlyát, társadalmi elismertségét növelni, miként lehet a hivatásosokkal való partnerséget erősíteni."

A tábornok a katasztrófavédelemben 2010 óta zajló változásokat érintve beszélt azokról a jogszabályi változtatásokról, amelyek a megtörtént esetek, így a borsodi árvíz, a vörösiszap-katasztrófa, a West Balkán tragédia tanulságainak felhasználásával történtek meg. A törvények és szabályzók kidolgozásakor a megelőzésre helyezték a hangsúlyt, éppen ezért az önkéntesekkel (az önkéntes tűzoltóságokkal) való együttműködésben is meg kell találni azokat a hatósági feladatokban meglévő kapcsolódási pontokat, amelyekkel ezek a szervezetek is támogathatják a prevenciót.

Számos megyében működik már önkéntes mentőszervezet, amelyek speciális felkészültségükkel és eszközeikkel dolgoznak helyi közösségükért, éppen ezért különösen fontos a velük való szoros együttműködés. Hasonló kapcsolatra törekszik a katasztrófavédelem az önkéntes karitatív szervezetekkel, illetve az önkéntes tartalékos katonai szervezetekkel is.

Bakondi György szerint előző években a közösségi érdekek háttérbe szorultak az egyéni érdekekhez képest, és ezzel egy időben az öngondoskodás is gyengült, mindez a köztestületi tűzoltóságoknál is éreztette hatását, lemorzsolódott azok önkéntes háttere. Erőtlenné vált a megelőzést szolgáló hatósági fellépés is, jogköröket veszített a katasztrófavédelem, létszámát és pénzügyi lehetőségeit tekintve is meggyengült. Így fordulhatott elő, hogy nem volt rálátása a panelprogramra éppúgy, mint az országon áthaladó veszélyes szállítmányok jó részére sem.

Az elvégzett munkája azt célozta – mondta el a tábornok - hogy sok más mellett új alapokra helyeződjék a vízgazdálkodás, a szórakozóhelyek működtetése, vagy éppen a kritikus infrastruktúrák védelme.

„Meg kellett teremteni a hivatásos szervezet egységes irányítási rendszerét, emellett az eszközellátottságában és felkészültségében is heterogén szervezetet homogénné kell tenni. Változtatni kellett a védelemigazgatás és a polgári védelem rendszerén is" – mondta Bakondi György.

Ennek szellemében készült a január elsejével hatályba lépett katasztrófavédelmi törvény. A közösségért tenni akaró emberek speciális tudásának megszerzését, felkészítését támogatja a szervezet, ezért tavasztól egységes képzési rendszerbe integrálva oktatják őket, és igazolványt is kaphatnak. Az évi 120 millió forintos működési támogatás mellett védőfelszerelésekkel, eszközökkel látják le őket a hivatásos tűzoltóságok segítségével. A cél az, hogy a katasztrófavédelem valamennyi településen jelen legyen.

[1] A katasztrófavédelem számít az önkéntes egyesületekre. In: http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_hirek&hirid=906

Hazánk mentő tűzvédelmének biztosítása alapvetően a hivatásos tűzoltóságok feladata, azonban az állam bizonyos katasztrófa-, illetve tűzvédelmi feladatokat civil szervezetek bevonásával kíván ellátni. Ilyenek például a speciális mentőszervezetek és a tűzoltó egyesületek. A hivatásos tűzoltóságok – áprilistól 105 hivatásos tűzoltó-parancsokság és 65 katasztrófavédelmi kirendeltség működik és mellettük három év alatt 64 katasztrófavédelmi őrs is segíti a tűzvédelmet – működési területükön folyamatosan biztosítják a települések tűzvédelmét, ám helyenként a vonulási idő aránytalanul magas. Ennek csökkentéséhez, a fehér foltok lefedettségének javításához a jelenlegi gazdasági körülmények között elengedhetetlen az önkéntes mozgalom közreműködése.

Az önkéntes tűzoltóknak nincs tűzoltás-, műszaki mentés vezetési jogosultságuk, tehát erő-eszközeik a műveletirányító tervben nem tervezhetők, de ha jól működnek, jelentős segítséget jelentenek a lakosság biztonsága érdekében végzett munkában.

2011-ben a tűzoltóságok 69 ezer 830 vonulást hajtottak végre, ebből a regisztrált 298 önkéntes tűzoltó egyesület több mint 2800 esetben avatkozott be. Magyarország katasztrófavédelmi feladatainak ellátásában továbbra is fontos szerepe van az önkéntes szervezeteknek, köztük a tűzoltó egyesületeknek is. A tűzoltási és műszaki mentési tevékenységet alapszabályukban vállaló ÖTE-k a működési terület szerinti hivatásos tűzoltósággal kötnek együttműködési megállapodást, szakmai tevékenységüket a hivatásos tűzoltóságok és a katasztrófavédelmi kirendeltségek ellenőrzik.

1.2. A katasztrófavédelmi őrsök – megoldás a „fehér foltokra”?

Toldi Péter tű. őrnagy a Katasztrófavédelem c. folyóirat 2012.májusi számában publikált írásában az új szabályozás egyik eleméről, a katasztrófavédelmi őrsök megalakításáról értekezik. Mint írja, az önkormányzati és a létesítményi tűzoltó-parancsnokságok működési területek meghatározásakor az volt a szempont, hogy az adott települést leghamarabb elérő tűzoltóság erői vonuljanak az adott területre. A hatékony tűz elleni védekezést és a műszaki mentés eredményességét nagyban befolyásolja, hogy a jelzéstől számítva mikor érkeznek és kezdik meg a beavatkozást az eseményhez riasztott erők.

„Ebből kiindulva. az ideális megoldás az lenne, ha minden településen lennének tűzoltói beavatkozásra alkalmas erők és eszközök, vagyis településvédelem lenne. Ez ellen szól azonban, hogy a káresetek gyakorisága az egyes településeken jelentős különbségeket mutat. Ha azonban azt nézzük, hogy vannak olyan települések, amelyeken alacsony a káresetek száma, kérdés: valóban indokolt-e minden egyes településen biztosítani a tűzoltáshoz szükséges technikai eszközöket és a képzett tűzoltói erőt.[2]” - írja Toldi Péter.

Egyes települések azonban, amelyekre a segítő erők 25 percnél hosszabb idő alatt érkeznek ki, ezek gyakorlatilag „fehér folton” találhatók. Ezekben az esetekben a beavatkozás hatékonysága jelentősen romolhat.

„A leterheltség csökkentésének és a működési terület hatékonyabb tűzvédelmének biztosítása érdekében a fejlesztés egyik lehetőségét a hivatásos beavatkozói létszám emelésében, új állomások és őrsök létesítésében látom[3]”- írta értekezésében Komjáthy László.

A mentő tűzvédelem újraszervezésének egyik alapelve, hogy a településeket 25 percen belül elérjék. A távlati cél ezt az időt a lehető legkisebbre csökkenteni. A katasztrófavédelmi őrs a HTP-k tűzoltási és műszaki mentési feladatainak ellátására létrehozott, a parancsnokság székhelyétől eltérő állomáshelyen működő hivatásos tűzoltó egység, amely a hivatásos tűzoltóság működési területének meghatározott részén 24/48 órás készenléti jellegű szolgálati rendben végzi feladatait.

---

[2] Toldi Péter: Katasztrófavédelmi õrsök helye és szerepe a tûzvédelmi rendszerben. In: Katasztrófavédelem, 2012. május

[3] Komjáthy László: Magyarország tűzvédelmi helyzete az EU tagság függvényében, tekintettel a közigazgatási reform és a tűzvédelmi képzés helyzetére. Doktori értekezés 44. oldal, 2005.

Toldi Péter szerint az őrsprogram keretében tehát nem önálló parancsnokságot telepítenek ki, hanem egy már meglévő részeként, annak székhelyétől távolabb, a működési területen belül, a „fehér foltok” közelébe helyeznek egy gépjárműfecskendőt (néhány különleges szert is) fél, illetve egy rajjal. Ez növeli azon települések számát, ahol a beavatkozásra alkalmas erők jelen vannak, és elérhetővé válik, hogy az első beavatkozás gyorsabban megkezdődjön.

A káresetek felszámolásáról szóló statisztikák azt mutatják, hogy a beavatkozások jelentős

része egyes riasztási fokozatban, egy gépjárműfecskendővel történik. Az elmúlt négy év mutatói szerint a káresetek 62-73 százaléka felszámolható volt ilyen erőkkel. Ez azt jelzi, hogy az őrsre tervezett erő és eszköz elegendő, jelenlétük nagymértékű javuláshoz vezet. Az őrsök telephelyének kiválasztásakor elsődleges szempont, hogy „fehér folton” legyen, legyen a településen megfelelő laktanyaépület, vagy kialakítására lehetőség. 2011-ben a megyei katasztrófavédelmi igazgatóságok közreműködésével megtörtént a lehetséges helyszínek felmérése.

A rendelkezésre álló állami tulajdonú létesítmények mellett több, az önkormányzatok által felajánlott létesítményt vagy telket szemrevételeztek, ezek közül választották ki az őrsök helyszínét. A tervek szerint 2014 végéig 65 katasztrófavédelmi őrs alakul meg.

Az őrsök működéséhez szükséges gépjárművet és technikai eszközt a hivatásos tűzoltó-parancsnokságok meglévő eszközeinek kihelyezésével, vagy az eddig tartalékban tartottakból biztosítanak.

2012. április elsején 16 katasztrófavédelmi őrs kezdte meg működését: az ezek számára rendelkezésre álló épületek megfelelőek voltak, vagy csak kismértékű átalakítást kellett rajtuk végezni ahhoz, hogy a szükséges feltételek biztosíthatóak legyenek. A működéshez szükséges létszám és technikai eszköz is megvolt. Az idei év végéig további három őrs kezdheti meg működését, 2013-ban a tervek szerint húsz, 2014-ben pedig 26 katasztrófavédelmi őrs indulhat.

„Az őrsök kialakításával az ország lefedettsége a mentő tűzvédelem szempontjából az alábbiak szerint módosul: a katasztrófavédelmi rendszer átalakításával, a katasztrófavédelmi őrsök beindításával elérjük azt a célt, hogy valamennyi bajbajutott állampolgár megsegítésére 25 percen belül érkezik tűzoltó egység, a lakosság 70 százalékához tíz percen belül. A cél, hogy a kiérkezési idő minél rövidebb legyen, lehetőség szerint hazánk teljes lakossága tíz percen belül kapjon segítséget. Ezt további katasztrófavédelmi őrsök felállításával, az önkéntes tűzoltói mozgalom előtérbe helyezésével, a tűzoltói létszám, illetve eszközpark növelésével, fejlesztésével érhetjük el” – fogalmaz Toldi Péter

Kiérkezés ideje →	Ellátott lakosság % →	Ellátott terület %¶
25 perc →	99,49 →	97,90¶
20 perc →	97,34 →	92,01¶
15 perc →	83,85 →	62,59¶
10 perc →	70,27 →	40,50¶

1. táblázat. Az OKF által 2014-ig tervezett lefedettség
(forrás: Katasztrófavédelem, 2012. május)

2. SZABOLCS-SZATMÁR-BEREG MEGYE TŰZVÉDELME

2.1. A megye – adatok és tények

Szabolcs-Szatmár-Bereg megye Magyarország legkeletibb megyéje. Északkeletről Ukrajna, dél-keletről Románia délnyugatról Hajdú-Bihar megye, északról Borsod-Abaúj-Zemplén megye és Szlovákia határolja.

A megye az Észak-alföldi régióban fekszik, székhelye Nyíregyháza. Területe 5936,45 km², 560 429 fő (2010. január 1.-án közölt adatok szerint), népsűrűsége 96,1 fő/km². 229 településsel rendelkezik, amelyből egy megyei jogú város, emellett 26 várossal rendelkezik (a legnagyobbak ezek közül Mátészalka, Kisvárda, Nyírbátor, Tiszavasvári, és Újfehértó).

2.2. A megyei katasztrófavédelmi igazgatóság

A katasztrófavédelem kelet-magyarországi rendszerében kiemelt szerepet tölt be a Szabolcs-Szatmár-Bereg Megyei Katasztrófavédelmi Igazgatóság. A szervezet országos hatáskörű központi szerve az Országos Katasztrófavédelmi Főigazgatóság, amely a polgári védelem és az állami tűzoltóság országos és területi szerveiből összevont, államigazgatási feladatot is ellátó országos hatáskörű rendvédelmi szerv. A területi szervek a megyei igazgatóságok, amelyek alárendeltségében helyi szervként katasztrófavédelmi kirendeltségek működnek.

Vállalt feladataik szerteágazóak és sokrétűek: a katasztrófák, valamint a veszélyes anyagok által okozott súlyos balesetek elleni megelőzéstől és felkészüléstől, az anyagi javakat fenyegető hatások elleni védekezésen és beavatkozáson át egészen a helyreállítási feladatokban vállalt feladatokig terjednek. A szervezet ellátja a hazai tűzvédelmi rendszer felügyeletét is.

A megyében 4 kirendeltség (Fehérgyarmat, Kisvárda, Mátészalka, Nyíregyháza) és 4 Hivatásos Tűzoltó Parancsnokság (Nyírbátor, Kisvárda, Mátészalka, Nyíregyháza) működik.

Feladatuk a katasztrófák elleni védekezésre történő felkészülés, a lakosság védelme, a veszélyhelyzetek megelőzése és a károk felszámolásában való közreműködés.

Az őrsprogramnak keretében a megyénkben már működő Záhonyi Katasztrófavédelmi Őrs mellett, most két újabb Őrs Fehérgyarmaton és Baktalórántáházán kezdte még működését januártól.

Tekintsük át a két új őrs történetét!

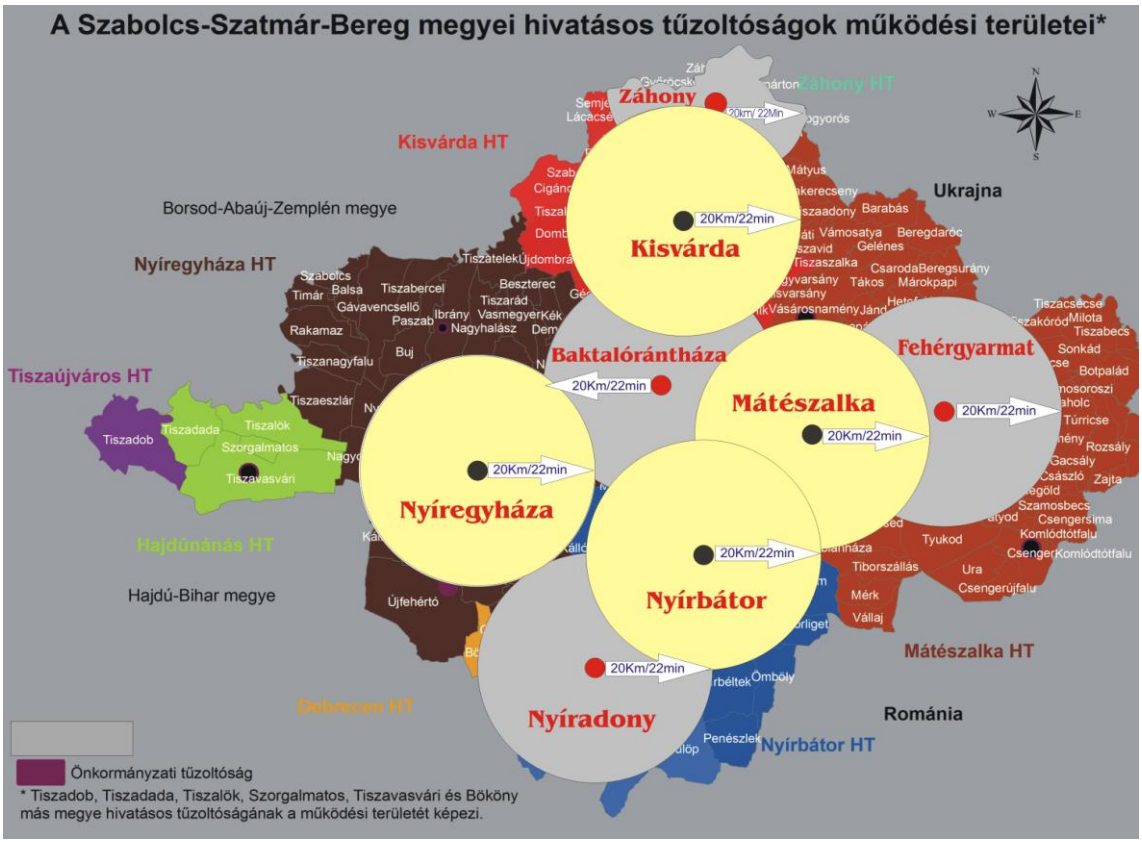
Baktalórántházán a Nyírbaktai Önkéntes Tűzoltó Egyesület 1925-ben hozták létre 12 fővel, a tűzoltók egyenruhával rendelkeztek. Ekkor az egyesület ellátta Nyírkércs és Nyírjákó csatolt községek mentő tűzvédelmét is. Az egyesület a több évtized alatt a Baktalórántházi Köztestületi Tűzoltósággá, majd Önkormányzati Tűzoltósággá alakult át. Hosszú előkészítő tevékenységet követően az újonnan létesülő Baktalórántházi Katasztrófavédelmi Őrs 2013-án kezdte meg munkáját. Az őrs, mint a Nyírbátori Hivatásos Tűzoltó parancsnokság egysége, napi 4 fővel 19 településen (471 km^2-en) élő 37245 ember védelmét biztosítja.

A Fehérgyarmati Önkéntes Tűzoltó Egylet működését 1882. szeptember 28-án hagytak jóvá.

Az idők folyamán a tűzoltó egylet tűzoltó egyesületté, majd 2005. december 1-jén Fehérgyarmati Önkéntes Tűzoltósággá alakult. 2013. január 1-ével Fehérgyarmat és környékének tűzvédelmének érdekében létrejön a Fehérgyarmati Katasztrófavédelmi Őrs. Az őrs, mint a Mátészalkai Hivatásos Tűzoltó parancsnokság egysége, napi 4 fővel 67 településen (1062 km^2-en) élő 48587 ember védelmét biztosítja.

A megyében ezzel mintegy hetven fővel, 530 főre bővült a hivatásos állomány, a növekmény a polgári védelemi szervezetből átkerült civilek mellett lényegében a két új őrs létszámát jelenti. A 229 településsel rendelkező Szabolcs-Szatmár-Bereg megyében Nyíregyházán, Mátészalkán és Kisvárdán alakultak katasztrófavédelmi kirendeltségek.

A fehérgyarmati hivatásos kirendeltség létrehozásával régi probléma és szükség oldódott meg: a szatmári és beregi térségben. A mátészalkai kirendeltség irányítása alatt Mátészalka és Nyírbátori Hivatásos Tűzoltó parancsnokság látja el 89 település mentő-tűzvédelmét. Ezek ugyan jól működnek, de mellettük szükség van egy hivatásos egységre (Fehérgyarmat), mivel a mátészalkai katasztrófavédelmi kirendeltség nem tudja ezt a viszonylag nagy területet egyedül ellátni. A másik, Baktalórántházán létrehozott őrs 19 hivatásos tűzoltóval alakult meg; az eddig a köztestületi tűzoltóság által használt laktanyát pedig az önkormányzat térítésmentesen átadta a katasztrófavédelem részére.



1. ábra. A Szabolcs-Szatmár-Bereg megyei hivatásos tűzoltóságok működési területei (forrás: Nyíregyháza Megyei Jogú Város, Geodézia és Térképészeti Zrt)

A cél, hogy a riasztást követően 25 percen belül mindenhová kiérjenek a tűzoltók mentő tűzvédelem érdekében. A térképen jól látható Szabolcs Szatmár Bereg megye 2013. január 1.-től érvényes tűzvédelmi lefedettsége. A körök méretarányosak és jól láthatóak: sárga színnel a Hivatásos Tűzoltó parancsnokságok, szürke színnel pedig a katasztrófavédelmi őrsök működési területét jelöltem. Megyei illetékesség szintjén három őrs működik, de a lefedettség javítása érdekében a határos Hajdú-Bihar megyében szintén január 1.-től működő nyíradonyi katasztrófavédelmi őrs hét település mentő tűzvédelmét biztosítja 20 percen belüli kiérkezési idővel. További kutatásomba táblázat formájában kívánom részletesen bemutatni Szabolcs-Szatmár-Bereg megye tűzvédelmi lefedettségét. Táblázatomban azokat a megyei településeket soroltam fel, melyek még így is 20 percen túl kapnak segítséget. A táblázatból parancsnokságonként látható, hogy hivatásos egységtől 25 percen túl (csillaggal jelölve) is vannak települések. Forrásként a település lélekszámát a népesség nyilvántartásból gyűjtöttem, távolság méréséhez útvonaltervező programot használtam. A vonulási időt az Országos Katasztrófavédelmi Főigazgatóságra vonatkozó hatályos BM rendelete egy kilométer megtételét egy percben határozza meg. A táblázatnál figyelembe veszem, hogy a riasztási idő 120 másodperc; olyan egyéb objektív tényezőket nem vettem figyelembe, mint

jelzésfelvételi idő, vasúti átjáró, valamint az évszakok közti vonulási időkülönbségeket is befolyásoló tényező lehet.

Nézzük részletesen milyen ma a helyzet ma a megye mentő tűzvédelmi biztonsága területén.

Település	Működési terület	km	idő	Lélekszám
*Gégény	Kisvárda	26	28	2018
Gyüre	Kisvárda	21	23	247
*Kisvarsány	Kisvárda	25	27	987
*Lácacséke	Kisvárda	35	37	360
Nagyvarsány	Kisvárda	22	24	1535
Tiszamogyorós	Kisvárda	22	24	709
Újdombrád	Kisvárda	20	22	700
*Zemplénagárd	Kisvárda	25	27	842

2. táblázat. Kisvárda Hivatásos Tűzoltó parancsnokság működési területén található települések. A csillaggal megjelölt teleülések huszonöt perc mentő tűzvédelmi lefedettségen kívül esnek. (saját)

Település	Működési terület	km	idő	Lélekszám
*Csenger	Mátészalka	33	35	4913
*Csengerújfalu	Mátészalka	38	40	838
*Jánd	Mátészalka	31	33	814
*Lónya	Mátészalka	52	54	749
*Mátyus	Mátészalka	51	53	338
*Olcsva	Mátészalka	25	27	670
*Pátyod	Mátészalka	28	30	641
*Pórcsalama	Mátészalka	23	25	2663
*Pusztadobos	Mátészalka	25	27	1334
Rohod	Mátészalka	20	22	1255
*Szamosanygyalos	Mátészalka	31	33	523
*Tiszaadony	Mátészalka	43	45	659
*Tiszakerecseny	Mátészalka	47	49	922
*Tiszaszalka	Mátészalka	38	40	871
*Tiszavid	Mátészalka	39	41	476
*Ura	Mátészalka	35	37	665
*Vállaj	Mátészalka	23	25	933
*Vásárosnamény	Mátészalka	25	27	8964

3. táblázat. Mátészalka Hivatásos Tűzoltó parancsnokság működési területén található települések. A csillaggal megjelölt teleülések huszonöt perc mentő tűzvédelmi lefedettségen kívül esnek. (saját)

A táblázatokból kiderül, hogy Kisvárda Hivatásos Tűzoltó Parancsnokság működési területén négy település 25 percen túl kap segítséget, az itt élő lakosságlétszám összesen 4207 fő. Mátészalka működési területén 17 település 2697 fő kap hivatásos egységtől 25 percen túl segítséget.

Település	Működési terület	km	idő	Lélekszám
*Ömböly	Nyírbátor	23	25	475
*Penészlek	Nyírbátor	24	26	1005

4. táblázat. Nyírbátor Hivatásos Tűzoltó parancsnokság működési területén található települések. A csillaggal megjelölt teleülések huszonöt perc mentő tűzvédelmi lefedettségen kívül esnek (saját)

Település	Működési terület	km	idő	Lélekszám
*Balsa	Nyíregyháza	33	35	860
*Beszterec	Nyíregyháza	27	29	1068
*Buj	Nyíregyháza	20	22	2364
*Érpatak	Nyíregyháza	28	30	1766
*Gávavencsellő	Nyíregyháza	31	33	3686
*Ibrány	Nyíregyháza	23	25	6979
*Kék	Nyíregyháza	23	25	1990
Nagyhalász	Nyíregyháza	21	23	5770
*Paszab	Nyíregyháza	24	26	1324
*Rakamaz	Nyíregyháza	28	30	5015
*Szabolcs	Nyíregyháza	35	37	432
*Tímár	Nyíregyháza	30	32	1428
*Tiszabercel	Nyíregyháza	25	27	1970
*Tiszaeszlár	Nyíregyháza	28	30	2758
*Tiszanagyfalu	Nyíregyháza	25	27	1930
*Tiszarád	Nyíregyháza	24	26	603
*Tiszatelek	Nyíregyháza	29	31	1527
Vasmegyer	Nyíregyháza	21	23	1710

5. táblázat. Nyíregyháza Hivatásos Tűzoltó parancsnokság működési területén található települések. A csillaggal megjelölt teleülések huszonöt perc mentő tűzvédelmi lefedettségen kívül esnek (saját)

település	Működési terület	km	idő	Lélekszám
Demecser	Baktalórántháza KÖ (Nyírbátor HTP)	22	29	4440

6. táblázat. Baktalórántháza Hivatásos Katasztrófavédelmi őrs működési területén található település. A csillaggal megjelölt település huszonöt perc mentő tűzvédelmi lefedettségen kívül esik (saját)

Nyírbátor működési területén két település közel 1500 fő. Nyíregyháza működési területén 15 település 33336 fő esik 25 perces lefedettségen kívül. Baktalórántháza esetében egy település van 25 perces lefedettségen kívül.

település	Működési terület	km	idő	Lélekszám
Benk	Kisvárda HTP (Záhony KÖ)	21	23	2018

7. táblázat. Záhony Hivatásos Katasztrófavédelmi őrs működési területén található település (saját)

település	Működési terület	km	idő	Lélekszám
*Beregdaróc	Fehérgyarmat KÖ (Mátészalka HTP)	26	28	791
Beregsurány	Fehérgyarmat KÖ (Mátészalka HTP)	20	22	640
*Botpalád	Fehérgyarmat KÖ (Mátészalka HTP)	28	30	578
*Csaroda	Fehérgyarmat KÖ (Mátészalka HTP)	25	27	627
*Császló	Fehérgyarmat KÖ (Mátészalka HTP)	23	25	391
Csegöld	Fehérgyarmat KÖ (Mátészalka HTP)	20	20	625
*Csengersima	Fehérgyarmat KÖ (Mátészalka HTP)	24	26	658
*Gacsály	Fehérgyarmat KÖ (Mátészalka HTP)	24	26	899
*Garbolc	Fehérgyarmat KÖ (Mátészalka HTP)	33	35	148
*Gelénes	Fehérgyarmat KÖ (Mátészalka HTP)	30	32	545
*Kishódos	Fehérgyarmat KÖ (Mátészalka HTP)	37	39	98
*Kispalád	Fehérgyarmat KÖ (Mátészalka HTP)	31	33	548
*Komlódtótfalu	Fehérgyarmat KÖ (Mátészalka HTP)	28	30	113
*Magosliget	Fehérgyarmat KÖ (Mátészalka HTP)	35	37	243
*Méhtelek	Fehérgyarmat KÖ (Mátészalka HTP)	32	34	721
*Milota	Fehérgyarmat KÖ (Mátészalka HTP)	30	32	849
*Nagyhódos	Fehérgyarmat KÖ (Mátészalka HTP)	35	37	115
*Rozsály	Fehérgyarmat KÖ (Mátészalka HTP)	27	29	782
Sonkád	Fehérgyarmat KÖ (Mátészalka HTP)	21	23	716
*Szamosbecs	Fehérgyarmat KÖ (Mátészalka HTP)	25	27	362
*Tákos	Fehérgyarmat KÖ (Mátészalka HTP)	26	28	2170
*Tiszabecs	Fehérgyarmat KÖ (Mátészalka HTP)	28	30	1007
*Tiszacsécse	Fehérgyarmat KÖ (Mátészalka HTP)	28	30	237
*Tiszakóród	Fehérgyarmat KÖ (Mátészalka HTP)	25	27	779
*Tisztaberek	Fehérgyarmat KÖ (Mátészalka HTP)	24	26	623
Túrricse	Fehérgyarmat KÖ (Mátészalka HTP)	21	23	635
*Uszka	Fehérgyarmat KÖ (Mátészalka HTP)	32	34	356
*Vámosatya	Fehérgyarmat KÖ (Mátészalka HTP)	33	35	565
*Zajta	Fehérgyarmat KÖ (Mátészalka HTP)	29	31	413

8. táblázat. Fehérgyarmat Hivatásos Katasztrófavédelmi őrs működési területén található település. A csillaggal megjelölt teleülés huszonöt perc mentő tűzvédelmi lefedettségen kívül esnek. (saját)

Fehérgyarmat működési területén 24 település 12618 főt érint a le fedettségi hiányosság. Záhony katasztrófavédelmi tűzoltó őrs területén nincs 25 percen túli lefedetlen település. A mentő-tűzvédelem az integrált katasztrófavédelem szerves eleme. Életmentés, tűzoltás, árbelvízvédelem ellen személyi és technikai felszereltsége a hivatásos, önkormányzati és önkéntes tűzoltóságoknak van ma Magyarországon a leggyorsabb reagálási képességgel. Ezt a státuszt nem is célszerű feladni. Minden magyar állampolgár elvárja, hogy egyforma segítséget kapjon az ország bármely pontján. Kutatásom által bemutatott 3. ábrán és az alatta kigyűjtött táblázatokban jól látható, hogy, Szabolcs-Szatmár-Bereg megyében a 229 települést tekintve 167 településen biztosított a 20 percen belüli mentő tűzvédelem. A hivatásos katasztrófavédelmi őrs program létrehozásával 62 településen az összes települések 27%-án 78298 fő, a lakosság összességét figyelembe véve 14% van a mentő tűzvédelem 25 percen túl biztosítva hivatásos tűzoltó egységgel.

A 2. ábra más lefedettségi képet mutat. Kutatásom során említést kell tenni, hogy ma Magyarországon működnek így a megyében is önkormányzati tűzoltó parancsnokságok. Jelenleg hat hivatásos önkormányzati tűzoltó parancsnokság: Ibrány, Újfehértó, Szakoly, Vásárosnamény, Tiszavasvári, Csenger önkormányzati tűzoltóságok működik a megyében. Az önkormányzati tűzoltó parancsnokságoknak elsődleges műveleti körzetük van: nyolc perces riasztási idővel kell a mentő tűzvédelmet biztosítaniuk. A bajban önálló beavatkozásra

képesek tűz és káresetnél fél vagy egy teljes rajjal egyaránt képesek beavatkozásra. A kell szót azért használtam, mert ezek a parancsnokságok törvényi keretek között vállalták műveleti körzetükben a kárelhárítást. A forrást számukra jelenleg az önkormányzatok és az állam adja az Országos Katasztrófavédelmi Főigazgatóság útján, szigorú havi elszámolási kötelezettséggel. Az önkormányzati tűzoltóságok támogatása egyébként differenciált, vagyis minél fehérebb folton található a tűzoltóság, annál nagyobb forrást biztosítanak működéséhez.

2. ábra. Szabolcs Szatmár Bereg Megye tűzvédelmi lefedettsége Önkormányzati tűzoltóságokkal (saját)

Mai hatályos jogszabályok szerint az önkormányzati tűzoltóságok hivatásos tűzoltó parancsnokságok működési területén belül elsődleges műveleti területükön avatkoznak be, akár önállóan is. A riasztást a megyei ügyelettől kapja és az önkormányzati tűzoltóságok is tervezve vannak a megyei műveletirányításnál, nyolc perces riasztási idővel számolva. A kiérkező önkormányzati tűzoltó parancsnokság tűzoltás vezetője kiérkezés után a káresetek helyszínén kérhet további segítséget a megyei ügyeleten keresztül. A katasztrófavédelem által pajzs rendszernek hívott jelzésfelvétel során automatikusan meghatározza, hogy az adott településre milyen egységek vonulnak biztosítani a mentő, tűzvédelmet, szem előtt tartva a költséghatékonyságot. A káresethez kiérkező első hivatásos egység az új katasztrófavédelmi rendszerben át kell vegye az irányítást az önkéntes tűzoltó parancsnokságtól.

Amennyiben a második térképet megfigyeljük, már teljesen más képet mutat a tűzvédelmi lefedettség még akkor is, ha nyolc perc a riasztási idő az önkormányzati tűzoltóságoknak. A Megyei Katasztrófavédelmi Igazgatóság tájékoztatása szerint a megyében működő önkormányzati tűzoltó parancsnokságok 2012-ben az ellenőrzések során minden esetben tartották a hivatásos tűzoltó parancsnokságok riasztási normaidejét, parancsnokságonként eltérően fél, vagy teljes rajjal. Amennyiben az önkormányzati tűzoltóságokat figyelembe vesszük a mentő tűzvédelem lefedettségében akkor a megyében nincs olyan település, mely 25 percen kívül kapna tűzoltói segítséget.

3.ÖSSZEGZÉS

2012. január 1.-től Magyarországon a mentő tűzvédelem állami feladat, így a mentő tűzvédelem, mint közbiztonság a rendvédelmi szervek eleme lett. Beágyazottsága bizonyítja. hogy a társ rendvédelmi szervek a nemes feladatot teljes mértékben elismerik. Minden állampolgár elvárja, hogy azonnal segítséget nyújtsunk és cserébe az erkölcsi támogatást kapjuk.

Megállapítható, hogy az önkormányzati intézményrendszerben nem teljesen ágyazódott be a tűzoltóság feladatköre. Máshoz nem hasonlítható szakmaisága miatt valamikor az önkormányzati képviselőtestületekkel más-más döntéseket hoztak, mint egyéb önkormányzati intézményekről. Többek között ez hívta életre az egységes állami rendvédelmi feladatok közé a tűzoltóságot, ezen belül a mentő tűzvédelem ismét állami szerepvállalását. Tűzoltóság államosítása után az állampolgárok továbbra is elvárják az egyenlő esélyt tűzoltáskor, műszaki mentéskor, ár- belvízvédelemnél és a katasztrófahelyzetekben.

Kutatásom során megállapítottam, hogy a megyében pozitív az elmozdulása a „fehér foltok"felszámolásában. A tűzoltó őrsprogram nagyban hozzájárul a lefedettség javításában, de még mindig nem elegendő az állampolgárok egyenlőségéhez a mentő tűzvédelem területén.

Az önkormányzati tűzoltó parancsnokságok nagymértékben hozzájárulnak a megye tűzvédelméhez. Figyelemre méltó, hogy technikai felszereltségük helyenként jobb, vagy közel azonos az állami tűzoltóságok ellátottságával. Képesítésük már alacsonyabb szinten van, mint a hivatásos tűzoltóké, mely abból adódik, hogy az önkormányzati tűzoltók forrásuk jelentős részét fenntartásra, felülvizsgálatra és bérre költik. Képzésekre-, gyakorlatra csak a kötelező minimális szintet teljesítik.

Ez abból fakad, hogy jövőjük bizonytalan. 2013-tól létrehozott járási rendszer kialakításánál az önkormányzatok kevesebb forrásból és szigorúan célzott költségvetésből gazdálkodnak. A tűzvédelem pedig állami feladat lett. Következésképpen a megyében található hat önkormányzati tűzoltóság fenntartása közvetlen veszélybe került. Ma megmondhatatlan hogy melyik önkormányzat fogja az állammal közösen fenntartani az önkormányzati tűzoltóságokat.

Ebből az elgondolásból kiindulva további vizsgálatot igényel, hogy ténylegesen melyik önkormányzati tűzoltóságot lenne szélszerű őrsprogram keretében állami irányítás alá vonni. Ezek a tűzoltóságok eszközparkjai épületei helyben maradnának, és ugyanúgy biztosítanának állami irányítás alatt a mentő tűzvédelmet. Így az önkormányzatok által beinvesztált forrás sem veszne el, valamint a jól képzett helyismerettel rendelkező tűzoltók hivatásos állományúak lehetnének, emellett életpályát adhatna az ott élő, jelenleg bizonytalanságban dolgozó fiatal tűzoltóknak. Ez a stratégia már nem csak elsődleges műveleti körzetről szólna, hanem a hivatásos őrs nagyobb terület tűzvédelmét is biztosítani tudná, vagy segítségnyújtás tekintetében távolabb is tervezhető lenne. Természetesen ez a gazdaság fellendülésén is múlik.

A tűzvédelemi lefedettség javításának reális lehetősége az önkéntes tűzoltóság életre hívása lenne. A megyében valamikor virágzott az önkéntes tűzoltóságok. A rendszerváltás után és az önkormányzati tűzoltóságok kialakulása miatt elkezdett hanyatlani az önkéntesek hivatástudata. De ebben más tényezők is közrejátszottak: a köztestületi tűzoltóságok megalakulása, fiatalok elvándorlása a településről. A tűzoltószövetség megyei szinten évente egyszer szervezett egy tűzoltóversenyt és évente összegyűjtötte a pályázatokat, az elnyert pénzekből képzéseket szerveztek. Természetesen található ellenpélda is a megyében; de ahol a település lakossága polgármester és a parancsnok egy célért küzd, ott van eszköz, képzettség és önkéntes segítség.

Ma a helyi közösségeknek is fel kell ismerni a társadalmi felelősség fogalmát tűzvédelem területén, illetve nem csak állami feladatként kell tekinteni a segítségnyújtásra.

Az Országos Katasztrófavédelmi Főigazgatóság elgondolásai is ebbe az irányba mutatnak. Szükséges a műveletirányítási rendszert kiterjeszteni és fejleszteni az önkéntes tűzoltóságok felé. Az önkéntes tűzoltóságok közül is fel kell mérni objektíven, hogy melyik településen szükséges az önkéntes tűzoltóságot úgy felfejleszteni, hogy önállóan is be tudjon avatkozni. Melyik önkéntes egyesület az, amelyik a hagyományőrzés miatt érdemes támogatással fenntartani. Összességében az önkéntes tűzoltóság egy közösségnevelő hatást is gyakorol az ott élőkre, valamint hozzájárul a fiatalok megbecsüléséhez.

Ma az ország vezetésének egyszerre kell megküzdeni a lefedettség biztosításának csökkentésével, az őrsprogram fejlesztésével, az önkéntes tűzoltóság fellendítésével, a mentő tűzvédelem technikai és személyi fejlesztésével.

Elgondolásom szerint a fentiek sorrendiségét nem kell felcserélni, mert elsődleges államilag biztosítani a tűzvédelemi lefedettséget. Önkormányzati tűzoltóságot - ha szükséges - őrssé kell átalakítani, valamint fontos, hogy az önkéntesség üzenete se vesszen el a magyar társadalomban. Nem utolsósorban megfelelő lefedettséghez megfelelő technika szükséges és folyamatos képzés. Ezekből az elgondolásokból kiindulva lehet a mentő tűzvédelmi lefedettség hatékonyságát növelni, mely közép és hosszú távon nagymértékű javulást eredményez - eredményezhet.

Felhasznált irodalom

[1] Priskin Győző: Előterjesztés Tét város önkormányzati képviselő-testületének 2011.12.21-én megtartandó ülésére

[2] http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_hirek&hirid=906

[3] Toldi Péter: Katasztrófavédelmi őrsök helye és szerepe a tűzvédelmi rendszerben. In: Katasztrófavédelem, 2012. május

[4] Komjáthy László: Magyarország tűzvédelmi helyzete az EU tagság függvényében, tekintettel a közigazgatási reform és a tűzvédelmi képzés helyzetére. Doktori értekezés 44. oldal, 2005.

A cikk a TÁMOP-4.2.1.B-11/2/KMR-0001 Kritikus infrastruktúra védelmi kutatások projekt támogatásával készült.

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Kozák Attila
kozaka24@gmail.com

SZABOLCS-SZATMÁR-BEREG MEGYE EGYÜTTMŰKÖDÉSE A SZOMSZÉDOS ORSZÁGOK KATASZTRÓFAVÉDELMI SZERVEZETEIVEL

Absztrakt

Magyarország katasztrófavédelmi veszélyeztetettség terén az emberi tevékenységeken kívül a természeti jelenségek is nagy veszélyforrást jelentenek. Ez különösen igaz Szabolcs-Szatmár-Bereg megyére ár- és belvíz veszélyeztetettség szempontjából. A közelmúltban többször előfordult határokon átívelő katasztrófahelyzet, amely szükségessé tette a Katasztrófavédelem és más szakhatóságok munkáját. A katasztrófahelyzeteket előidéző környezeti veszélyt, kockázatot rejtő jelenségek bekövetkezősége, esetleges hatásuk és terjedésük vizsgálata Magyarország és a szomszédos partnerországok kiemelt feladata. Sok esetben nehézséget jelent a szomszédos országok katasztrófavédelmi szerveinek hatékony együttműködése az elkülönült védelmi rendszerek miatt. Írásomban szeretném bemutatni a határon átnyúló pályázatok nyújtotta új lehetőségeket a természeti katasztrófák előrejelzésének fejlesztésében.

In Hungary both human activities and natural phenomena entail high risks concerning disaster relief risk. This is particularly true for Szabolcs-Szatmár-Bereg County in terms of flood and internal water risk. Disaster situations have occurred several times recently, which has necessitated the work of the disaster relief and other authorities. Investigating the predictability, potential effect and extent of phenomena entailing an environmental danger is a key task for Hungary and the neighbouring partner countries. In many cases it is difficult for the disaster relief organs of the neighbouring countries to co-operate efficiently owing to the isolated protection systems. In this article I aim to present the new opportunities offered by the cross-border applications in the development of forecasting natural disasters.

Kulcsszavak: *információ, katasztrófa, biztonság, riasztási terv, beavatkozás ~ information, catastrophe, safety, alarm plan, intervention*

1.EGYÜTTMŰKÖDÉS A SZOMSZÉDOS ORSZÁGOK KATASZTRÓFAVÉDELMI SZERVEZETEIVEL

A katasztrófahelyzeteket előidéző környezeti veszélyt és kockázatot rejtő jelenségek bekövetkezése, esetleges hatásuk és terjedésük vizsgálata minden állam kiemelt feladata. A természetben előforduló események, mint amilyenek az erdőtüzek, árvizek, egyéb katasztrófák, nem állnak meg az ember által mesterségesen meghatározott országhatároknál. Számos esetben nehézséget jelent a szomszédos országok katasztrófavédelmi szerveinek hatékony együttműködése, az elkülönült védelmi rendszerek következtében. Korábban is előfordultak katasztrófahelyzetek, de az elmúlt tíz évben az időjárási szélsőségek megszaporodtak, így korábban kevésbé tapasztalt rendkívüli aszályok, szárazságok és heves, nagy mennyiségű csapadékos időszakok viszonylag rövid időn belül válthatják egymást. A száraz időszakokban jelentősen megnőtt az erdőtüzek száma, míg a nagy csapadékokat követően az árvizek is jelentős károkat okoznak. Az elmúlt évek nem megfelelő erdőgazdálkodása tovább fokozza ezeket a jelenségeket.

A természeti jelenségeken kívül az emberi tevékenységek is veszélyforrást jelentenek. Romániában és Magyarországon a közelmúltban többször előfordult a határokon átívelő katasztrófahelyzet, amely szükségessé tette a katasztrófavédelem, továbbá a vízügy és a környezetvédelmi szakhatóságok összehangolt munkáját. Különösen igaz ez az erdőtüzekre, amelyek rövid idő alatt nagy területre terjedhetnek ki, az árvizekre, amelyek emberéleteket és anyagi javakat veszélyeztető katasztrófa helyzeteket idézhetnek elő. Az elhárítás költségeit jelentősen csökkentheti az időben és térben pontos információk hatékony áramlása. A projekt megvalósulásával olyan infokommunikációs kapcsolat épül ki, amely a határon átnyúló együttműködést jelentősen erősíti a térségben. A természeti erőforrások és anyagi javak védelmében érintett szervek közti korábbi együttműködést tovább erősíti a megvalósuló projekt, amely csökkenti az éles helyzetek kezelésekor a határ által okozott akadályt.

A Szabolcs-Szatmár-Bereg Megyei Katasztrófavédelmi Igazgatóság határon átnyúló tevékenységei, együttműködései az alábbiak:

1.1. Norvég alapú (magyar-ukrán) pályázat

A pályázat célkitűzései között szerepel, hogy Ukrajna és Magyarország partnerei között egy valós, magyar-ukrán határon átnyúló kapcsolat alakuljon ki. A pályázatban a Záhonyi térség kockázatainak felmérésén, térképezésén, valamint a terjedési modellek kidolgozásán túl további célként határozzák meg, a határon átnyúló műveletirányítási terv elkészítését, valamint egy infokommunikációs hírlánc kialakítását is. A határon átnyúló kapcsolattartás, valamint a határon átnyúló információáramlás különösen fontos az országhatárral érintett megyéknél, így a mi megyénkben is. Országunk sajátos adottságait tekintve alvízi ország, így a hozzánk érkező vizekhez alkalmazkodnunk kell. Ebből fakadóan megyénk legnagyobb potenciális veszélyforrása az árvíz, illetékességi területünk 38,3 %- a árvízzel veszélyeztetett.

A megyénk legjelentősebb folyója a Tisza (235 km). A levonuló árhullámok 16-32 óra alatt érik el területünket, ezért a védekezésre történő felkészülésre rövid idő áll rendelkezésünkre. A Tisza folyó Tiszakóródtól - Zsurkig terjedő részén, jobb parti töltésszakadás, esetleges töltésmeghágás esetén, a kiáramló víz magyar területekről, ukrán területekre folyhat, ezáltal veszélyeztetheti az ott élő polgári lakosság biztonságát. A Magyarországról átfolyó víz gravitációs úton a természetes terepvonulatokat követve jut át ukrán területekre, majd a káros vizek a Csaronda csatornán keresztül kerülnek visszavezetésre a Tiszába.

A megyei Kitelepítési - Befogadási Összesített Tervben 9 település – Beregdaróc, Barabás, Beregsurány, Csaroda, Gelénes, Lónya, Mátyus, Tiszaadony, Tiszakerecseny – Ukrajnán keresztül történő kimenekítésével számolunk, ha Vásárosnamény fölött a Tisza jobb partján

gátszakadás következik be. Ez mintegy 3400 főt érint. Többek között ez is eredményezte a pályázat mielőbbi benyújtását[1].

1.2. Infó-kommunikációs hírlánc kialakítása

A webes kapcsolatok sokszínűségét figyelembe véve a két partnernek a legtöbb lehetősége az infokommunikációs rendszer kialakítására elektronikus kapcsolat útján létrehozható. A weben keresztül ugyanis többféleképpen is kapcsolatot tudunk tartani a nemzetközi együttműködő szervekkel a katasztrófák mielőbbi elhárítása és megelőzése céljából.

Az információk hatékony áramlása érdekében a költséghatékonyság figyelembe vételével kialakításra került a webes felületen működő internet alapú közös elektronikus levelező rendszer, valamint a Skype programmal mindkét partnernek lehetősége nyílik a határon át történő kapcsolattartásra. A partnerek webes kapcsolat segítségével azonos e-mail rendszeren keresztül tudnak e-mail kapcsolatot tartani, továbbá a Skype program használatával lehetőség nyílik videó konferenciák lebonyolítására, valamint ezen a szoftveren keresztül ingyenes és azonnali telekommunikációra, adatok küldésére és fogadására van lehetőség a szervezetek számára.

Az e-mail összeköttetés a gmail internetes levelező rendszeren keresztül működik, mely kiválasztására azért került sor, hogy egyforma e-mail rendszeren keresztül működjön a kapcsolattartás mindkét nemzetközi katasztrófavédelmi szerv részéről. A két kapcsolati lehetőség üzembiztonsága és külső behatolástól való védelme megfelelő, mivelhogy csak regisztrált felhasználóként tudják használni a két kapcsolati megoldást. Így az infokommunikációs védett kapcsolatok között zajlik folyamatosan. A tervezett két rendszer működtetése megoldható külső terepen való munkavégzés során is, mivelhogy megfelelően beállítható rendszernek bizonyulnak hordozható számítógépes rendszereken alkalmazva is. Így akár a kihelyezett vezetési pontok összeköttetését is biztosíthatják, természetesen mobil internet kapcsolat alkalmazásával.

2. EGYÜTTMŰKÖDÉSEK A SZOMSZÉDOS ORSZÁGOKKAL

2.1. Határon átnyúló Riasztási - Műveletirányítási Terv

Műveletirányítási terv a Szabolcs-Szatmár-Bereg Megyei Katasztrófavédelmi Igazgatóság és az Ukrán Rendkívüli Helyzetek Minisztériumának Kárpátaljai Megyei együttműködése, kapcsolatainak folyamatos fenntartása és fejlesztése, továbbá a két megye lakosságának biztonsága és védelme, az időben és megfelelő módon történő kölcsönös tájékoztatás, valamint a természeti és civilizációs katasztrófák elleni védelem és egyéb súlyos, határon átnyúló hatású balesetekkel kapcsolatos megelőző, veszélyelhárító tevékenység elhárítására készült. A terv rögzíti, hogy a megyei szintű katasztrófák vagy azok veszélye, illetve a másik fél területére kiható katasztrófahelyzet vagy veszély esetén, a megyei katasztrófavédelmi szervek haladéktalanul információkat cserélnek a fellépő vagy fenyegető katasztrófa idejéről, jellegéről, méreteiről és veszélyeiről, továbbá segítik annak elhárítását.

A terv tűzesetek eloltására, műszaki mentést igénylő események felszámolására és a katasztrófák elleni védekezésre irányuló terv, amely a Szabolcs-Szatmár-Bereg Megyei Katasztrófavédelmi Igazgatóság és az Ukrán Rendkívüli Helyzetek Minisztériumának Kárpátaljai Megyei Igazgatóságának, hivatásos és önkéntes tűzoltóságainak, szervezeteinek, erőinek és eszközeinek, igénybevételének rendjét határozza meg. A terv alkalmazásához szükséges a másik fél segítségigénylő adatlapjának kitöltése, mely nyomtatvány két nyelven (magyar és ukrán) készült a könnyebb kitölthetőség és a nyelvi nehézségek elkerülése miatt. A segítségigénylő adatlap duplikálva érkezik meg a segítséget nyújtó szervezet felé (e-mail és fax), amit nyugtázás után megerősítenek.

A Riasztási terv és az infokommunikációs hírlánc kialakítása és beüzemelése, az időben történő riasztás pontos megbízható információk alapján, megfelelő szintű, modern kommunikációs eszközök segítségével (interaktív kommunikáció) megvalósult. Ezt bizonyítja az is, hogy a pályázatban rögzítettek szerint megszervezésre került az infokommunikációs hírlánc működésének bemutatása céljából a közös magyar-ukrán törzsvezetési gyakorlat is.

2.2. Magyar - Román pályázatok

Mint már a fentiekben említettem, a megyénk legnagyobb potenciális veszélyforrása az árvíz, illetékességi területünk 38,3 %- a árvízzel veszélyeztetett.. A Románia felől érkező nagyobb folyók a Szamos, a Kraszna, és a Túr. A hazai és romániai árvíz- és katasztrófavédelmi központok közötti biztonságos és stabilan üzemelő információs rendszer megvalósítása érdekében a jelenlegi meglévő mikrohullámú gerinchálózat kiterjesztését terveztük. A kirendeltségek beintegrálásával lehetőség nyílna az eddiginél pontosabb előrejelzések készítésére a kölcsönös együttműködés jegyében. Ennek alapfeltétele egy stabil, független, saját üzemeltetésű kapcsolat létesítése az érintett védelmi központok, kirendeltségek között, valamint a közös beavatkozásokat megalapozó lokalizációs és kitelepítési tervek kidolgozása, a felkészültség megteremtése.

A határon átnyúló együttműködés szükségessége ebben az esetben az ár- és belvízi védekezés sajátosságából ered, ahol az információk időben történő feldolgozása és a gyors reagálás létfontosságú elem. Nemzeti árvíz-megelőzési program részeként több beavatkozási, veszély-elhárítási elemzés is készült a megyében, amely rámutat ezen információk szükségességére.

Számos esetben nehézséget jelent a szomszédos országok katasztrófavédelmi szerveinek hatékony együttműködése, az elkülönült védelmi rendszerek következtében.

A természeti jelenségeken kívül az emberi tevékenységek is veszélyforrást jelentenek. Romániában és Magyarországon a közelmúltban többször előfordult a határokon átívelő katasztrófahelyzet, amely szükségessé tette a katasztrófavédelem, továbbá a vízügy és a környezetvédelmi szakhatóságok összehangolt munkáját. Különösen igaz ez az erdőtüzekre, amelyek rövid idő alatt nagy területre terjedhetnek ki, az árvizekre, amelyek emberéleteket és anyagi javakat veszélyeztető katasztrófa helyzeteket idézhetnek elő. Az elhárítás költségeit jelentősen csökkentheti az időben és térben pontos információk hatékony áramlása. A projekt megvalósulásával olyan infokommunikációs kapcsolat épül ki, amely a határon átnyúló együttműködést jelentősen erősíti a térségben.

A természeti erőforrások, és anyagi javak védelmében érintett szervek közti korábbi együttműködést tovább erősíti a megvalósuló projekt, amely csökkenti az éles helyzetek kezelésekor a határ által okozott akadályt. A rendszer adatainak hozzáférése, a hálózat bővítése megnöveli a katasztrófavédelemben résztvevő szervezetek hatékonyságát. A helyzet közös elemzése, a feladatok konstruktív megbeszélése megalapozott döntés-előkészítést és döntéshozatalt eredményezhet, támogatja a katasztrófavédelmi tevékenység gördülékenyebbé tételét. A megvalósulás esetén olyan előrejelző, illetve kommunikációs rendszer jön létre, melynek kölcsönösen használhatja mindkét ország a katasztrófahelyzetek kezelése során. Ezzel jelentős időt nyernek a katasztrófa helyzetek elhárításával kapcsolatban [2].

Ez olyan új és hasznos rendszert eredményez a területen, amely a természeti erőforrások, a lakosság és anyagi javainak megóvását eredményezi. A hatékonyan és jól működő hálózat alkalmazása példaértékű lenne és várható lenne annak kiterjesztése a szlovák és ukrán határ menti területeken is. A projekt során a veszélyhelyzetekre való időben történő felkészülés, illetve a bekövetkezett katasztrófák által okozott károk csökkentése is megvalósul. Ennek keretében olyan szoros együttműködés és kapcsolatrendszer alakul ki a katasztrófavédelem, a vízügy szervei között, amely megsokszorozza a cselekvési lehetőségeket.

A rendszer biztosítja a megfontolt irányítást és intézkedést a legrövidebb időn belül, a szükséges segítségnyújtás és a közvetlen segítség elérhetővé válik az érintettek számára. A létrehozott rendszer lehetővé teszi a beavatkozás nyomon követhetőségét annak érdekében, hogy meghatározhasson megfelelő beavatkozási intézkedéseket a fontos paraméterek változása esetében (veszélyeztetettségi szintek, tendenciák, egyes eseménytípusok bekövetkezési valószínűségei). A létrehozandó honlap értékes információkkal szolgál majd a lakosságnak és minden érintett szervezetnek.

A portál fóruma a régió érintett szervezeteinek és képviselőinek találkozóhelye lesz majd, és nyitott lesz azok számára is, akik csatlakozni szeretnének a vészhelyzeti irányításhoz (jótékonysági szervezetek, kis- és középvállalkozások, akik anyagi forrásokat és segítséget ajánlanak fel a lehetséges természeti katasztrófák áldozatainak). Mindenféleképpen a lehetőségeinkhez mérten, a megelőzésre kell törekednünk az együttműködések tekintetében is, ezért is fontosak a pontos előrejelzések, valamint a határon átnyúló gyors és megbízható információk közlése.

3.ÖSSZEGZÉS

Megállapítható, hogy a tervezett rendszerek biztosítani fogják a megfontolt irányítást és intézkedést a legrövidebb időn belül. A segítségnyújtás közvetlenül elérhetővé válik az érintettek számára.

Fontos kiemelni, hogy a rendszer képes a beavatkozás nyomon követésére annak érdekében, hogy meghatározható legyen a megfelelő beavatkozás. A rendszer kiépítése és az adatok hozzáférése megnöveli a védelemben résztvevők hatékonyságát, konstruktív döntés-előkészítését eredményezhet, mellyel jelentős idő nyerhető a katasztrófahelyzetek elhárításával kapcsolatban.

A közös projektek hasznos eredménye, hogy mind a lakosság, mind az anyagi javak megóvását eredményezheti, valamint az anyagi károk csökkentésével jelentős állami forrás-tőke takarítható meg.

Felhasznált irodalom

[1] http://www.szabolcs.katasztrofavedelem.hu

[2] http://www.fetikovizig.hu

A cikk a TÁMOP-4.2.1.B-11/2/KMR-0001 Kritikus infrastruktúra védelmi kutatások projekt támogatásával készült.

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Miskey Tamás
miskeytamas@gmail.com

TŰZOLTÁS ÉS BEAVATKOZÁS PROBLÉMÁI KÖZÉPMAGAS ÉS MAGAS ÉPÜLETEKBEN

Absztrakt

A középmagas, magas épületek kiürítése nagyon sok időt vehet igénybe, életeket és vagyontárgyakat kell megmenteni, a tűzoltásnak pedig ezzel párhuzamosan gyorsnak és hatékonynak kell lennie. A hasonló épületek többségét a 60-es, 80-as években építették és az azóta eltelt idő alatt állaguk jelentősen romlott. Elhanyagolt az épületek karbantartása, számos esetben elöregedett elektromos rendszerekkel találkozhatunk. A szellőző rendszerek tisztításának hiánya is komoly problémaként lebeg a fejünk felett, melyet jól tükröznek az elmúlt időszakban bekövetkezett „panelház tüzek" is. A tűzoltás és beavatkozás problémáival azért szeretnék foglalkozni, mivel gyakorló tűzoltóként számos esetben kell azzal szembesülnünk, hogy a lakók az alapvető előírásokat sem tartják be. A feltárt problémákat, tapasztalataimat egy Veszprémben történt középmagas panelépület tűzesetén, keresztül kívánom bemutatni.

It can take a lot of time to evacuate middle-high and high-rise buildings. Not only lives but also assets must be saved, while fire-fighting even must be very quick and effective. The most of these buildings were built in the 60s and 80s, since then their consistence has declined significantly. The conditioning of these buildings are neglected, the cables are often too old, the aerator systems aren't planned properly (there are many problems with cleaning). To my opinion in most cases these problems can be the reason of the fires in the block of flats nowadays. I would like to deal with the problems of fire fighting because a direct fireman has to face the problem that the flat owners do not even keep the essential instructions. I would like to show and introduce you these problems, difficulties and my experiences through a fire in a block of flats, which happened in Veszprém.

Kulcsszavak: *középmagas épület, panelház tűz, tűzoltás ~ middle-high building, fire in a block of flats, fire fighting*

BEVEZETŐ

A vonatkozó Jogszabály szerint: „Középmagas épület: amelyben a legfelső építményszint szintmagassága 13,65 m és 30 m között van. Magas épület: amelyben a legfelső építményszint szintmagassága a 30 m-t meghaladja.” [1].

Magyarország lakosságának jelentős része hasonló épületekben él, ezért rendkívül fontos ezt az összetett kérdéskört vizsgálni. A mentés problémáival azért szeretnék foglakozni, hogy ráirányítsam a figyelmet a téma összetettségére, az ebből fakadó feladatok végrehajtásának nehézségeire. A lakosság szempontjából döntő fontosságú, hogy a beavatkozó tűzoltó rajok feladataikat a lehető leghatékonyabban és gyorsabban hajtsák végre.

Szeretném röviden bemutatni a tűzmegelőzéssel, tűzoltás és beavatkozással foglalkozó kollégáim elképzeléseit, gyakorlati tapasztalatait, melyek segítségével betekintést kaphatunk a középmagas és magas épületekben bekövetkezett tüzek oltása során fellépő nehézségekről is.

ÁLTALÁNOS JELLEMZŐK

A középmagas- és magas épületek sok évtizede épültek, és a korszerűsítés, karbantartás hiányában az elöregedett rendszerek (elektromos, fűtési), valamint a nem megfelelően kialakított szellőző-és közmű csatornák egyre nagyobb gondot jelenthetnek egy esetleges tűzeset során, komoly kihívás elé állítva a beavatkozó rajokat [3].

A középmagas- és magas épületeket nehéz lenne valamilyen rendszer alapján osztályozni és kategóriákba sorolni, ezért megkülönböztetésük három építési, kialakítási módozat alapján lehetséges:

- Larsen-Nielsen típusú lakóépületek,
- sávházak,
- „P” jelű (pontház) középlépcsőházas lakóépületek.

Fentiek közül országos viszonylatban is a sávházak a legelterjedtebbek, ezért a továbbiakban fenti kialakítású épületekkel foglalkozom.

A típus jellemzői, hogy több lépcsőházzal készülnek, melyek az épület közepén találhatóak a liftaknával együtt. A folyósok alaprajza változatos. A lépcsőházak közötti egyedüli összekötetést a tetőn, vagy az alagsorban kialakított átmenő folyósokkal oldják meg. Az esetek döntő többségében ráccsal és lakattal zárják le ezeket az átmenő folyósokat. Az emeleti szintek között magas párkányszintű ablakokkal vannak ellátva a lépcsőházak, ennek következtében a nyitásuk valamint az ablakszárny leszerelése nehéz feladat. A hő-és füstelvezetés hatásfoka nem megfelelő, ezért könnyen alakul ki nagy hő terhelés és nagy mennyiségű elvezetetlen füst. A függőleges födémáttörések nem megfelelően kivitelezettek a konyhai és a vizesblokk szellőző-és közműcsatornájánál.

ÉPÜLETEK KIALAKÍTÁSA, HATÁROLÓ SZERKEZETEK TŰZÁLLÓSÁGA

Panelos kivitelűek a falszerkezetek, tűzállósági határértékük 0,2 és 3 óra között van. A födémszerkezetek határértéke nagyon különböző, a födémre éghető anyaggal építik meg a padozatokat. A válaszfalak 0,5 óra tűzállósági határértékűek, lehetnek égéskésleltetés nélküli, éghető anyagúak, alapterület nagyságától függetlenül egy kikötéssel, irodaépületben 150 m^2-en belül kell maradni létesítéskor. Padlás nincs kialakítva, ezen a szinten kerül elhelyezésre a gépészeti-vagy szerelőszint, itt találhatóak a közműrendszerekhez csatlakozó gépészeti berendezések, pl.: liftgépház, elszívó-és szellőző berendezések. A nyílászáró szerkezetek meghibásodása tűz esetén befolyásoló tényezőként jelentkezik. Közmű, liftakna, szellőztető

berendezés és a szemétledobó miatt nagy számban fordulnak elő olyan födémáttörések, melyeknek kialakítása az érvényben lévő szabályzóknak nem felel meg.[4]

A MENTÉS PROBLEMÁI

A mentésben résztvevők szempontjából problémát jelent a tűz késői észlelése, mert kiérkezéskor már kiterjedt tűzzel találkozhatnak. Az elsőnek kiérkező rajok létszáma meghatározó a feladatok megoszthatósága szempontjából. Már egy szinten lévő tűz oltáshoz és az életmentés megkezdéséhez is legalább 2 teljes raj szükséges. A tűzjelzésből nehéz következtetni a várható helyzetre, feladatokra. A magas hőmérséklet, illetve relatív páratartalom, a látótávolság lecsökkenése, a nagy fizikai és mentális igénybevétel, az elhúzódó mentési feladatok szintén nagy tűrőképességet és fizikai állóképességet igényelnek. A mentésben résztvevők pihentetése nehezen megoldható a tartalékképzés nehézségei miatt.[2]

Az *épületek megközelítése* sok esetben nehéz, mert az úthálózat vezetése, úttengely távolság és a kis kanyarívek nehezíti a mentésre érkező gépjárművek mozgását. A terepadottságok, az épületek környezete sok esetben akadályozzák a magasból mentő gépjárművek alkalmazását és a felvonulási terület megközelítését. A parkoló gépjárművek gyakran akadályozzák a tűzi víz hálózat használatát, veszélyeztetve ezzel az oltás és beavatkozás sikerét.[5]

Tűzkeletkezés szempontjából jellemző a nagy sebességű füstképződés és az épület füsttel való telítettsége. A lépcsőház aerodinamikai jellemzői miatt gyorsan áramlanak az égéstermékek, a keletkező hő és füst a tűz helyszínétől a lépcsőház felé áramlik. A beépített műanyagok és egyéb éghető anyagok égése során felszabaduló égéstermékek többsége sajnos mérgező. Tapasztalatom szerint amennyiben a tűz az épület alsó 2-3 szintjén keletkezik, a füst gyors, függőleges irányú terjedése miatt a lépcsőház 15-20 perc alatt füsttel telítődik. Felkészülve a felderítésre, valamint a benn tartózkodó személyekre, minden esetben légzőkészülékben lehet az épületbe hatolni. A lépcsőházba jutó égéstermékek nagymértékben emelik a hőmérsékletet, mely az emberi bőr számára elviselhetetlen. Romlik a tájékozódás, a látótávolság szinte a nullára csökken.

Tűzterjedés szempontjából a függőleges irányú terjedés gyorsabb a vízszinteshez képest (7-8 méter percenként).[2] Tűzterjedés a legtöbb esetben a födémeken képzett nyílásokon, áttöréseken keresztül (vízvezeték, csatorna, elektromos kábelek, szellőzés), az ablakok kitörése után a homlokzaton, az erkélyek éghető borításán valósul meg. A konkrét veszprémi tűzesetnél is azzal szembesültünk, hogy a szemétledobó is fokozhatja a gyors terjedést, mivel egy mesterséges kürtőként nagy mennyiségű oxigénnel látja el és táplálja a tűzet. Befolyásoló tényező lehet például a felszálló vezetékekben létrejövő nyomásesés több emeleten való vízkivétel miatt, az eltömődött száraz felszálló vezetékek, a fali tűzcsap szekrényben gyakori felszerelések hiánya (sugárcső, tömlő), illetve az üzemi berendezések zavara (áramszolgáltatás, oltóberendezés, lift).[5]

Veszélyforrások szempontjából a forró, toxikus égéstermékek, füstgázok a legveszélyesebbek (kén-dioxid 0,05 tf%, cianhidrogén), melyek már alacsony koncentrációban halálosak. A CO koncentráció zárt térben elérheti a 0,15 tf%-ot, amely az emberi szervezet veszélyes dózisának háromszorosa. Komoly gondot és feladatot jelent továbbá a magas hőmérséklet, illetve relatív páratartalom.[6]

Épületgépészet szempontjából problémát jelent, hogy a legtöbb esetben nincs biztonsági, illetve tűzoltólift. A kialakított szellőzőcsatornák elősegítik a tűz gyors, függőleges irányú terjedését. Jellemzően anyaguk, vagy a bennük lerakódott szennyeződések miatt, a falakon, födémeken átmenő épületgépészeti vezetékek melletti hézagok nem biztosítják a megfelelő tűzgátló leválasztást.

A középmagas- és magas épületek sok évtizede épültek, és a korszerűsítés, karbantartás hiányában az elöregedett rendszerek (elektromos, fűtési), valamint a nem megfelelően kialakított szellőző-és közmű csatornák egyre nagyobb gondot jelenthetnek egy esetleges tűzeset során, komoly kihívás elé állítva a beavatkozó rajokat [3].

A lépcsőházi füstelvezetés berendezéseinek működtetése nem üzembiztos és nehézkes, a lakók nem ismerik a hasznosságát és használatát. Az épületekben elhelyezett száraz felszálló vezetékek többnyire használhatatlanok, karbantartásukra, védelmükre nem fordítanak figyelmet az ott lakók. A fali tűzcsap szekrényekből sokszor hiányzik a felszerelés. A füstmentesítésre tervezett lépcsőházba telepített ventilátorok teljesítménye általában nem megfelelő, az ajtók nem önműködően csukódnak. A tűz hatására a közművekben és az üzemi berendezésekben hibák keletkezhetnek, tehát a gázvezeték, a vízvezeték lezárására és a villamos leválasztásra is minimum egy fél raj kiesik az életmentés megkezdéséből.

Menekülési útvonalak esetében a gyakori egy lépcsőházas megoldás miatt menekülésre a lépcsőház csak a tűz kezdete utáni néhány percben jöhet számításba, később a füst és a magas hőmérséklet miatt ez már nem lehetséges. A tűz feletti szintekről a mentés a megközelítés nehézsége miatt bonyolult. A tetőn létesített, lépcsőházakat összekötő átvezető folyosón a menekülés ritkán biztosított, mivel lezárják, durvább esetekben lehegesztik a kivezető ajtókat, a kulcsot pedig, nem helyezik el a jogszabályokban foglaltaknak megfelelően, amivel komoly nehézséget okoznak a lakókés a mentésükre érkező tűzoltók számára is. Az erkélyek beépítése, valamint a folyosók ráccsal történő lezárása füst esetén végzetes a lakókra nézve, a tűzoltók számára plusz időveszteség.

Gyakran szabálytalan módon és mennyiségben *tárolnak* tűzveszélyes anyagokat a lakók lakásban, pincében, tároló helyiségben, folyosókon, és ezek váratlan helyzetek és feladatok elé állítják a tűzoltókat.

Lakók szempontjából egy tízemeletes épületben a szintenként elhelyezett lakások számától függően, lakásonként 4 emberrel számolva akár 100-400 ember is tartózkodhat, mentésük a helyszínen lévő beavatkozó rajok létszámánál fogva időigényes, nehéz feladat. Az épületekben különböző korosztályú, fizikai állapotú emberek tartózkodnak, nehéz tájékozódni hollétük felől. A mozgáskorlátozottak, gyerekek mentése különösen nagy figyelmet igényel, mivel a gyerekek például hajlamosak elbújni veszély esetén. Tömegriadalom, pánik alakulhat ki, nehéz a lakóktól kapott információkat kezelni. Magasból mentővel, vagy mentőkötéllel végzett mentés veszélyes és időigényes, illetve sok esetben tapasztaltam, hogy a lakók a hő terhelés és füst hatására nem próbálkoznak a meneküléssel. Ennél sokkal rosszabb a helyzet, amikor adott személyeket több alkalommal is le kell vezetni, mivel féltve értékeiket visszatérnek otthonaikba. Ebben az esetben csak a rendőri segítség lehet a jó megoldás, így kizárhatjuk a be, illetve visszahatolókat.

ÖSSZEGZÉS

Célom volt e témával kapcsolatban, hogy röviden bemutassam a tűzoltás és beavatkozással kapcsolatban felmerülő problémákat, gyakorlati kérdéseket.

Bejárások, helyismereti foglalkozások, ellenőrző, vagy begyakorló gyakorlatok során is találkozunk olyan kérdésekkel, hiányosságokkal, melyek a legtöbb esetben a lakók, közös képviselők, vagy a lakásfenntartó szövetkezetek hibájából adódnak.

Hasonló épületekben bekövetkezett tűzesetek kapcsán rendkívül fontos a tűz pontos jelzése és a lehető legtöbb hiteles adat begyűjtése, hiszen az első helyszínre érkező beavatkozó rajok hatékonysága meghatározó lesz az életmentés és oltás terén is.

2010. március 27.-én Veszprémben történt egy olyan tűzeset, amely segítségével igyekeztem megfelelő hitelességgel bemutatni tapasztalataimat és a felmerülő problémákat.

Felhasznált irodalom

[1] 2/2002. (I. 23.) BM rendelet a tűzvédelem és a polgári védelem műszaki követelményeinek megállapításáról

[2] Bleszity János-Zelenák Mihály: *A tűzoltás taktikája II*. Tankönyvkiadó, Budapest, 1986.

[3] Szedlák József: A lakóházi tüzek kockázati tényezői. *Védelem*, IX. évf. (2002) 1. sz. 27-29. p.

[4] Összefoglaló jelentés Veszprém város területén található középmagas épületek átfogó tűzvédelmi ellenőrzéséről 2009. - 2010. években, 2010.12.06

[5] Eseménynapló Veszprém Megyei Jogú Város Hivatásos Önkormányzati Tűzoltósága „C" szolgálati csoport, 2010.03.27

[6] Mi a teendő vegyi baleset esetén? Segédlet a súlyos balesetek elleni védekezés lakossági tájékoztató kiadványhoz. BM Nyomda Kft. 2003., 20.

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Miskey Tamás
miskeytamas@gmail.com

TŰZOLTÁS ÉS BEAVATKOZÁS PROBLÉMÁI KÖZÉPMAGAS ÉS MAGAS ÉPÜLETEKBEN

Absztrakt

A középmagas, magas épületek kiürítése nagyon sok időt vehet igénybe, életeket és vagyontárgyakat kell megmenteni, a tűzoltásnak pedig ezzel párhuzamosan gyorsnak és hatékonynak kell lennie. A hasonló épületek többségét a 60-es, 80-as években építették és az azóta eltelt idő alatt állaguk jelentősen romlott. Elhanyagolt az épületek karbantartása, számos esetben elöregedett elektromos rendszerekkel találkozhatunk. A szellőző rendszerek tisztításának hiánya is komoly problémaként lebeg a fejünk felett, melyet jól tükröznek az elmúlt időszakban bekövetkezett „panelház tüzek" is. A tűzoltás és beavatkozás problémáival azért szeretnék foglalkozni, mivel gyakorló tűzoltóként számos esetben kell azzal szembesülnünk, hogy a lakók az alapvető előírásokat sem tartják be. A feltárt problémákat, tapasztalataimat egy Veszprémben történt középmagas panelépület tűzesetén, keresztül kívánom bemutatni.

It can take a lot of time to evacuate middle-high and high-rise buildings. Not only lives but also assets must be saved, while fire-fighting even must be very quick and effective. The most of these buildings were built in the 60s and 80s, since then their consistence has declined significantly. The conditioning of these buildings are neglected, the cables are often too old, the aerator systems aren't planned properly (there are many problems with cleaning). To my opinion in most cases these problems can be the reason of the fires in the block of flats nowadays. I would like to deal with the problems of fire fighting because a direct fireman has to face the problem that the flat owners do not even keep the essential instructions. I would like to show and introduce you these problems, difficulties and my experiences through a fire in a block of flats, which happened in Veszprém.

Kulcsszavak: *középmagas épület, panelház tűz, tűzoltás ~ middle-high building, fire in a block of flats, fire fighting*

BEVEZETŐ

A vonatkozó Jogszabály szerint: „Középmagas épület: amelyben a legfelső építményszint szintmagassága 13,65 m és 30 m között van. Magas épület: amelyben a legfelső építményszint szintmagassága a 30 m-t meghaladja.” [1].

Magyarország lakosságának jelentős része hasonló épületekben él, ezért rendkívül fontos ezt az összetett kérdéskört vizsgálni. A mentés problémáival azért szeretnék foglakozni, hogy ráirányítsam a figyelmet a téma összetettségére, az ebből fakadó feladatok végrehajtásának nehézségeire. A lakosság szempontjából döntő fontosságú, hogy a beavatkozó tűzoltó rajok feladataikat a lehető leghatékonyabban és gyorsabban hajtsák végre.

Szeretném röviden bemutatni a tűzmegelőzéssel, tűzoltás és beavatkozással foglalkozó kollégáim elképzeléseit, gyakorlati tapasztalatait, melyek segítségével betekintést kaphatunk a középmagas és magas épületekben bekövetkezett tüzek oltása során fellépő nehézségekről is.

ÁLTALÁNOS JELLEMZŐK

A középmagas- és magas épületek sok évtizede épültek, és a korszerűsítés, karbantartás hiányában az elöregedett rendszerek (elektromos, fűtési), valamint a nem megfelelően kialakított szellőző-és közmű csatornák egyre nagyobb gondot jelenthetnek egy esetleges tűzeset során, komoly kihívás elé állítva a beavatkozó rajokat [3].

A középmagas- és magas épületeket nehéz lenne valamilyen rendszer alapján osztályozni és kategóriákba sorolni, ezért megkülönböztetésük három építési, kialakítási módozat alapján lehetséges:

- Larsen-Nielsen típusú lakóépületek,
- sávházak,
- „P” jelű (pontház) középlépcsőházas lakóépületek.

Fentiek közül országos viszonylatban is a sávházak a legelterjedtebbek, ezért a továbbiakban fenti kialakítású épületekkel foglalkozom.

A típus jellemzői, hogy több lépcsőházzal készülnek, melyek az épület közepén találhatóak a liftaknával együtt. A folyósok alaprajza változatos. A lépcsőházak közötti egyedüli összekötetést a tetőn, vagy az alagsorban kialakított átmenő folyósokkal oldják meg. Az esetek döntő többségében ráccsal és lakattal zárják le ezeket az átmenő folyósokat. Az emeleti szintek között magas párkányszintű ablakokkal vannak ellátva a lépcsőházak, ennek következtében a nyitásuk valamint az ablakszárny leszerelése nehéz feladat. A hő-és füstelvezetés hatásfoka nem megfelelő, ezért könnyen alakul ki nagy hő terhelés és nagy mennyiségű elvezetetlen füst. A függőleges födémáttörések nem megfelelően kivitelezettek a konyhai és a vizesblokk szellőző-és közműcsatornájánál.

ÉPÜLETEK KIALAKÍTÁSA, HATÁROLÓ SZERKEZETEK TŰZÁLLÓSÁGA

Panelos kivitelűek a falszerkezetek, tűzállósági határértékük 0,2 és 3 óra között van. A födémszerkezetek határértéke nagyon különböző, a födémre éghető anyaggal építik meg a padozatokat. A válaszfalak 0,5 óra tűzállósági határértékűek, lehetnek égéskésleltetés nélküli, éghető anyagúak, alapterület nagyságától függetlenül egy kikötéssel, irodaépületben 150 m^2-en belül kell maradni létesítéskor. Padlás nincs kialakítva, ezen a szinten kerül elhelyezésre a gépészeti-vagy szerelőszint, itt találhatóak a közműrendszerekhez csatlakozó gépészeti berendezések, pl.: liftgépház, elszívó-és szellőző berendezések. A nyílászáró szerkezetek meghibásodása tűz esetén befolyásoló tényezőként jelentkezik. Közmű, liftakna, szellőztető

berendezés és a szemétledobó miatt nagy számban fordulnak elő olyan födémáttörések, melyeknek kialakítása az érvényben lévő szabályzóknak nem felel meg.[4]

A MENTÉS PROBLEMÁI

A mentésben résztvevők szempontjából problémát jelent a tűz késői észlelése, mert kiérkezéskor már kiterjedt tűzzel találkozhatnak. Az elsőnek kiérkező rajok létszáma meghatározó a feladatok megoszthatósága szempontjából. Már egy szinten lévő tűz oltáshoz és az életmentés megkezdéséhez is legalább 2 teljes raj szükséges. A tűzjelzésből nehéz következtetni a várható helyzetre, feladatokra. A magas hőmérséklet, illetve relatív páratartalom, a látótávolság lecsökkenése, a nagy fizikai és mentális igénybevétel, az elhúzódó mentési feladatok szintén nagy tűrőképességet és fizikai állóképességet igényelnek. A mentésben résztvevők pihentetése nehezen megoldható a tartalékképzés nehézségei miatt.[2]

Az *épületek megközelítése* sok esetben nehéz, mert az úthálózat vezetése, úttengely távolság és a kis kanyarívek nehezíti a mentésre érkező gépjárművek mozgását. A terepadottságok, az épületek környezete sok esetben akadályozzák a magasból mentő gépjárművek alkalmazását és a felvonulási terület megközelítését. A parkoló gépjárművek gyakran akadályozzák a tűzi víz hálózat használatát, veszélyeztetve ezzel az oltás és beavatkozás sikerét.[5]

Tűzkeletkezés szempontjából jellemző a nagy sebességű füstképződés és az épület füsttel való telítettsége. A lépcsőház aerodinamikai jellemzői miatt gyorsan áramlanak az égéstermékek, a keletkező hő és füst a tűz helyszínétől a lépcsőház felé áramlik. A beépített műanyagok és egyéb éghető anyagok égése során felszabaduló égéstermékek többsége sajnos mérgező. Tapasztalatom szerint amennyiben a tűz az épület alsó 2-3 szintjén keletkezik, a füst gyors, függőleges irányú terjedése miatt a lépcsőház 15-20 perc alatt füsttel telítődik. Felkészülve a felderítésre, valamint a benn tartózkodó személyekre, minden esetben légzőkészülékben lehet az épületbe hatolni. A lépcsőházba jutó égéstermékek nagymértékben emelik a hőmérsékletet, mely az emberi bőr számára elviselhetetlen. Romlik a tájékozódás, a látótávolság szinte a nullára csökken.

Tűzterjedés szempontjából a függőleges irányú terjedés gyorsabb a vízszinteshez képest (7-8 méter percenként).[2] Tűzterjedés a legtöbb esetben a födémeken képzett nyílásokon, áttöréseken keresztül (vízvezeték, csatorna, elektromos kábelek, szellőzés), az ablakok kitörése után a homlokzaton, az erkélyek éghető borításán valósul meg. A konkrét veszprémi tűzesetnél is azzal szembesültünk, hogy a szemétledobó is fokozhatja a gyors terjedést, mivel egy mesterséges kürtőként nagy mennyiségű oxigénnel látja el és táplálja a tűzet. Befolyásoló tényező lehet például a felszálló vezetékekben létrejövő nyomásesés több emeleten való vízkivétel miatt, az eltömődött száraz felszálló vezetékek, a fali tűzcsap szekrényben gyakori felszerelések hiánya (sugárcső, tömlő), illetve az üzemi berendezések zavara (áramszolgáltatás, oltóberendezés, lift).[5]

Veszélyforrások szempontjából a forró, toxikus égéstermékek, füstgázok a legveszélyesebbek (kén-dioxid 0,05 tf%, cianhidrogén), melyek már alacsony koncentrációban halálosak. A CO koncentráció zárt térben elérheti a 0,15 tf%-ot, amely az emberi szervezet veszélyes dózisának háromszorosa. Komoly gondot és feladatot jelent továbbá a magas hőmérséklet, illetve relatív páratartalom.[6]

Épületgépészet szempontjából problémát jelent, hogy a legtöbb esetben nincs biztonsági, illetve tűzoltólift. A kialakított szellőzőcsatornák elősegítik a tűz gyors, függőleges irányú terjedését. Jellemzően anyaguk, vagy a bennük lerakódott szennyeződések miatt, a falakon, födémeken átmenő épületgépészeti vezetékek melletti hézagok nem biztosítják a megfelelő tűzgátló leválasztást.

A középmagas- és magas épületek sok évtizede épültek, és a korszerűsítés, karbantartás hiányában az elöregedett rendszerek (elektromos, fűtési), valamint a nem megfelelően kialakított szellőző-és közmű csatornák egyre nagyobb gondot jelenthetnek egy esetleges tűzeset során, komoly kihívás elé állítva a beavatkozó rajokat [3].

A lépcsőházi füstelvezetés berendezéseinek működtetése nem üzembiztos és nehézkes, a lakók nem ismerik a hasznosságát és használatát. Az épületekben elhelyezett száraz felszálló vezetékek többnyire használhatatlanok, karbantartásukra, védelmükre nem fordítanak figyelmet az ott lakók. A fali tűzcsap szekrényekből sokszor hiányzik a felszerelés. A füstmentesítésre tervezett lépcsőházba telepített ventilátorok teljesítménye általában nem megfelelő, az ajtók nem önműködően csukódnak. A tűz hatására a közművekben és az üzemi berendezésekben hibák keletkezhetnek, tehát a gázvezeték, a vízvezeték lezárására és a villamos leválasztásra is minimum egy fél raj kiesik az életmentés megkezdéséből.

Menekülési útvonalak esetében a gyakori egy lépcsőházas megoldás miatt menekülésre a lépcsőház csak a tűz kezdete utáni néhány percben jöhet számításba, később a füst és a magas hőmérséklet miatt ez már nem lehetséges. A tűz feletti szintekről a mentés a megközelítés nehézsége miatt bonyolult. A tetőn létesített, lépcsőházakat összekötő átvezető folyosón a menekülés ritkán biztosított, mivel lezárják, durvább esetekben lehegesztik a kivezető ajtókat, a kulcsot pedig, nem helyezik el a jogszabályokban foglaltaknak megfelelően, amivel komoly nehézséget okoznak a lakókés a mentésükre érkező tűzoltók számára is. Az erkélyek beépítése, valamint a folyosók ráccsal történő lezárása füst esetén végzetes a lakókra nézve, a tűzoltók számára plusz időveszteség.

Gyakran szabálytalan módon és mennyiségben *tárolnak* tűzveszélyes anyagokat a lakók lakásban, pincében, tároló helyiségben, folyosókon, és ezek váratlan helyzetek és feladatok elé állítják a tűzoltókat.

Lakók szempontjából egy tízemeletes épületben a szintenként elhelyezett lakások számától függően, lakásonként 4 emberrel számolva akár 100-400 ember is tartózkodhat, mentésük a helyszínen lévő beavatkozó rajok létszámánál fogva időigényes, nehéz feladat. Az épületekben különböző korosztályú, fizikai állapotú emberek tartózkodnak, nehéz tájékozódni hollétük felől. A mozgáskorlátozottak, gyerekek mentése különösen nagy figyelmet igényel, mivel a gyerekek például hajlamosak elbújni veszély esetén. Tömegriadalom, pánik alakulhat ki, nehéz a lakóktól kapott információkat kezelni. Magasból mentővel, vagy mentőkötéllel végzett mentés veszélyes és időigényes, illetve sok esetben tapasztaltam, hogy a lakók a hő terhelés és füst hatására nem próbálkoznak a meneküléssel. Ennél sokkal rosszabb a helyzet, amikor adott személyeket több alkalommal is le kell vezetni, mivel féltve értékeiket visszatérnek otthonaikba. Ebben az esetben csak a rendőri segítség lehet a jó megoldás, így kizárhatjuk a be, illetve visszahatolókat.

ÖSSZEGZÉS

Célom volt e témával kapcsolatban, hogy röviden bemutassam a tűzoltás és beavatkozással kapcsolatban felmerülő problémákat, gyakorlati kérdéseket.

Bejárások, helyismereti foglalkozások, ellenőrző, vagy begyakorló gyakorlatok során is találkozunk olyan kérdésekkel, hiányosságokkal, melyek a legtöbb esetben a lakók, közös képviselők, vagy a lakásfenntartó szövetkezetek hibájából adódnak.

Hasonló épületekben bekövetkezett tűzesetek kapcsán rendkívül fontos a tűz pontos jelzése és a lehető legtöbb hiteles adat begyűjtése, hiszen az első helyszínre érkező beavatkozó rajok hatékonysága meghatározó lesz az életmentés és oltás terén is.

2010. március 27.-én Veszprémben történt egy olyan tűzeset, amely segítségével igyekeztem megfelelő hitelességgel bemutatni tapasztalataimat és a felmerülő problémákat.

Felhasznált irodalom

[1] 2/2002. (I. 23.) BM rendelet a tűzvédelem és a polgári védelem műszaki követelményeinek megállapításáról

[2] Bleszity János-Zelenák Mihály: *A tűzoltás taktikája II*. Tankönyvkiadó, Budapest, 1986.

[3] Szedlák József: A lakóházi tüzek kockázati tényezői. *Védelem*, IX. évf. (2002) 1. sz. 27-29. p.

[4] Összefoglaló jelentés Veszprém város területén található középmagas épületek átfogó tűzvédelmi ellenőrzéséről 2009. - 2010. években, 2010.12.06

[5] Eseménynapló Veszprém Megyei Jogú Város Hivatásos Önkormányzati Tűzoltósága „C" szolgálati csoport, 2010.03.27

[6] Mi a teendő vegyi baleset esetén? Segédlet a súlyos balesetek elleni védekezés lakossági tájékoztató kiadványhoz. BM Nyomda Kft. 2003., 20.

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Nikodém Edit
nikodem@t-email.hu

FELHASZNÁLHATÓ-E EGY ADOTT ORSZÁG ATOMERŐMŰVE NUKLEÁRIS TERRORTÁMADÁS ESZKÖZEKÉNT, CÉLPONTJAKÉNT?

Absztrakt

A XXI. századi megújuló energiaforrások mellett még mindig az egyik legmeghatározóbb villamosenergia-forrás a nukleáris energia. Legfőbb előnye, hogy előállítása olcsó és – megfelelő üzembiztonsági környezetben – mentes a káros kibocsátásoktól, hatékony és gazdaságos energiaforrás. Mindamellett, hogy ipari, mezőgazdasági, gyógyászati és kutatási területeken is számos esetben alkalmaznak sugárzó (radioaktív) anyagokat, sajnos a történelem során példát kaptunk harcászati és tömegpusztító célzatú felhasználására is. A cikkben bemutatom, hogy egy adott ország atomerőműve egy esetleges harci helyzetben alkalmazható-e nukleáris fegyverként, illetve egy atomerőművel rendelkező ország képes-e nukleáris fegyver előállítására, továbbá érdemi célpontot jelenthet-e egy atomerőmű egy esetleges terrortámadás esetén.

Beside the renewable resources of the 21st century one of the most significant source of electricity is nuclear energy. Its main advantage is that its prime cost is low and – applying appropriate operational safety - it is free of harmful emission, effective and economical energy source. Moreover to the frequent utilization of radioactive matter in the industrial, agricultural, therapeutic and research domains, unfortunately through history we have experienced its application as tactical and mass destruction weapons. In my publication I will present whether a nuclear power plant of a country could be used as a nuclear weapon in a possible military action, in addition the capability of a country possessing a nuclear power plant of producing nuclear weapons, furthermore I will examine if a nuclear power plant might be considered as a high-value target in case of terrorist attack.

Kulcsszavak: *atomerőmű, nukleáris, dúsítás, láncreakció, detektálás, proliferáció, szabályozás, védelem ~ nuclear power plant, nuclear, enrichment, chain reaction, detection, proliferation, regulation, defense.*

BEVEZETÉS

Az állampolgárok többségét még ma is megosztja annak ténye, hogy az otthonába eljutó – mára már létszükségletet biztosító – villamos energia legjavát atomerőmű biztosítja. E fogalmat egyfajta misztikum öleli körül. A világot megrázó (II. Világháború végén bekövetkezett) Hiroshimát /1945. 08. 06./ és az azt követő Nagasakit /1945. 08. 09./ ért atombomba-támadás óta sokan eme energiaforrásra, mint annak fizikai hatásainak tömegpusztító erejére asszociálnak. Nem akarunk róla tudomást venni, azonban be kell látnunk, hogy még ma is léteznek kísérletek atomfegyverek előállítására, de ennek bebizonyítása igen körülményes. Nemcsak azért, mert az efféle atomkísérletek legtöbbször titokban zajlanak (még annak ellenére is, hogy pl. Észak-Korea elismerte, hogy 2006-ban és 2009-ben is tesztelt atomfegyvereket, sőt megerősítette, hogy 2013. februárjában végrehajtotta harmadik kísérleti atomrobbantását). A titkos kísérletekre több jel is utal (például műholdas fényképfelvételek, informátorok közlései), azonban minderről kézzelfogható bizonyítékot a földmozgások által keltett szeizmikus rezgések adnak. A szakértők szerint – mérőműszerekkel kimutatható, hogy – a földrengéstől, bányarobbantásoktól, vulkánkitöréstől, ahol egy törés jellegű elmozdulás keletkezik eltérő szeizmikus hullámmozgás detektálható egy-egy atomfegyver-kísérletet követően, ahol a robbanástól keletkezett erő egyenletesen szétterjedve minden irányban egyforma erővel hat a talajra. Ezek tények, azonban sokakban az a hiedelem él, miszerint, ha egy ország képes atomenergiát előállítani, akkor adottak a lehetőségei nukleáris fegyver létrehozására. Ahhoz, hogy ennek az állításnak a létjogosultságát bebizonyítsuk, avagy cáfoljuk közelebbről meg kell ismerkednünk a békés célú felhasználásra és fegyver előállítására is egyaránt alkalmas legkisebb kémiai egységnek, az atomnak a tulajdonságaival és felfedezésének történetével. Elemeznünk kell továbbá, hogy a nukleáris anyagok szállításával kapcsolatban van-e reális veszélye a terrorcselekményeknek, illetve azt, hogy egy atomreaktor célponttá válhat-e, és ha igen, milyen mértékben válhat veszélyforrássá.

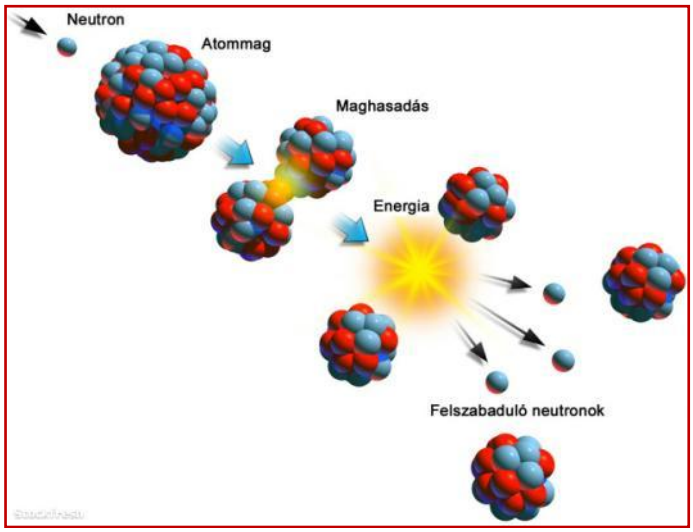
A NUKLEÁRIS PUSZTÍTÓFEGYVEREK ELLŐÁLLÍTÁSÁNAK FELTÉTELEI

Marie Curie, leánykori nevén Marie Sklodowska, (szül.: Varsó, 1867. november 7.) kétszeres Nobel-díjas fizikus, akit a radioaktivitás kutatásában elért eredményei tettek világhírűvé. 1903-ban férjével, Pierre Curie-vel, valamint Henri Becquerellel megosztva kapta meg a fizikai Nobel-díjat és korszakalkotó tudományos tevékenységéért az 1911-es kémiai Nobel-díj egyedüli díjazottja volt. [1] A radioaktivitás mai megfogalmazás szerinti definíciója: „[…] egyes kémiai elemek minden külső behatás, vagy kényszer nélkül is jól meghatározható és könnyen észlelhető sugárzásokat bocsátanak ki. E jelenséget radioaktivitásnak, a kibocsátott sugárzást radioaktív sugárzásnak, a sugárzást kibocsátó elemeket radioaktív elemeknek nevezték el. A radioaktív sugárzás az atommagok bomlásával, átalakulásával van összefüggésben.” [2]

Az emberek félelmének kiindulópontját az atommagban rejlő, elemi szinten jelen lévő energia és annak pusztító hatása jelenti. Csak viszonyításképp: egy atombomba robbanásakor felszabadult energia a TNT robbanóanyag erejének közel egymillió-szorosa. Ez az erő 300m/s-os sebességű lökéshullámot kelt és a keletkezett hő nem kevesebb, mint 5000 °C. Az említett értékek mellett fontos tényező még, hogy a létrejött radioaktív felhőt a szél több száz kilométerre is elviszi és az emberekre gyakorolt pusztító hatást több évig fennálló és tapasztalható sugárszennyezettség is kísérheti. Ez a mérhetetlen pusztító erő egyetlen parányi részecskéből, a már említett atomból ered. Tisztáznunk kell, hogy a fissziós (atommaghasadás elvén működő) atomfegyver előállítása két kémiai elem bármelyikének atomfizikai tulajdonságai felhasználásával lehetséges. Ez a két elem: a plutonium (Pu) és az urán (U). Az

atomerőművek működése során az energia előállításának egyfajta melléktermékeként keletkezik a radioaktív plutonium (239) izotóp. Ebből kifolyólag a plutonium „beszerzése" egyszerűnek bizonyulhat, azonban az atombomba elkészítése már közel sem az. Annak tömegpusztító fegyverként való felhasználásához nagyon körülményes eszközök, eljárások, szakértelem és laboratóriumi körülmények szükségesek, amely e célra való alkalmazása a kívülállók (terroristák) számára szinte megvalósíthatatlan, mérhetetlenül nagy kihívást állít.

Az atomerőművek reaktoraiban és a nukleáris fegyverekben lezajló fizikai és kémiai folyamatok mechanizmusa hasonló. Egy atom belsejében helyezkedik el az atommag, amely pozitív töltéssel rendelkezik. Köztudott, hogy a pozitív töltés taszítja a másik pozitív töltést, azonban az atomot a magerő ennek ellenére mégis összetartja. Amennyiben ez az erő megszűnik, az atommag részei egymástól elszabadulnak. Ezt nevezzük maghasadásnak. A felszabadított részecskék repülés közben újabb atomoknak ütköznek, amelynek következtében hő fejlődik és beindul egy ún. láncreakció.



1. ábra. A maghasadás folyamata neutron besugárzással
Forrás: http://index.hu/tudomany/2012/02/21/teller_ede_is_a_torium_mellett_volt/

Az atombomba működése is ezen az elven alapul. Elemi részecskék közül egy neutront nagy energiával mesterségesen továbbítanak egyetlen urán, vagy plutonium atomba, ezzel egy robbanást idézve elő. Maghasadáskor két-három újabb neutron szabadul fel, amely további atommal találkozva újabb robbanást és maghasadást generál. A felszabaduló energia minden egyes esetben duplázódik. A plutonium esetében az atomot (gömbszerűen) körülölelő robbanóanyaggal kell azt maghasadásra kényszeríteni, amely precíziós atomfizikai, mérnöki és ballisztikai eljárás. Uránt használva az eljárás valamelyest egyszerűbbnek titulálható. Itt az elv, hogy az atommaghasadáshoz két darab 235-ös izotópú uránt ütköztetnek egy bizonyos energiával egymásnak, így elérve az atom kritikus tömegét, amely annak hasadásához vezet. (Az első urán atombombát az Amerikai Egyesült Államok vetette be és dobta le Hiroshimára)

Az atomfegyverek között az uránnal működő bombák működésének tematikája, valamint előállítása is egyszerűbbnek bizonyul, így a terroristák is e megoldást preferálják leginkább. Azonban az urán beszerzése nehéz és körülményes, ugyanakkor tisztítása (dúsítása) gyárméretű laboratóriumokat és igen hosszú tisztítási időt igényel. Az urán természetes környezetéből ércbányászattal nyerhető ki. A kitermelt uránérc a bombakészítéshez szükséges 235-ös uránból kevesebb, mint 1%-ot tartalmaz. A benne lévő többi izotóp az urán 238-as izotóp. Ez utóbbi szennyezőanyagként van jelen, ami meggátolja a láncreakciót. A legnagyobb kihívást jelentő feladat megszabadulni a 238-as izotóptól és kinyerni a tiszta 235-ös izotópot. Ennek az eljárásnak – amit dúsításnak, vagy tisztításnak neveznek – a lényege a minél nagyobb 235-ös izotóp-koncentráció elérése, mivel a bomba működéséhez

elengedhetetlen a legalább 90%-os tisztaságú urán-235 jelenléte. Egy modernkori eljárás során az uránt gáz halmazállapotúvá alakítva egy centrifugának nevezett hengerbe juttatják, ahol nagy sebességgel forgatni kezdik.

2. ábra. Urándúsító centrifugák
Forrás: http://www.dehir.hu/vilag/hatalmas-urandusito-uzem-eszak-koreaban/2010/11/21/

A centrifuga-hatásnak köszönhetően az urán két említett izotópja elkülöníthető egymástól. Ezzel az eljárással 80-100%-os tisztaság érhető el. Léteznek egyéb dúsítási technológiák is (elektromágneses szeparálás, gázdiffúzió, lézer), azonban kijelenthető, hogy ez az ipari technológia csak állami keretek között valósítható meg. Akár az atomreaktorokat, akár az atombomba előállítását vizsgáljuk, az urán dúsításának folyamata mindkét esetben megegyezik. Az eltérés a tisztított urán mennyiségében mérhető, mivel egy atombombához 30 kg szükséges ebből a hasadóanyagból, amelynek tisztításához megközelítőleg 3000 centrifugát kellene üzemelni megállás nélkül egy éven keresztül. Az urándúsítás rendkívül bonyolult, időigényes és nem utolsó sorban precíz folyamat, így kijelenthető, hogy terroristák igen kis valószínűséggel tudnak saját részre tisztított uránt előállítani. Számos ország rendelkezik dúsított uránnal, példaként említve Oroszországban legalább 60 ezer atombombához elegendő urán áll rendelkezésére.

A fentiekből megállapítható, hogy amennyiben rendelkezésre áll minden nukleáris fegyver előállításához szükséges erőforrás, még abban az esetben is problémát okoz a robbanóanyag célba juttatása, mivel csak néhány ország rendelkezik ilyen – a feladatra alkalmas – nagy hatótávolságú ballisztikus rakétával. A terrorszervezetek csak a legritkább esetben képesek ezeknek a feltételeknek a megteremtésére, még akkor is, ha világméretű a szerveződésük.

A NUKLÁRIS ANYAGOK ILLEGÁLIS KERESKEDELMÉNEK MEGAKADÁLYOZÁSÁRA TETT TÖREKVÉSEK

Az előzőekben bemutattam a nukleáris fegyver előállításához szükséges alapfeltételeket, amelyekből egyértelműen levonható az a következtetés, hogy az ilyen típusú pusztító eszközök létrehozásának legfőbb akadálya az előállítás nehézsége. Ebben a fejezetben kitérek azokra a megállapodásokra, utasításokra, amelyek az egyes országokra vonatkozó jogszabályok alapköveiként kerültek kialakításra, illetve a detektálást elősegítő eszközökre, vizsgálva, hogy elég garanciát biztosítanak-e arra, hogy ezek az eszközök ne kerüljenek olyan körökbe, ahol azokat ártó szándékkal használják.

Nemzetközi egyezmények szabályozzák a veszélyes anyagok – ezen belül a radioaktív anyagok – szállítását. Az Európában megalkotott szabályozások alapvetően hasonlóak, de az egyezmények külön kitérnek a szárazföldi (közúti és vasúti), a légi és a vízi (tengeri és folyami) úton történő szállításokra. A legjelentősebb szerepet a közúti szállítási képviseli. Ennek oka, hogy általában a berakodás helyére történő eljuttatás ezen utakon valósítható meg.

A radioaktív anyagok békés célú felhasználásának szabályozása során nagy hangsúlyt fektetnek azok tárolására, szállítására és fuvarozására, amely szigorú előírásoknak és követelményeknek kell, hogy megfeleljen. Ezt alapvetően az 1979. évi 19. törvényerejű rendelettel kihirdetett Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Európai Megállapodás és mellékletei (ADR), valamint az 1986. évi 2. törvényerejű rendelet alapján kihirdetett Veszélyes Áruk Nemzetközi Vasúti Fuvarozásáról szóló Megállapodás (RID), továbbá az 1971. évi 25. törvényerejű rendelet alapján kihirdetett Veszélyes Áruk Légi Szállításának Biztonságát Szolgáló Műszaki Utasítások (ICAO TI) szabályozza.

Magyarországon az ionizáló sugárzást kibocsátó radioaktív anyagok és az önfenntartó, nukleáris láncreakcióra képes vagy képessé tehető anyagok biztonságos alkalmazását szigorú hatósági rendszer felügyeli. Hazánkban az 1996. évi CXVI. törvény (az atomenergiáról) rendelkezik „a lakosságnak és a környezetnek az ionizáló sugárzás káros hatásai elleni védelméről, valamint az atomenergia alkalmazásának szabályozásáról, az ezekkel összefüggő engedélyezési eljárásról, e téren a hatóságok és az atomenergiát alkalmazók alapvető feladatairól, kötelezettségeiről.” [3] A törvényben foglalt kormányzati feladatok végrehajtásáról a Kormány az Országos Atomenergia Hivatal (OAH), valamint az érintett minisztériumok útján gondoskodik, amelyek tevékenységét az atomenergia alkalmazásának biztonsága területén az OAH főigazgatójának vezetésével működő Atomenergia Koordinációs Tanács hangolja össze. Az OAH hatáskörébe tartozik többek között a radioaktív anyagok szállításának engedélyezése a veszélyes áruk szállításáról szóló jogszabályok rendelkezései szerint, valamint a radioaktív anyagok csomagolásának jóváhagyása és ellenőrzése. Ezek alapján az OAH engedélyezi a nemzetközi szállítást és a különösen nagy aktivitású radioaktív anyagok belföldi szállítását. A Hivatal hatáskörébe tartozik továbbá az ezzel kapcsolatos nemzetközi értesítések kiadása és fogadása, valamint a nemzetközi szállítás közben esetleg bekövetkezett rendkívüli eseményeknél szükséges operatív intézkedések kezdeményezése. [3] [4]

A nukleáris hasadóanyagok proliferációjával szembeni legfontosabb feladatnak a Nemzetközi Atomenergia Ügynökség (NAÜ) már hosszú idő óta a nukleáris anyagok fizikai védelmének megerősítését tekinti. Ide tartozik a szigorúbb jogi szabályozások életbe léptetése, a radioaktív anyagok nyilvántartásának pontosítása (precízebb feljegyzések az anyagok adásvételéről, nyilvántartásáról, ellenőrzéséről, valamint eltűnésének körülményeiről), valamint az exportellenőrzés rendszerének hatékonyabbá tétele. A világ feketepiacán a sugárforrásokkal való kereskedelmet – a korszerű detektoros eszközöknek köszönhetően – mára már sikerült a korábbi évekhez képest visszaszorítani, azonban tisztában kell lennünk azzal a ténnyel, hogy a még ma is élénken zajlik a világ legkülönfélébb helyein a radioaktív anyagokkal való illegális tevékenység. A NAÜ központi feladatként kezeli a nukleáris és egyéb radioaktív anyagok védelmét, a legnagyobb kihívást mégis az elmúlt másfél évtized „atom-csempészetének” egyre növekvő tendenciája jelenti. A visszaélések megakadályozásának egyik legfontosabb részét képezi a NAÜ részes országai és hatóságai közötti intenzívebb együttműködés.

A másik fő szempont, hogy mennyire sikerül ezeket az anyagokat detektálni. A radioaktív csempészáruk átvizsgálásához külön erre a célra kifejlesztett detektorokat használnak. Ezeknek a mérőműszereknek három fő típusát különböztetjük meg:

1. Zsebméretű detektorok

3. ábra. GammaRAE II Personal Radiation Detector (PRD)
Forrás: http://www.wormald.co.nz/fire-products/gas-detection-portable/gammarae-ii-personal-radiation-detector

Általában elemmel működő, ütés-és vízálló, könnyen kezelhető, kisméretű detektor. Hátránya, hogy nem minden típusú sugárzást érzékel.

2. Kézben hordozandó és mobil eszközök

4. ábra. Lahore Radiation Detection Devices
Forrás: http://www.pk.all.biz/radiation-detection-devices-g38845

Méretét tekintve nagyobb, mint a zsebméretű (súlya kb. 1-2 kg), de a jobb minőségűekkel az összes típusú sugárzás kimutatható.

3. Rögzített eszközök

5. ábra. Sugárkapu Forrás:
http://www.sciencedirect.com/science/article/pii/S0969804305001569

Ezeket az ún. sugárkapukat leginkább kikötők be- és kijáratánál, repülőtereken, közúti és vasúti határátkelőhelyeken állítják fel. Ezek az eszközök folyamatos áthaladást biztosítanak a

járművek és a gyalogosok részére. Sok esetben még röntgengépekkel is kiegészítik, így azt is ki lehet mutatni, ha valaki fémtárgyba rejti az átcsempészendő anyagot. [5]

A jogi szabályozások, illetve a detektálásra tett törekvések hivatottak a radioaktív anyagok tekintetében az illegális felhasználást kizárni. Különböző egyezmények, megállapodások, szabályok szigorúsága, valamint a detektáló eszközök alkalmazása révén, jelentősen javult a helyzet, a szabályozottság, valamint a szigorú ellenőrzések okán elmondható, hogy a radioaktív anyagokkal végzett tevékenység során kevés eséllyel kerülnek hozzá nem értő, illetéktelen, ártó szándékú kezekbe ezek az anyagok. A radioaktív anyagok eltulajdonításának talán legsebezhetőbb pontja maga a szállítás, így fentiek ellenére nem zárható ki teljes bizonyossággal egy esetleges terrortámadás lehetősége. Elgondolkodtató az is, hogy a terroristák részéről egy nukleáris szállítmány – vagy akár egy atomerőmű – megtámadása csupán elterelő manőverként szolgál. Egy nukleáris fenyegetettség minden figyelmet magára irányít, így eredményesen valósíthatnak meg más, fő célpontok elleni támadást.

NUKLEÁRIS LÉTESÍTMÉNYEK VÉDELME, BIZTONSÁGA

Az előző fejezetben kitértünk a szállítás és a detektálás eredményességét szolgáló alapvető intézkedésekre és eszközökre. Ebben a részben bemutatom, hogy mitől biztonságos egy atomerőmű működése, valamint egy ilyen nukleáris létesítmény jelenthet-e célpontot a terroristák számára.

Minden atomerőművet üzemeltető ország rendelkezik radioaktív anyagokkal. Fontos az atomerőműveken belül a radioaktív anyagok védelme, de ezen túlmenően ki kell zárni annak lehetőségét, hogy azt békés célú rendeltetésén túlmenően is felhasználhassák. Világméretű viszonylatban több mint 400 atomerőmű üzemel aktívan. Ezek többsége uránnal működik, amelynek során az energia előállításának egyfajta melléktermékeként keletkezik a radioaktív plutónium izotóp. Egy esetleges terrortámadás méltó célpontjának tűnhet egy atomerőmű, mivel annak megtámadása a kritikus infrastruktúra összeomlását vagy megsemmisítését okozhatja és mindez súlyos következményekkel járhat. Éppen ezért a legkorszerűbb védelmi rendszerek és védelmi kialakítások kerülnek előtérbe egy ilyen erőmű üzemeltetésekor. A szigorú biztonsági előírások, beléptetés és zártláncú kamerarendszer üzemeltetése mellett elengedhetetlen a sugárzó anyagra vonatkozó megfelelő épület-szerkezeti kialakítások megléte. Általában a radioaktív magot 20 cm acél és 1-2 méter vastag beton borítja. Ezt az egységet újabb 5 cm vastag acél és másfél méter vastag vasbeton fedi. Ez a szerkezet kiemelkedően ellenálló tulajdonságokkal rendelkezik. A tervezéskor figyelembe véve az esetleges természeti erők behatásait is, az így kialakított vasbeton szerkezet akár egy erős hurrikánt, vagy földrengést is gond nélkül átvészel.

6. ábra. Pennsylvaniai atomerőmű forrás:
http://kitekinto.hu/amerika/2009/11/23/nuklearis_szivargas_az_atomermben/

A nukleáris létesítmények, valamint radioaktív anyagok védelmét mind technikai eszközökkel, mind emberi erőforrásokkal biztosítani kell. Ezt az 1980. évi Nukleáris Anyagok Fizikai Védelméről szóló nemzetközi egyezmény szabályozza. Ehhez Magyarország is csatlakozott, amelynek eredményeképp készült el az 1987. évi 8. törvényerejű rendelet. A terrorizmus elleni egyre nagyobb küzdelem kikényszerítette a fenti rendelet módosítását, amelyre 2005-ben került sor. Ennek tükrében 2008-ban hazánk is aláírta az egyezménymódosítást és kihirdette a 2008. évi LXII. törvénnyel.

A NAÜ által kiadott Nukleáris anyagok és nukleáris létesítmények fizikai védelméről szóló (INFCIRC/225/rev. 5., 2011.) dokumentum alappillérként foglalja össze a nukleáris anyagok kategóriákba sorolását, a használatban lévő, szállított, vagy tárolt nukleáris anyagokkal szemben támasztott védelmi követelményeket, továbbá a nukleáris létesítmények szabotázs elleni védelmének követelményeit.

Az ide vonatkozó fizikai védelmet, mint fogalmat az alábbiak szerint definiálja: „Fizikai védelem azon belső szabályozás, technikai eszköztár és élőerős elhárítás összessége, amely a nukleáris védettség részeként a nukleáris létesítményekkel, valamint nukleáris és más radioaktív anyagokkal, valamint az ionizáló sugárzást kibocsátó, de radioaktív anyagot nem tartalmazó berendezésekkel szemben elkövetendő jogtalan eltulajdonítás és szabotázs, illetve egyéb bűncselekmények megelőzésére és elrettentésére, észlelésére, késleltetésére és elhárítására irányul.” [6] Egy másik megfogalmazásban a fizikai védelem célja a nukleáris létesítmények, illetve a radioaktív és nukleáris anyagok biztonságos őrzésének, védelmének megteremtése, valamint annak megakadályozása, hogy a fent említettek a biztonságos őrzés alól kikerüljenek, azokhoz illetéktelen személyek hozzáférjenek.

Hazánkban a nukleáris létesítmények őrzésével, védelmével és a nukleáris anyagok szállításának biztosításával összefüggő feladatokat az atomtörvény és az atomenergia alkalmazásával összefüggő rendőrségi feladatokról szóló 47/1997. (VIII. 26.) BM rendelet szabályozza. [7] A fizikai védelem biztosítása a nukleáris anyagok szállításakor a rendőrség feladata. A rendőrség engedélyt ad a friss és kiégett nukleáris üzemanyag szállításához, radioaktív anyagok esetében pedig meghatározott veszélyesség elérése esetén meghatározza a szállítás útvonalát. A közvetlen őrzési, védelmi feladatokat a rendőrség fegyveres őrséggel látja el, a szállítás biztonságáról előre kidolgozott és minősített intézkedési terv szerint gondoskodik. A hatályos előírások és tapasztalatok alapján a nukleáris anyagok szállítása során a megfelelő védelmi szint biztosított. A nukleáris létesítmények, az elhasznált fűtőelemek tárolói, gyógyászati, ipari és kutatási célú sugárforrások védelme diverzió, valamint terrortámadás ellen nemzetközi ajánlások alapján, szigorú előírások és keretek között került megtervezésre és szervezésre. Az elmúlt évtizedekben tapasztalt terrorcselekmények miatt a védelem megerősítésre került, még drasztikusabb és szigorúbb lépéseket tettek a nukleáris létesítmények behatolás elleni védelme, illetőleg a nukleáris és radioaktív anyagok biztonságának növelése érdekében.

Az atomerőművekben, ha azok terrorcselekmény célpontjává válnának, nem a reaktorsérülés vagy a cikk elején leírt láncreakció bekövetkezte, hiszen annak esélye meglehetősen kevés, hanem az esetleges üzemzavar kapcsán kialakult energiaszolgáltatás kiesése – különösen, ha egyszerre több erőmű ellen irányulna a csapás – okozna ellátási zavarokat.

Elfogadott tény, hogy Magyarország jelenleg nem tartozik a nemzetközi terrorszervezetek ellenségképébe, így az ország terrorfenyegetettségét a környező országok, az Európai Unió, valamint a NATO ilyen irányú veszélyeztetettsége határozza meg.

Nukleáris terrorelhárító intézkedések terén az alábbi három kiemelkedő szervezet az élenjáró:

- Nemzetközi Atomenergia Ügynökség (NAÜ), mint az ENSZ atomenergia békés felhasználására szakosodott szervezete
- Amerikai Egyesült Államok Nukleáris Szabályozó Hatósága (Nuclear Regulatory Comission, rövidítése: NRC)
- OECD-NEA a legfejlettebb országok nukleáris szakértőit tömörítő testület.

A fentiek tükrében azonban joggal tehetnénk fel a kérdést, hogy Magyarország képes lenne atombomba előállítására?

Egy nemzetközi nukleáris fegyverekre vonatkozó felmérés álláspontja alapján Magyarország minden olyan szükséges eszközt és technikát birtokol, amely nukleáris fegyverek előállításához szükséges, legalább is korlátozottan, de a lehetőség rendelkezésre áll. A magyar szakemberek szerint azonban ezt több korlátozó tényező is cáfolni igyekszik. Elsősorban a probléma már az alapanyag és az előállítási folyamat realizálásánál jelentkezik. A szükséges hasadóanyag előállítása is már rendkívül körülményes, beszerezni szinte lehetetlen. Ahogyan arra a fentiekben is kitértem, nukleáris fegyver előállításához elengedhetetlen a magasan dúsított urán, amelynek előállításához (centrifugák létesítéséhez) Magyarország nem rendelkezik technikai háttérrel, valamint azok működtetéséhez szükséges megfelelő mennyiségű energiával, továbbá a hasadóanyag kereskedelmét nemzetközi egyezmények és szervezetek tiltják. Hiányosságok között említhető még, hogy a magyar atomfizikusok kizárólag polgári célú, békés nukleáris energiában rendelkeznek tapasztalattal. [8] Az 1970-ben életbe lépett – nukleáris fegyverek elterjedésének megakadályozásáról szóló – Atomsorompó szerződés (Non-Proliferation Threaty) biztosítja, hogy a nukleáris fegyverrel rendelkező államok senkinek nem adnak át nukleáris fegyvert, az azzal nem rendelkezők, pedig vállalják, hogy nem állítanak elő efféle fegyvereket. Magyarország ezt az egyezményt 1972-ben kötötte meg (1972. évi 9. tvr.).

Ennek megfelelően hazánk biztosítékokat vállalt annak igazolására, hogy a területén folytatott nukleáris tevékenység során a nukleáris anyagokat nem használják fel nukleáris fegyverek vagy más nukleáris robbanó szerkezetek előállításának céljára. Az atomtörvény az atomenergia biztonságos alkalmazásának irányítását és felügyeletét az Országos Atomenergia Bizottság (OAB) és az OAH kezében összpontosítja. Az OAH hatáskörébe tartoznak többek között a nukleáris létesítmények biztonságával kapcsolatos és a nukleáris fegyverek elterjedésének megakadályozásával összefüggő feladatok. Az atomtörvény az Atomenergia Hivatal részére jogosultságot biztosít bármely atomenergiát alkalmazónál ellenőrzést folytatni. A nukleáris biztonság érdekében ellenőrizheti a jogszabályokban, szabályzatokban előírt rendelkezések betartását, az általa elrendelt intézkedések végrehajtását és a nukleáris létesítmények minőségbiztosítási rendszereit. [9]

A fent említett tények alapján megállapítható, hogy Magyarországon a nukleáris létesítmények ellen irányuló terrortámadás esélye igen csekély, mindezek ellenére a védelem jogi-, intézményi- és műszaki elvárásai nemzetközi szinten is magas színvonalúnak számítanak. Ennek megnyilvánulása abban mutatkozik meg, hogy egy esetleges terrortámadás esetében mind az üzemeltetők, mind a hatóságok képesek a kihívásnak megfelelő védelmi reagálásra, az eszkalálódás megakadályozására, illetve a következmények mérséklésére.

ÖSSZEGZÉS

Az előzőekből láthatjuk, hogy egy atomfegyver előállítása még a nagyobb országok számára is körülményes folyamat, amely igen kifinomult szaktudást, mérhetetlen energiát és időt emészt fel. A mai korszerű technológia igyekszik kizárni annak lehetőségét, hogy valamely államtitokban atombomba-kísérleteket hajtson végre és igyekszik az ahhoz szükséges alapanyagok beszerzését a legszigorúbb felügyelet alá vonni. A címben szereplő hiedelmet – amely szerint egy atomerőmű bevethető és alkalmazható tömegpusztító fegyverként (illetve atomfegyver előállításának eszközeként) – szinte kizártnak tarthatjuk. Ehhez mind a technikai megoldások, mind pedig a fizikai korlátok (a kémiai és fizikai láncreakció beindulása) akadályt jelentenek. Biztonsági szempontból vizsgálva, veszélyforrásnak sokkal inkább tekinthető az erőműből egy esetleges radioaktív sugárzás légtérbe való jutása (*lsd. 1986-Csernobil; 2011-Fukushima*), amely azonban egy atomerőmű működése során a legszigorúbb védelmi megoldások alkalmazásával és betartásával, még meghibásodás esetén sem fordulhat elő. Elfogadva annak tényét, hogy a távol-keleti országok atomkísérletei titokban zajlanak, kijelenthetjük, hogy az elengedhetetlen villamos energiát biztosító atomerőművek továbbra is az emberek javát szolgálják és a legkevésbé sem a tudomány, a fizika és a kémia pusztító célzatú felhasználását.

A kérdés még továbbra is az, hogy egy atomreaktor átalakulhat-e atombombává?!

A választ az energia előállítás központi szerepét jelentő láncreakció adja meg. A korábban már taglalt láncreakció az atombomba esetében annyit jelent, hogy egyetlen maghasadás több millió másik atom robbanását vonja maga után. Egy atomerőmű reaktorában a maghasadások száma ezzel szemben – szabályozott eljárás mellett – állandó. Ebben az „önfenntartó láncreakcióban" egy neutron szabadul fel maghasadásonként és okoz egy másik hasadást. Megerősítésként szolgáló tény az energia előállításhoz használt urán tisztasága is, amely szerint a reaktor működéséhez kevesebb, mint 3%-os urándúsítás szükséges, szemben az atombomba 90%-os dúsításával. A fentiek tükrében kijelenthető, hogy az atomerőmű nem robbantható fel atombombaként.

A nukleáris tevékenység szabályzását tekintve megállapítható továbbá, hogy az erre vonatkozó szabályzókban a biztonság minden más szemponttal szemben elsőbbséget élvez. Az elsődleges cél az, hogy a lakosság, a környezet ne szenvedjen károsodást a nukleáris létesítménytől eredő hatások miatt. Ezen cél érdekében az előírt biztonsági elveket és kritériumokat maradéktalanul be kell tartani. Egy atomerőmű célponttá válásával kapcsolatban megállapítható, hogy egy terrortámadásnál kitüntetett szerepe lehet egy ilyen létesítménynek. Minden biztonsági előírás, létesítményvédelmi szabályzó ezt hivatott megakadályozni.

Felhasznált irodalom

[1] Fizikai Szemle 1996/11. 369.o.: A radioaktivitás felfedezése (Pierre Radványi)

[2] Radiológiai tájékoztató - Magyar Polgári Védelmi Szövetség www.mpvsz.hu/kpanyag/download.php?id=38 (2013. 03. 05)

[3] 1996. évi CXVI. törvény az atomenergiáról

[4] Dr. Ormai Péter: Radioaktív hulladékok csomagolása és szállítása. Paksum Nyomda Szekszárd, 2009.

[5] Répási Krisztián: A hasadóanyagok csempészetének problémájáról. Védelempolitika, 2008. 07. 15

[6] Országos Atomenergia Hivatal – Fizikai védelem http://www.haea.gov.hu/web/v2/portal.nsf/feladatok_hu/6F709EFC60F8FB37C12579DD00406619?OpenDocument (2013. 03. 06)

[7] Solymosi József, Rónaky József, Lévai Zoltán, Vincze Árpád: A nukleáris létesítmények terrorfenyegetettsége

[8] Ferenczi András: Füvet kellene enni a magyar atombombához, 2013. 02. 13. http://www.origo.hu/itthon/20130213-lehete-magyar-atombomba.html (2013. 03. 06)

[9] Országos Atomenergia Hivatal feladatai http://www.haea.gov.hu/web/v2/portal.nsf/feladatok_hu (2013. 03.08)

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Teknős László
teknos.laszlo@gmail.com

A SANDY HURRIKÁN EGYESÜLT ÁLLAMOKAT SÚJTÓ HATÁSAINAK ELEMZÉSE[1]

Absztrakt

Az amerikai nép több megrendítő természeti eseményt kénytelen átélni. Ha csak a 2005-ös Katrína hurrikánra gondol az ember, be kell látnia, hogy a természet szépsége mellett erejének pusztító hatásával is számolni kell. A kérdés az, hogy a szörnyű katasztrófák ellen, hogyan védekezhet az ember, illetve a lakosságnak mennyi esélye van a megfelelő védelemre? A tanulmány próbál választ adni, hogy a Sandy hurrikán érkezése előtt az amerikai polgárok milyen lépéseket tettek, azok megfelelőek voltak-e, illetve milyen új lehetőséget alkalmaztak a saját védelmük érdekében. Továbbá a Sandy hurrikán a kritikus (létfontosságú) infrastruktúrákat pusztító, megsemmisítő romboló munkája milyen módon akadályozta és veszélyeztette a lakosság biztonságát.

The American people are forced to face shocking natural events. If you think about the 2005 Hurricane Katrina, you have to admit that in addition to its beauty the nature has destructive power effect. The question is how poeple can protect themselves from the terrible disasters, and additionaly if the population has the chance to set up an adequate protection? The study attempts to answer if before the arrival of Hurricane Sandy the action taken by the Americans were adequate, and what could be learned as a new way to protect population. In addition it attenmps to study how Sandy Hurricane had a devastative effect on critical infrastructure, in which manner the destructive effect were obstructing or endanger public safety.

Kulcsszavak: *Sandy hurrikán, kritikus infrastruktúra, árvíz, extrém csapadék, erős szél, NOAA ~ hurricane Sandy, critical infrastructure, flood, extreme moisture, strong wind, NOAA*

1 A cikk a Kritikus Infrastruktúra Védelmi Kutatások TÁMOP-4.2.1.B-11/2/KMR/001 „Civil-katonai partnerség” alprogram „Közlekedési kritikus infrastruktúra védelem” kiemelt kutatási terület támogatásával készült el.

BEVEZETÉS

Az amerikai lakosság valamennyi tagjának a hurrikán szezon maga a pokol. A júniustól novemberig tartó viharos, hurrikános időszak gazdasági, biztonsági kihívások egész sorát zúdítja a társadalomra. Az utóbbi évtizedekben számos olyan katasztrófa söpört végig – többek közt – Amerika keleti partjain, amit az amerikai lakos még eddig nem tapasztalt. Az amerikai védelmi erők sorra olyan esemény sorozatokkal találkoznak, amik a felkészültségüket, együttműködésüket, addigi szakmai tapasztalataikat nagymértékben új szintre emeli. A katasztrófák elleni védekezés kulcsszereplője a FEMA (Federal Emergency Management Agency). A 2005-ös Katrína hurrikán (mint, az eddigi legpusztítóbb hurrikán) bizonyította be, hogy a jól felkészült védelmi erők több ponton gyengeséget mutattak. Az akkori tapasztalatokat beépítették a megelőzési, kárelhárítási, helyreállítási feladatcsoportokba, amiket jól alkalmaztak minden évben. 2012-ben a Sandy hurrikán is hatalmas pusztításokat végzett, komplex megnyilvánulásai időben és térben egymás mellett, többször egymást erősítve jelentek meg. A vihar okozta károk, és a pusztítást lereagálni képes védelmi lehetőségek, a nélkülözhetetlen katonai-rendvédelmi-civil kooperációk a magyar hivatásos katasztrófavédelemnek hasznos információkat tud biztosítani.

A hurrikán egyik „új” szerzeménye, hogy a leterhelt segélykérő vonalak miatt a közösségi médián belül a twitteren keresztül történtek meg a segély kérések, több családot, emberi életet mentve ezáltal.

CIKLONOKRÓL ÁLTALÁBAN

A ciklon egy légörvény, ami nagy sebességgel áramol. Mivel középpontjában a légnyomás a legalacsonyabb, ezért a levegő befelé áramlik. Az északi féltekén enyhén befelé mutató mozgással forog az óramutató járásával ellentétes irányban. A ciklonok kisérője a csapadékos időjárás, ami a belsejében létrejövő felhő - és csapadékgerjesztő feláramlások miatt következik be. [1] A másik kísérő elem, ami a pusztítást végzi a szél, aminek ereje az áramlási sebességtől függ, ami a légnyomási gradienshez[2] köthető. Tehát a nagyobb légnyomási gradiens nagyobb áramlási sebességet von maga után, ezáltal a szél ereje is nagyobb lesz. A ciklonok fajtái alapján a következőkre lehet felosztani: trópusi (tájfun – Ázsia; hurrikán - Amerika) és mersekelt övi ciklon. A hurrikán[3] nagy kiterjedésű (több száz kilométer) felhőörvény. Mozgása az északi féltekén az óramutató járásával ellentétes a délin azzal megegyezik. Keletkezéséhez min. 26 °C-os vízi hőmérséklet és nedves trópusi levegő kell.

Kialakulásukban és fejlődésükben fontos szerepet játszik a meleg tenger, a látens hőfelszabadulás, a konvekció, a tengerszinti légnyomásesés, a szélsebesség növekedés, és az erős konvergencia. [2]

Általában május elejétől (hivatalosan június 1-től) november végéig tartó időszakban (ún. hurrikán szezon) fordulhatnak elő az 10. és a 20. szélességi kör között. [3] A meleg óceán felett a levegő felemelkedik - északi féltekén az óramutató járásával ellentétesen – spirális forgásba kezd, majd kialakul a trópusi vihar (19-34 m/s-os sebesség). 18m/s alatti sebességnél trópusi depresszióról beszélhetünk. 35 m/s sebesség fölött hurrikánról van szó. [2] A hurrikánnak van szeme, ami a középpontban található, ahol a legkisebb a légnyomás. A szem körül van a viharzóna (felhőfal), melyből intenzív csapadék hullik ki. [1]

---

[2] Az a vektor, amely nagysága a nyomáskülönbséggel arányos, iránya a legerősebb nyomásváltozás irányába mutat. Ez az irány a nyomási felülethez húzott normális irány.
Forrás: http://www.pumaszallas.hu/elmeleti-anyagok/meteorologia.html

[3] A hurrikán elnevezés a huracan szóból ered. Jelentése esőcsepp és a Közép-Amerikai maják használták. A maja civilizációban a vihar istene volt. Az aztékoknál hasonló isten neve: Tlaloc

AMI AZ ELŐREJELEZHETŐSÉGET ILLETI…

A 2012-es atlanti hurrikán szezon június 1-től (hivatalosan) november 30-ig tartott. A legtöbb hurrikán és trópusi vihar megjelenés augusztus közepe és október vége között zajlott le (csúcsidőszak).

A National Oceanic and Atmospheric Administration's Climate Prediction Center (NOAA CPC) 2012. augusztus 9-i előrejelzése szerint 70 % az esélye, hogy 2012-ben 12-17 nevezett vihar lesz, 39 mph vagy attól erősebb széllel, 5-8 hurrikán várható, amiből 2-3 darab (111 mph vagy attól erősebb széllel) 3-5 kategóriás nagy hurrikán lesz. [4]

A hurrikánok keletkezésének (lassú folyamata miatt) előrejelezhetősége nagyobb valószínűséggel bír, mint a pályájának (útvonalának) meghatározása.

Középtávú Előrejelzések Európai Központja [ECMWF[4] - Reading város (Anglia székhelyű)] több mint 8 nappal jelezte előre a ciklon amerikai kontinens elérését, illetve a rendkívüli pályamódosítások ellenére az irányvonalat is. Az ECMWF IFS (Integrált előrejelző rendszer) nagyban segítette előrejelzéseivel (pálya, intenzitás, várható hatások) az amerikai meteorológiai számításokat. A nagy felbontású előrejelzések (HRES) elég pontosnak bizonyultak. Október 23-án 12 UTC-s[5] (7 nappal a partot érés előtt) 52 futtatás közül 47 azt adta, hogy a Sandy eléri az északkeleti partvidéket. A széllökések előrejelzése is pontos volt, a New Jersey partvidékére mivel 75-85 mph (120- 136 km/h) volt előrejelezve. Főként 70-80 mph-t (112-129 km/h) mértek 55-96 mph-s (89- 155 km/h) határokon belül.

A GFS (globális időjárás-előrejelző modell) azonban később (a hurrikán érkezése előtt 5 nappal) tudta előrejelezni mindazt, amit az ECMWF modellek. Az európai modell a fejlettebb számítógépes infrastruktúrája, a finomabb rácsfelbontások alkalmazása miatt sokkal pontosabbak voltak, mint az amerikai modellek. Bár a Karib-tengeri gyors kimélyülést egyik modell sem tudta pontosan előre jelezni, így Kubára, Jamaikára nem lehetett jó előrejelzést készíteni. A hurrikánná alakulás után lehetett az előrejelzéseket pontosabban (meghatározni) megadni a nyomásváltozásokra, szélsebességekre, csapadékokra vonatkozóan.

A 2012-es szezonban a NOAA előrejelzési modelljeihez felhasználta a Suomi-NPP műhold adatait is, ugyanis az pontosabb méréseket végez a légkörben, s ezáltal jobban megjósolható a vihar nagysága és mozgási útvonala. [5]

2012. május 3-án a Floridai Állami Egyetem óceáni-atmoszférikus előrejelző központja (FSU COAPS) szerint 13 nevezett viharral, 7 hurrikánnal kialakulása várható. Az Egyesült Királyság Országos Meteorológiai Szolgálata (Met Office) is kiadott egy előrejelzést 2012. május 24-én. E szerint 10 nevezett viharral kell számolni. A hurrikánok és a nagyobb hurrikánok számát azonban nem határozta meg.

A Tropical Storm Risk (TSR) előrejelzéseket készít és térképeken ábrázolja a trópusi vihar előfordulásokat, tevékenységeket szerte a világon. 2011. december 7-én kiadott jelentése szerint átlag feletti hurrikán szezon várható. A trópusi ciklonok az 1950-2010 átlaghoz viszonyítva kb. 49%-kal lehet magasabb aktivitásuk. 14,1 (± 4,2) trópusi viharral, 6,7 (± 3,0) hurrikánnal, és 3,3 (± 1,6) nagyobb hurrikánnal lehet számolni az atlanti hurrikán szezont.

2012. május 25-i előrejelzés szerint 12.7 (+/-3.9) nevezett vihar és 5.7 (+/-2.7) hurrikán várható. 2012. június 6-án egy újabb előrejelzést adott ki, ami szerint 14 nevezett vihar, hat hurrikán, és három nagyobb hurrikán alakul ki a 2012-es atlanti hurrikán szezonban. [6]

Philip J. Klotzbach, William M. Gray csapata (Colorado State University) szerint 1981-től 2010-ig tartó szezon alapján átlagosan egy szezonban 12,1 trópusi viharral, 6,4 hurrikánnal,

[4] Az Országos Meteorológiai Szolgálat középtávú előrejelzései (2-10 nap) döntően az ECMWF prognózisokra épülnek. Magyarország teljes jogú tagfelvételi kérelmének benyújtását a 1492/2011. (XII. 27.) Korm. Határozat tette lehetővé. Forrás: http://www.met.hu/ismeret-tar/meteorologiai_hirek/index.php?id=430&hir=Sandy_hurrikan_elorejelezhetosege

[5] Koordinált világidő. A Föld időzónáit ehhez viszonyítják

2,7 nagyobb hurrikánnal kellett számolni. [7] 2012. június 1-én kiadtak egy szezon előrejelzést, miszerint a 2012-es szezonban 13 nevű vihar, öt hurrikán, és (amelyből) kettő nagy hurrikán várható.

2012-es év atlanti hurrikán szezonjában[6] 19 elnevezett trópusi viharral (Alberto, Beryl, Debby, Florence, Helene, Joyce, Oscar, Patty, Tony, Chris, Ernesto, Gordon, Isaac, Kirk, Leslie, Michael, Nadine, Rafael, *Sandy*) zárult az atlanti hurrikán szezon (amik közül a felsorolásban az utóbbi 10 hurrikán volt). [8]Ez rendkívüli mennyiség.

SANDY HURRIKÁN METEOROLÓGIAI TÖRTÉNETE

Az Atlanti-óceánon az atmoszférában egy apró légörvény alakul ki, Afrika észak-nyugati partjainál 2012. október 19-én. A 18-as számú trópusi depresszió[7] nevet kapta meg. A következő napokban nyugat felé haladt, ahol az alacsony légnyomású terület (kedvező feltétel) miatt tovább erősödött. Közben az amerikai Nemzeti Hurrikán Központ (NHC) kiértékelte a trópusi képződményt és nagy valószínűséggel állította, hogy a kedvező feltételek miatt trópusi ciklonná fog fejlődni. [9] Mivel az uralkodó szélsebesség meghaladta a 64 km/h-t (40 mph-t), ezért október 22-én trópusi viharrá nyilvánították. [10] Sandy a 2012-es atlanti hurrikán szezonban a 18. viharként (később a tizedik hurrikánként) regisztrálták. Október 23-án északra fordult a pályája a Nagy-Antillák[8] (Karib-térség) felé és az ereje tovább nőtt. Október 24-én várható módon elérte Jamaicát. Az amerikai Nemzeti Hurrikánközpont a Sandy-t átminősítette egyes fokozatú hurrikánná.[9] Kingston (Jamaica) déli részén már 105 km/h-s szeleket is mértek, ami 130 km/h-ra erősödött a nap folyamán. Október huszonötödike hajnalán mozgása felgyorsult és elérte a kubai partokat. Ekkor a Saffir-Simpson szél skála szerinti 175 km/h-s (110 mph) szelei miatt kettes fokozatú hurrikánná erősödött. [11] A szem már 37 km-es átmérőjű. Kuba keleti részén áthaladva 26-án továbbhaladt a Bahamákhoz, de intenzitás gyengülés miatt visszafokozták egyes fokozatú hurrikánra. Észak-nyugatra fordult, de szerencsére elkerülte Floridát.[10] A Golf-áramlat[11] (a 27 ^{0}C-os vízhőmérséklet kedvező) mentén észak-Amerika keleti partja mellett halad tovább. Október 28-án a vihar magja New Yorktól 930 km-re délre volt. Másnap hajnalban, ahogy azt a modell-előrejelzések is mutatták északnyugat felé fordult, és elindult a partok felé. Délután 14:00 órakor a vihar középpontja kb. 285 kilométer távolságra közelítette meg New Yorkot és este 20:00-kor Atlantic Citytől (New Jersey állam, Atlantic megye) 10 kilométerre lépett be a szárazföldre (ért partot). [11] Sandy mielőtt elérte New Jerseyt (Egyesült Államok legsűrűbben lakott állama) post-trópusi viharrá (mivel nem az óceán feletti meleg levegőből táplálkozik, úgynevezett téli ciklonná vált) minősítette át az amerikai Nemzeti Hurrikánközpont. Október 29-én este mérsékelt övi viharciklonná alakult át, de a magával hozott trópusi levegő hatására rengeteg csapadékkal vonult tovább. Virginia Beach-en (legnépesebb Virginia állambeli tengerparti város) a csapadék mennyisége a 235 mm-t is elérte. A keleti parton 120-140 km/h-s széllökéseket mértek. Kanada felöl hideg levegő keveredett Sandyval, így Appalache-hegység 600 m-nél

[6] A 2012-es hurrikán szezonja hivatalosan június 1-én kezdődött. De két trópusi vihar, név szerint Alberto (május 19.) és Beryl (május 26.) már az előző hónapban jelentkeztek. A szezon november 30-ig tartott.

[7] A trópusi képződmények a bennük uralkodó szélsebesség alapján lehet trópusi depresszió, trópusi vihar, trópusi ciklon

[8] Kuba, Dominikai Köztársaság, Haiti, Jamaika, Puerto Rico (USA), a Kajmán-szigetek (Egyesült Királyság), Navassa-sziget (USA), valamint Turks és Caicos (Egyesült Királyság) szigetekből áll.

[9] Hurrikán vadászok 99 mph-s (159 km/hI szélerősséget mutattak ki.

[10] Földrajzi helyzete miatt (alacsonyan fekvő viszonylag egyenletes síkság) komoly károkat szenvedhetett volna, mint Dennis, Katrina, vagy a Rita hurrikánok alatt)

[11] Szél által hajtott tengeráramlat, ami a Mexikói-öböltől indul, onnan meleg vizet szállít a Floridai-szorosnál mellett az Amerikai Egyesült Államok keleti partjai mentén Észak-Atlanti-óceánon keresztül Észak-Európába és fűti a kontinenst

magasabb nyugati részein az esőt havazás (60-92 cm-es) váltotta fel. [9] Főbb érintett területei West Virginia, Tennessee, és Maryland.

SANDY HURRIKÁN PUSZTÍTÓ HATÁSÁNAK BEMUTATÁSA[12]

A Sandy az amerikai történelem második legkegyetlenebb hurrikánja, de kiterjedésében a legnagyobb (átmérője csaknem 1600 km). A pusztítást vizsgálva csak a 2005-ös Katrína hurrikán előzi meg. A Sandy hurrikán hatásait tekintve hasonló volt az 1938-as New England-i hurrikán. Rengeteg eső, hatalmas erejű szelek, gyorsan terjedő tüzek, árvizek okoztak tetemes mértékű károkat mind a lakosság, mind az anyagi javak körében.

A Sandy pusztító hatását – annak összetettsége miatt – minimum két csoportra lehet osztani.

Elsődleges hatások, amiből számos egyéb hatás következtethető le, vagyis a Sandy hurrikán közvetlen hatásai:

1. Rendkívüli szélsebesség, erős széllökések pusztító hatásai (89- 155 km/h)
2. Extrém mértékű felhőszakadás, csapadékhullás (átlagosan 120-150 mm csapadék, Virginia Beachen 235 mm!); havazás (pl: West-Virginiában három méteres hó volt)
3. Vihardagály hatalmas hullámokkal (teliholdkor érkezett a hurrikán, mikor legmagasabb a dagály)

Másodlagos hatások, amik az elsődleges hatásokból alakulhatnak ki:

1. Közüzemek sérülései – zavarok a szolgáltatásban, lakossági ellátásban (Pl. A New York áramellátását biztosító Consolidated Edison egyik manhattani alállomásán robbanás történt)
2. Az áramszolgáltatás kiesése miatt kórházakban nehézségek lépnek, így a kitelepítés újabb kihívásokat állít a védekező erők számára. A kiesett kórház a kimentett sérültek ellátására nem alkalmas, ezáltal másik kórházi intézményre hárul az ellátás
3. Lakóingatlanok romosodásai – szükségszállások kialakítása – logisztikai kihívások a lakosság ellátása miatt
4. Tűzesetek – rendkívüli szélerősség miatt a leszakadó villanyvezetékek okozta tüzek oltása komplikált és nehéz
5. Az elárasztás miatt a védekezési munkálatok néhány helyen (Queens-i tűzesetek) a tűzoltási, védekezési munkálatok hatékonysága akadályozva van
6. Az elárasztások miatt közlekedési gondok. Több napig az 5 milliós ingázó utazási feltételeit nem tudják biztosítani, a munkahelyek állása miatt gazdasági károk lépnek fel (csak kevés munkáltató tudja a távmunkát biztosítani)
7. Az elárasztás miatt fontosabb, az ellátást biztosító rendszerek mennek tönkre pl.: ivóvízbázis stb.
8. Az elöntés miatt a pincékből kimossa a vegyi és egyéb környezetre ártalmas anyagokat – környezeti károk helyi szinten
9. A lakóingatlanokból közterületre kihordott veszélyes hulladékok (az épület megtisztítása címszó alatt) további rizikót képeznek
10. A rendkívüli csapadék (mint a hurrikán jöttének előzménye) feláztatja a talajt, amit az erős széllökések könnyen kidöntenek, rá a villamos vezetékekre, ami áramkimaradást okoz, vagy közvetlen életveszélyt az emberre nézve. Továbbá a későbbi kárfelmérésnél okozhat kihívást az egy időben jelentkező lakossági kártérítési igények kielégítése

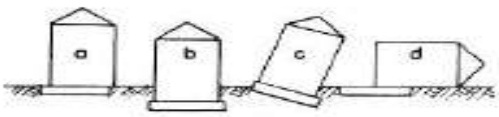
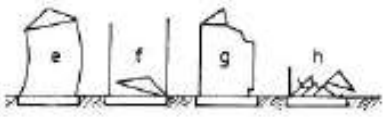
[12] Sandy hurrikán hatásainál nem cél (helykorlátok) elemezni minden érintett városnak, (kár)területnek a Sandy hurrikán által elszenvedett károkat, de a hatások mértéke és milyenségének komplexitása miatt a kialakult kárterületek összefoglaló módon az olvasó számára érthetően bemutatásra kerülnek

A hatalmas széllökések számos amerikai városban vastag törzsű fákat csavartak ki. Maga a szél ereje „csak” közepes méretű fákat tépett ki a földből, de a hirtelen lezúduló csapadék (vihar egyik velejárója) miatt - amit a csatornarendszer már nem tudott befogadni - ez könnyen megvalósulhatott. A kertek és közparkok területén a túlázott szivacsos, laza talajba a gyökerek már nem bírtak kapaszkodni így egyszerűen eldőltek. A kidőlő fák egyrészt károkat okoztak a villamos vezetékekben, áramkimaradásokat okozva, illetve a gépjárművek súlyosan megrongálódtak. Az úttesten, járdán pedig akadályt képezve okozott nehézséget a mentési munkálatoknak. Az amerikai lakosság nagy pechje, hogy a tomboló szélvihar „csak” egyetlen hatás volt, ami kihívásokat eredményezett. A vihar leforgása alatt azonban több természeti tényező együttesen lépett fel (kombinált hatás – időben és térben együttesen jelentkezik), ami több kárterületet hozott létre, illetve az egyes kárterületeken (az a terület, ahol a pusztító, romboló hatás(ok) legjobban bekövetkeznek) nagyobb pusztítást eredményezett és a megfelelő védekezési munkálatokhoz nagyobb beavatkozó / mentő egységek szükségesek kombinált koordinációval.

1. ábra. Vezetékek leszakadása Hopewell Township egyik útján (New Jersey) [12]

A szélvihar további hatása volt, hogy épületek és egyéb műtárgyak részeit szakította le.

Voltak olyan lakások ahol több ablakot is betört a szél és sérüléseket okozott. A vihar előtt – többek között - New York utcáin több üzletnek bedeszkázták kívülről a nyílászáróit, ami egy egyszerű megoldása az épület gyenge pontjainak ideiglenes és elégséges szintű megerősítéséhez. Amennyiben a megelőző intézkedések közül ez a módszer nem valósul meg, fennáll a veszélye, hogy tetemesebb anyagi kár éri a tulajdonosát / használóját, illetve a bennrekedteknek személyi sérülései nagyobbak lehetnek a könnyebb tárgyak elmozdulása miatt.

Épületek helyzeti sérülésének fajtái, megváltozása az alaphoz viszonyítva	Az egyes épületszerkezetek vagy azok elemeinek sérülése
	
a) Elmozdulás b) Süllyedés c) Megdőlés d) Borulás	a) Deformáció b) Leomlás c) Sérülés d) Összeomlás

1. táblázat. Az épületek sérüléseinek formái [13]

A Sandy hurrikán pusztító hatását jellemzi, hogy az érintett kárterületeken levő épületeket, lakóingatlanokat a táblázat által bemutatott sérülések közül mindegyik sérülés típus érintette.

2. ábra. A szél pusztító erejének különböző megnyilvánulásai épületek esetében [14]

Az érintett városok, települések számos lakóépületeiben, több esetben az oldalsó támfalak, homlokzati falak is leomlottak. A fenti ábrán látható, hogy az egyes lakóingatlanok milyen súlyos károkat szenvedtek. Ezeket az embereket (családokat) jobb esetben rokonok fogadják be, vagy szükséglakhelyeken (befogadó pontokon) szállásolták el.

A közlekedés, mint kritikus infrastruktúra is sérült az erős szélvihar miatt. Elsősorban a közlekedési lámpák, amik teljesen tönkrementek. Természetesen a meteorológiai előrejelzések alapján az érintett városrészeket kiürítették, a tömegközlekedést a vihar előtti napokban (este 19:00 órakor) leállították, a metró állomásokat, utakat, alagutakat, hidakat lezárták a nyilvánosság elől. Az utóbbit a beavatkozó-mentő erők használhatták vészhelyzetben. A lezárás lakosságot óvó megelőző intézkedés, mert a hurrikánnal járó vihar nagyobb területet fog le, ezért nagyobb kárterülettel kell számolni, nagyobb lakosság számot érintve, és a feltorlódások, bennrekedések miatt (lásd pánikszerű menekülés) jobb az emberektől lezárva hagyni.

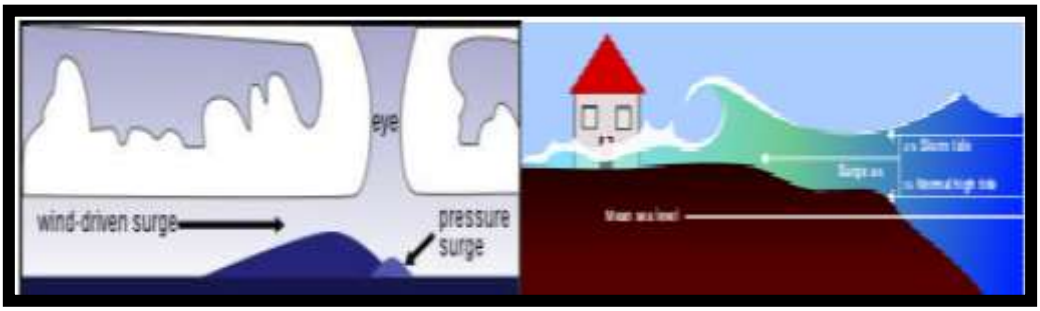
3. ábra. Balról: Fakidőlés autóra Hobokenben (New Jersey) távvezetékre Cranfordban (New Jersey), házra Garden Cityben (New York) [15]

A vihar ereje és a velejáró csapadékhullás rendkívüli volt (de, egyéb trópusi ciklonokhoz képest elhanyagolható). Ilyen intenzitás megnyilvánuláskor általában épületek, közművek, kritikus infrastruktúrák (közlekedési, maga az épület, áramszolgáltatási, vízbázis stb.) környezeti károk (olajkimosdások, pincékből háztartási hulladékok, csatornarendszerekből fekália kerülhet ki) keletkeznek, ami átmeneti zavart okoz. A kárterület méretétől, a sérült elemek fajtáitól, kialakult helyzet bonyolultságától, helyreállítási munkálatok végrehajtóin illetve a rendelkezésre bocsátható gazdasági erőforrásokon múlik, hogy az eredeti (vagy ahhoz közeli) állapot mikor állítható vissza.

Kanada (az Amerikai Egyesült Államokkal határos, az észak-amerikai kontinens részen fekvő terület) felöl hideg levegő keveredett Sandyval, így az Appalache-hegység (hegységrendszer Észak-Amerikában) 600 m-nél magasabb nyugati részein az esőt havazás váltotta fel. Főbb érintett területei West Virginia, Tennessee, és Maryland volt.

4. ábra. Belingtonban (nyugat- Virginia) a 33-as országúton elakadt egy mentőautó a hirtelen leesett, nagy mennyiségű hóban [16]

A vihar jelentősen megnyomta az Atlanti-óceánt, és méterekkel felduzzasztotta a part menti vizeket, valamint a városokat átszelő folyókat is. Az áradás miatt a New Yorkot átszelő Hudson folyó több mint 5 métert emelkedett, és elöntötte New York alacsonyabban fekvő részeit. New York-i Harbornál rekord magasságot ért el a vízszint, amikor a bólya szerint 32,5 láb (9,9 m) hullámok tomboltak október 30-án, ami 7,5 lábbal (2,3 m-rel) magasabb, mint a 2011-es Irene hurrikán idején [25 láb (7,6 m)]. [17]



5. ábra. Vihardagály keletkezése [18]

A ciklon belsejében van az alacsony légnyomás, ami miatt a tenger szintje megemelkedik. Minél kisebb a légnyomás annál nagyobb hullámokat gerjeszt (1 hPa nyomáscsökkenés kb. 1 cm-rel emeli a vízszintet). A spirálisan befelé áramló levegő a tengervízet maga előőt tolja, így egy vízkupola alakul ki, ami akár 2-6 méterrel is megnövelheti a tenger vízszintjét. A veszélyben levő alacsonyabb tengerpartoknál még 8-10-méteres hullámokkal is lehet számolni. [18] Ezért mosta el a partmenti homok védősáncokat a betörő óceán, mert a védvonalak alacsonyabbak voltak a hullámoknál, illetve a magasabb hullámok hatalmas ütőerővel nyomultak a védvonalaknak, így azokat könnyedén el tudta mosni, zavartalanul haladva a házak, lakóingatlanok felé. Az amerikai építkezési szokások korántsem fenntarthatóak, mivel nem célszerű olyan területre építkezni, amit a természet ereje sokszor nagy erőkkel érinteni tud.

A másodlagos hatások, amik az elsődleges hatásokból levezethetőek. Az egyik hatás a másikat felerősítheti, ezért a kárterületen keletkező romboló hatások térben és időben párhuzamosan vagy egymásra épülve alakulnak ki, mennek végbe. Másodlagos hatás például a rendkívüli erős széllökések hatására az infrastruktúrák zavarai, úgymint az áram szállításában részt vevő felső vezetékek sérüléséből származó átmeneti működés kiesések. Ezek részleges vagy teljes megrongálódása miatt leállások lép(het)nek fel, ami a védekezést nagymértékben hátráltatja (áramkimaradáskor sötétben történő tűzoltás, műszaki mentés). New Yorkban korom sötét uralkodódott a beavatkozást igénylő kárhelyeken. A háztartások áram nélkül maradása a pánikot, és az idő múlásával a bizonytalanságot növeli, ami újabb sebezhetőséget vonhat maga után, mivel az elhamarkodott menekülés a beavatkozó erők által

végzett mentési munkálatokat nehezíti meg. Az áram számos létfontosságú berendezést működtet, mint például az intenzív osztályokon levő készülékek, amik az emberi élet szempontjából nélkülönözhetetlenek. Egy New Yorki kórházban az áramellátás megszűnése után a tartalék generátorok sem tudták a megfelelő energiaigényt biztosítani, így a betegeket evakuálni kellett.

A helyzet a korai felismerést követően kritikus lehet, ha pánikol avagy túlizgulja (túlpörgeti) magát a mentendő személy (de ide lehet sorolni magát a beavatkozót is). Ha egy időben több probléma is fennáll, mint például nincs áram, az utcán víz zúdul és közben a széllökések a menekülésre igénybe vett szilárd burkolatú utat kidöntött fákkal, leszaggatott faágakkal elzárja, akadályt képez, akkor a hirtelen jött új kihívásokra - a túlélés érdekében - hatékony reagálás szükséges, amihez a hatóságok által koordinált állampolgári együttműködés és segítségnyújtás rendkívül hasznos védelmi potenciál lehet.

A rendkívüli esőzés vagy a betörő óceán, illetve megáradt folyók is komoly kihívást jelentenek. A meteorológiai előrejelzések már egyre pontosabbak, és előre meg tudják mondani a sebezhető területeket. A pusztító hatások elleni felkészülés így időben elkezdhető. A víz áradása okozta problémákat komolyan kell venni minden esetben. Az árvíznek több súlyos hatása is van. A romboló hatás kialakulhat a víz hidromechanikai „ütőhatásaiból" ami például a parti falsáncokat (például Westportnál- Connecticutban) könnyen szétrombolta. Ez történt a keleti parton fekvő településekkel, mikor az Atlanti-óceán hatalmas hullámokkal a partokra tört.

Mikor betör a víz az épületek közé, akkor a víz áramlásából adódó „mechanikai hatás" (sodró hatás) könnyen visz mindent, ami az útjába kerül. Mikor nagy sodrással halad a víz, akkor SOHA sem szabad kimenni a házból. Fontos továbbá, ha betör a víz a házba és telíti azt, akkor sem szabad kimenni a házból, mert kint az utcán sokkal rosszabb a helyzet és az emberiélet könnyen veszélybe kerülhet. Az utcákon árvízként szereplő víztömegnek van áztató hatása is, a vegyi anyagokat és egyéb szennyező anyagokat a pincékből, raktárakból kimossa, továbbá a csatornarendszerek elárasztásával fekáliával szennyeződhet a közterület és az ivóvízbázis - mint kritikus infrastruktúra – könnyen sérül és ez közegészségügyi és környezeti problémákat okoz. Ezek mind beigazolódtak New York (mint az egyik legjobban érintett nagyváros) különböző utcáin. A hatóságok az előző hurrikánok tapasztalatai alapján a lakosságot erről előre tájékoztatták. A két legfelkapottabb árucikk a palackozott viz (ivóvízbázis szennyezés miatt) és az elemlámpa (áramszünet esetén) volt.

Az elöntött területen az ott rekedt emberek élete is veszélybe került. Az épületek, utak, műtárgyak és más létesítmények részben vagy teljes mértékben víz alá kerültek, átáztak, rongálódtak, megsemmisültek. Az áramszolgáltatást és egyéb közműveket szüneteltetni kellett, nehogy a víz zárlatot okozzon az elektromos- és távközlési rendszerekben. Sajnos volt olyan kárterület, ahol gyorsan terjedő tűzzel kellett szembenéznie a tűzoltóknak, de közben a leszakadt villanyvezetékekben még volt áram. Itt egyértelmű az emberi mulasztás, mert a mentő erőknek ez életveszélyes helyzetet is teremthetett volna. A beavatkozóknak számolni kell a közlekedési úthálózatok és műtárgyak sérüléseivel is, ami a kárterülethez való megközelítést nehezítheti. Az árvíz miatt kialakulhat járvány, illetve fertőzés is. A csatornarendszerből kimosott szerves anyagok, a szennyvízhálózat feltöltése komoly közegészségügyi problémákat okoz. Haitin (Karib-térség) a Sandy miatti esőzések következtében kolera járvány alakult ki a szegényebb negyedekben.

A Sandy hurrikán által okozott tűzesetek a leszakadt felsővezetékek miatt keletkeztek. A nagy erejű szél a tűzet gyorsan szétterítette, ami a tűzoltási munkálatokat szinte lehetetlenné tette. A leszakadt vezetékek következtében nem volt közvilágítás. A sötétben a mentő munkálatokat a hatalmas víztömeg még jobban nehezítette. A leszakadt kábelekben viszont áram volt, amit csak később kapcsolt le az áramszolgáltató.

Queens kerületben leszakadt vezetékek miatt a 112 km/h-s széllökések hatására kb. 111 otthon égett le. Amit nem árasztott el víz, tűzben égett el. A hatalmas szélerő miatt a tűz irányítása lehetetlen volt, a tűzcsapokból a vízkivétel pedig az elöntés miatt nem volt kivitelezhető.

6. ábra. Több, mint 100 ház égett le Breezy Point-ban, Queens kerületben (New York) [19]

A kárterületen a mentési munkák végrehatását alapvetően befolyásolja az utak, a közművek műszaki állapota, használhatósága, valamint az épületek romosodása is. A Sandy hurrikán több fontos utat súlyosan megrongált, ami befolyásolta a mentési munkák végrehajtását: egyrészt a kárterületre való eljutást, másrészt a megrongált út, mint kritikus infrastruktúra lesz a későbbiekben megoldandó helyreállítási feladat. Azonnali helyreállítást igényel az út, ha egy város, vagy település be-kivezető útjaként funkcionál, mert logisztikai szempontok sérülnek, illetve (lakosság)ellátási nehézségek lépnek fel.

Stephen Flynn Northeastern Egyetem professzora szerint, a legfontosabb, a nemzeti létfontosságú infrastruktúrák (közlekedési rendszerek, az elektromos hálózat, a friss víz-és szennyvíztisztító rendszerek) biztonsága, amiket ellenállóbbá kell alakítani, fejleszteni a természeti katasztrófák hatásaival szemben. [20] Ez a lakosság kitettségét és érzékenységét csökkenti.

7. ábra. Az alsó-manhattani South Ferry állomás (1. számú metró vonala) elöntése [21]

A vihar következtében az áramellátó rendszer is sérült. Több helyen a felsővezetékek súlyos mértékben rongálódtak meg. A vihar következtében hirtelen lezúduló csapadékmennyiség feláztatta a talajt, amit az erős széllökések könnyen kicsavartak, kidöntöttek, amik egy része a vezetékekre ráborultak így érve el vezetékszakadást. Az egyik

erőmű is megsérült, mert víz áztatta el és nem tudta ellátni a ráháruló energiaigény kiszolgálását. Felrobbant, tovább növelve a lakosság áram nélkül maradását. Ez több ponton is veszélyes. Egyrészt több védekezési, tájékoztatási rendszert nem lehet működtetni. A lakásban maradtak szempontjából: kint tombol a vihar, közben pedig hatalmas sodrású víztömeg zúdul végig az utcákon, amik az otthonokat elöntik vízzel. Egy sötét lakásban ilyen méretű katasztrófa komoly pszichés terhet ró az egyénre.

A mai urbanizált társadalomban az energia (áram) nélkülönözhetetlen alapvető létszükséglet. Ha a gépek, a kényelemért, biztonságért felelő gépek, szerkezetek, technikák nem működnek, akkor a pánik erősödésének (bizonytalanság növekedése idő múlásával párhuzamosan) veszélye egyre nagyobb mértékben és méretekben fennáll. Erre jó példa, hogy az áramszolgáltató szakembereit a lassabb helyreállítási munkálataik miatt több helyen megdobált a csalódott és dühös lakosság, ezért rendőri biztosítás mellett tudtak csak dolgozni.

53 halálesettel New York államban történt a legtöbb emberi tragédia, ebből New York Cityben 43 fő vesztette életét. New Jerseyben 37-en haltak meg, Pennsylvaniában 13-an, Marylandben 11-en, Nyugat-Virginiában 6-an, Connecticutban 5-en, Virginiában 3-an, Észak-Karolinában 3 ember halt meg a Sandy hurrikán tombolása miatt az Egyesült Államokban. [22] A Sandy hurrikán kb. 70 milliárd dollárnyi kárt okozott. A lerombolt vagy súlyosan megrongált otthonok számát mintegy hatszázezerre becsülik.

ÖSSZEFOGLALÁS

Amerikában minden évben van hurrikán. Hivatalosan a június 1-től november 30-ig tartó atlanti hurrikán időszak az amerikai lakosság rémálma. Ebben a természeti jelenséggel teli ciklusban minden egyes amerikai a saját önmentési és a szervezett, katasztrófa-elhárítási védelemre, ismeretekre szorul. Az egyik kihívás, hogy a szezonban egy területet több természeti anomália is érinthet rövid időn belül. Többször volt olyan alkalom, hogy a második természeti csapás nem volt olyan intenzív, mint az elődje, de mégis rendkívüli hatásokkal bírt, mert a környezet és a benne élők nemrég éltek át egy pusztító eseménysorozatot, így az érzékenység nagyobb a második esetében. Ennek megfelelően a lakosságfelkészítés nagyon nagy figyelmet kell, hogy kapjon. Az esemény bekövetkezte előtt, közben és utána a védekezési vagy kárcsökkentő lehetőségek ismerete és begyakorlása életeket ment.

A hurrikánok, trópusi viharok számos olyan hatás együttessel rendelkeznek, amit a társadalom szenved el, illetve egyre nagyobb mértékben az alapvető ellátást biztosító infrastruktúrák. Az amerikai lakosság a 21. században folyamatosan átalakul. Több olyan változás van, ami nem a biztonságot szavatolja egy közösségnek, hanem a kitettséget. A folyamatosan növekvő energiaigények, a természeti környezetet benépesítő társadalom bizonyos időközönként szembesül a természet pusztító nagyságával. A hatások vizsgálatánál célszerű, ha az emberi szokásokat is elemezzük. Az egyik legsürgetőbb probléma maga az építkezési szokások. Egyrészt a tengerparti települések fenntarthatatlan területfoglalásai (betelepülései), továbbá az épületek anyagai. A faszerkezetű házak sokkal gyengébbek, mint a téglából, vasbetonból készültek. Az utóbbiak a szélnek jobban ellenállóbbak és a tűzterjedésük is lassabb. A másik probléma, hogy egyre nagyobb értéket halmoznak fel egyre kisebb területen, így a biztosítások kártalanítása egyre nehezebb feladat.

A Sandy hurrikán az amerikai történelem második legpusztítóbb természeti jelensége. Mérete alapján az egyik legnagyobb. Olyan nagy területet foglalt le, hogy az egész keleti partot érintette. Afrikától indulva, haladt a Karib térség felé, ahol több országban fejtette ki pusztító hatását. Sajnos a Karib térségi kimélyülését nem lehetett előre eredményesen kimutatni, de az amerikaiak „nagy szerencséjére" a további történéseket egész pontosan tudták előre jelezni. Az amerikai előrejelzések mellett európai becslések és számítások is előtérbe kerültek, olyannyira, hogy az európai előrejelzések pontosabban és előbb születtek

meg. Az európai modellek előnye a jobb rácsfelbontás és a korszerűbb technológiai háttérnek köszönhető. Mindenesetre mindkét futtatási eredményt fel lehetett használni, így a lakosság - az előrejelzések alapján – az érintett területekről történő kitelepítés megfelelő időben elkezdődött. Az evakuálási parancsot a szükségállapot kihirdetése után már katonai támogatással bonyolították le. A megjelölt kiürítési zónákat térképeken ábrázolták, amit nyilvánossá tettek a lakosság számára. A FEMA, mint a hivatalos katasztrófavédelmi szerv közleményben hívta fel a figyelmet a közelgő veszélyre, és adott ki lakosságot érintő helyes információkat. A politikusok is részt vettek az előkészületekben és kérték az amerikai embereket a hatóságokkal történő együttműködésére. A hurrikán Atlantic City mellett érte el a szárazföldet és fejtette ki pusztító hatásait. A rendkívüli romboló hatást a szél, a csapadék és a vihardagály okozta. A mélyen fekvő területeket az alacsony légköri nyomás következtében fellépő hullámok könnyen elöntötték, sőt néhány várost ölelő folyót megduzzasztva okozott nagymértékű áradásokat. Az elöntések több létfontosságú infrastruktúrát is elöntött, több helyi probléma sorozatot generálva ezzel. A baj ott tetőzött mikor egyes káresemények egy újabb káros hatást gerjesztett, ami komplexebb és méreteiben nagyobb pusztító hatást fejtett ki. Az egyik legfontosabb üzenete a Sandy hurrikánnak, a térben és időben egyszerre fellépő negatív hatások jelenléte ott ahol maga az ember él, vagy ott ahol nem biztos, hogy építési szándékkal élnie kellene. Ez egyértelmű figyelemfelhívó jelzés, amire a társadalomnak cselekednie kell…

ÖSSZEGZETT KÖVETKEZTETÉSEK

A hurrikános időszakokat vizsgálva megállapítható, hogy egyre pusztítóbb hurrikánokkal, trópusi viharokkal kell szembenézni. Az óceán folyamatosan melegednek, ami annyit jelent, hogy a hurrikánok száma nem, de az intenzitásuk növekedni fog. Erre példa az utóbbi két szezon időjárási anomáliái. Ez azért fontos, mert a jövőben is számolni ezeken a területeken hasonló erejű, jellegű természeti csapással. Ez viszont megkérdőjelezi a tengerparti települések fenntarthatóságát. A szeminolai (Florida) és póheteni (New Jersey és Pennsylvania területén) indiánok nem építkeztek a tengerpartokra. Az európai telepesek azonban nagyvárosokat hoztak létre (Miami, Boston, New York, stb.).

Ahhoz képest, hogy ez a hurrikán átmérőjében nagyon hatalmasnak mondható, nem okozott annyi emberi tragédiát (bár 253 áldozattal több volt, mint kellett volna lennie). Viszont anyagi kárt igen. Bebizonyosodott, hogy az időben és térben összetett, pusztító hatásokra a létfontosságú infrastruktúrák nagyon érzékenyek, és a természeti jelenségekre könnyen rongálódnak, zavarokat okozva a lakosság életritmusában.

Meteorológiai szempontból a Sandy hurrikán nem volt szupervihar. Ami viszont megemlítendő, hogy szélességében és hosszában kiterjedt volt, ami a rendkívüliségét alapozza meg. A kérdés, hogy ennyire hatalmas természeti jelenségre fel lehet-e készülni. A térben és időben egyszerre támadó hatások „elviselésére” csak a gazdagabb országoknak van esélye. Mennyire növeli meg a szegényebb közép- és dél amerikai emberek migrációs hajlamát a nagyobb védekezést felmutató észak-Amerika.

Felhasznált irodalom

[1] [OMSZ]: Légköri képződmények

http://owww.met.hu/omsz.php?almenu_id=misc&pid=metsuli&pri=1&sm0=&dti=5 (2013. január 16.)

[2] TIBA CINTIA: A Katrina hurrikán, Eötvös Loránd Tudományegyetem Földrajz- és Földtudományi Intézet Meteorológiai Tanszék, Budapest: 2011. pp. 46.

http://nimbus.elte.hu/hallgatok/graduated/docs/BSc/2011/TibaCintia_2011.pdf (2013. január 16.)

[3] [Külügyminisztérium] Hurrikánok, tájfunok, trópusi ciklonok

http://www.kormany.hu/download/d/c4/10000/Hurrik%C3%A1nok,%20t%C3%A1jfunok,%20tr%C3%B3pusi%20ciklonok.pdf (2013. január 16.)

[4] [USACE] 2012 Hurricane Season

http://www.usace.army.mil/Missions/EmergencyOperations/HurricaneSeason.aspx (2013. január 17.)

[5] [OMSZ]: A 2012-es atlanti hurrikán szezon 4.5 percben, 2012. december 3.

http://www.met.hu/ismeret-tar/meteorologiai_hirek/index.php?id=461&hir=A_2012-es_atlanti_hurrikan_szezon_4.5_percben (2013. január 16.)

[6] [COAPS]: 2012 FSU COAPS Atlantic Hurricane Season Forecast http://coaps.fsu.edu/hurricanes/ (2013. január 16.)

[7] [WIKIPÉDIA] 2012 Atlantic hurricane season,

http://en.wikipedia.org/wiki/2012_Atlantic_hurricane_season (2013. január 16.)

[8] [NHC]: 2012 Atlantic Hurricane Season, http://www.nhc.noaa.gov/2012atlan.shtml (2013. január 16.)

[9] [OMSZ]: Röviden a Sandy hurrikánról, 2012. október 30.

http://www.met.hu/omsz/OMSZ_hirek/index.php?id=420&hir=Roviden_a_Sandy_hurrikanrol (2013. január 16.)

[10] [FEMA]: Hurricane Sandy: Timeline, http://www.fema.gov/hurricane-sandy-timeline (2013. január 17.)

[11] [HOTDOG]: Sandy hurrikán, http://www.hotdog.hu/worldgeo/katasztrofak/sandy-hurrikan (2013. január 16.)

[12] [ABCNEWS]: Superstorm Sandy's Wide Swath of Destruction

http://abcnews.go.com/International/slideshow/hurricane-sandy-east-braces-superstorm-17561482 (2013. január 16.)

[13] DR. HORNYACSEK JÚLIA**:** A települési védelmi képességek a katasztrófa-kihívások tükrében, a települések katasztrófa-elhárítási feladatai, a végrehajtáshoz szükséges helyi védelmi képesség alapvető területei, azok kialakításának folyamata. "Biztonságunk érdekében" Oktatási- és Tanácsadó Tudományos Egyesület Budapest, 2011. pp. 57. ISBN: 978-963-08-2606-8

[14] [DAILYMAIL]: MARK DUELL - JILL REILLY: FIFTY DEAD...and it's NOT over: Obama's grim warning as he prepares to visit scenes of hurricane 'major disaster' tomorrow, In. Mail Online, 2012. október 30., 1.-2. kép: http://www.dailymail.co.uk/news/article-2225108/Hurricane-Sandy-2012-pictures-FIFTY-DEAD--NOT-over.html#axzz2Kj3ncXYg (2013. január 16.)

3. kép, jobb oldalt: [ABCNEWS]: Superstorm Sandy's Wide Swath of Destruction, 49. fotó

http://abcnews.go.com/International/slideshow/hurricane-sandy-east-braces-superstorm-17561482 (2013. január 16.)

[15] Bal oldali kép: [WordPress]: Hurricane Sandy Slams into Northeast USA » 00 Hurricane Sandy. Hoboken NJ. 30.10.12., http://02varvara.wordpress.com/2012/10/30/hurricane-sandy-slams-into-northeast-usa/00-hurricane-sandy-hoboken-nj-30-10-12/ (2013. január 16.)

2. kép: CAROOM Eliot: N.J. out of power: 2.38 million still lack electricity, 2012, október 31., http://www.nj.com/news/index.ssf/2012/10/nj_out_of_power_238_million_st.html (2013. január 16.)

3. kép: GIARDINO, Carisa: Village Lost 516 Trees to Sandy, 2012. november 19.,

http://gardencity.patch.com/groups/hurricane/p/village-lost-516-trees-due-to-sandy (2013. január 16.)

[16] [ABCNEWS]: RAY, Robert (photo): Superstorm Sandy's Wide Swath of Destruction, 99. fotó http://abcnews.go.com/International/slideshow/hurricane-sandy-east-braces-superstorm-17561482 (2013. január 16.)

[17] [WIKIPÉDIA]: Meteorological history of Hurricane Sandy

http://en.wikipedia.org/wiki/Meteorological_history_of_Hurricane_Sandy (2013. január 16.)

[18] FÖVÉNYI, Attila: Sandy: Egy hurrikán New Yorkban, Budapest, 2012. november 28., pp. 22. http://www.mettars.hu/wp-content/uploads/2012/12/Sandy.pdf (2013. január 16.)

[19] [CBSNEWS]: Before-and-after views of Sandy destruction 1. fotó, http://www.cbsnews.com/2300-201_162-10014400.html (2013. január 16.)

[20] KORNWITZ Jason: Taking lessons from Hurricane Sandy, 2012. november 2., http://phys.org/news/2012-11-lessons-hurricane-sandy.html (2013. január 16.)

[21] [ABCNEWS]: Photo: METROPOLITAN TRANSPORTATION AUTHORITY: Superstorm Sandy's Wide Swath of Destruction, 57. fotó, http://abcnews.go.com/International/slideshow/hurricane-sandy-east-braces-superstorm-17561482 (2013. január 16.)

[22] [MTI]: Sandy hurrikán - 132-re nőtt a halálos áldozatok száma az Egyesült Államokban és Kanadában, 2012. november 16., http://archiv1988tol.mti.hu/Pages/HirSearch.aspx (2013. január 16.)

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

András Németh - Attila Horváth – Attila Gulyás
nemeth.andras@uni-nek.hu

ULTRA WIDEBAND DATA CHANNELS FOR SPECIAL OPERATIONS FORCES

Abstract

Hungarian and coalition special operations forces – striving to satisfy the growing need for information – conduct information and communications support for their operations using almost the entire throughput capacity available to them. Innovative methods, such as extremely high frequencies and alternative modulation modes, offer so far unprecedented ways in frequency bandwidth development. Transmission technology, miniaturization, and the development of optimization processes facilitate the use of innovative applications in providing increased bandwidth and channel capacity with smaller form factor and less power consumption. This scientific essay presents a usable solution to achieve increased bandwidth for supporting the full spectrum of the voice and data communications activity of special operations forces.

A nemzeti és koalíciós különleges műveleti erők - a megnövekedett információigény kielégítése céljából - a rendelkezésükre álló rádiófrekvenciás spektrum lehető leghatékonyabb kihasználásával igyekeznek megvalósítani műveleteik infokommunikációs támogatását. Innovatív megoldásokkal (magasabb frekvenciasávok használata, magasabb rendű modulációs módok alkalmazása) újabb lehetőségek nyílnak meg a jelenleg rendelkezésre álló sávok kiterjesztésére. Az átviteltechnika, - technológia, és miniatürizáció, valamint az optimalizálási eljárások fejlődése olyan új megoldások alkalmazását teszi lehetővé, amelyek a csatorna-sávszélesség hatékony felhasználása és a támogató rendszerek méret és energiafelvétel csökkentése területén jelentős előrelépést jelenthetnek. A közleményben egy ilyen lehetséges megoldás, illetve annak háttere kerül bemutatásra a különleges műveletek teljes spektrumában végrehajtott műveletek híradó és informatikai támogatása területén.

Keywords: *bandwidth, special operations forces, communications ~ sávszélesség, különleges műveleti erők (KME), híradó biztosítás*

INTRODUCTION

Numerous scientific essays have been published in military literature about the operations carried out by conventional and special operations forces, manoeuvres in the open field, on different types of terrain and in built-up areas and about planning and executing combat activities. The tasks of small units include support to own force and the enhancement of combat effectiveness. If we look at 21st century military operations and the political and economic processes of our asymmetric and multi-polar globe, it can be seen that the war on international terrorism requires special methods, techniques and procedures that meet the new challenges [1].

The training and preparation for battle of international special operations forces require a special emphasis on information and communications support. The 21st century witnesses revolutionary developments in the microelectronics industry, both in civilian and military applications. These developments enable the special operations forces to reach a higher level of operational effectiveness and facilitate a higher level of situational awareness[1] [2].

In military jargon we can often come across the phrase "digital soldier", i.e. a soldier equipped with target-oriented optical and communications and information devices, integrated weapons and communications systems which provide secured communications with command and control [3]. His equipment consists of modern software defined radios[2] for voice and data communications systems to visualize the movements of own forces for better situational awareness[3], systems against improvised explosive devices[4] and systems to process, analyze and transmit aerial reconnaissance data [4].

The requirement of near real time data transmissions and situational awareness visualization necessitate the use of satellite communications to maintain battlefield initiative and superiority and consequently achieve success. As operational communications require higher and higher bandwidths to transmit the increased amount of information, a lot of attention must be paid to how data transmission channels are designed in the interest of the optimal utilization of the frequency spectrum. Its practical realization requires great familiarity with the command and control systems and, if necessary, their reinforcement and further development with modern software defined(SD) radios.

This essay tries to provide an overview of a wide bandwidth radio communications system that can broaden the possibility of special operations applications worldwide.

SPECIALTIES OF SOF[5] OPERATIONS

In order to provide signal and IT support as well as information security for SOF commanders, planners must know the full spectrum of SOF operations. In peacetime and in the battle preparation phase, it may be the basis of the development of an operable and efficient system, which in the theatre of war – even with considerable changes if required – is capable of supporting command and control. The AJP-3.5[6] defines more than precisely the SOF operations in the NATO/ISAF joint operational area. These are special reconnaissance and surveillance (SR&S), direct action (DA) and military assistance (MA). SR&S complements national and allied theatre intelligence collection assets and systems by obtaining specific, well-defined, and possibly time-sensitive information of strategic or

[1] Situational Awareness SA
[2] Software Defined Radio SDR
[3] Blue Force Tracking System BFTS
[4] Improvised Explosive Device IED
[5] SOF - Special Operations Forces
[6] AJP-3.5 – Allied Joint Doctrine for Special Operations

operational significance. It may complement other collection methods where constraints are imposed by weather, terrain-masking, hostile countermeasures or other systems availability. SOF may conduct these tasks separately, supported by, in conjunction with, or in support of other component commands [5]. DA missions are precise operations that are normally limited in scope and duration. Forces usually incorporate a planned withdrawal from the immediate objective area. DA is focused on specific, well-defined targets of strategic and operational significance, or on the conduct of decisive tactical operations. SOF may conduct these tasks independently, with support from conventional forces, or in support of conventional forces [6]. MA is a broad spectrum of measures in support of friendly forces throughout the spectrum of conflict. MA can be conducted by, with, or through friendly forces that are trained, equipped, supported, or employed in varying degrees by SOF. The range of MA is thus considerable, and may vary from providing low-level military training or material assistance to the active employment of indigenous forces in the conduct of major operations [7].

The security requirements of SOF demand that special care is taken to ensure that SOF C2[7] is closely integrated with the C2 of the joint force through appropriate liaison and communications and information systems interfaces. NATO and the nations are responsible for the extension of secure CIS connectivity to the highest level of national or multinational tactical and operational command in theatre. For special operations this equates to the joint force command providing connectivity to the combined joint forces special operations component command (CJFSOCC) for C2 during the operations and exercises. The nation appointed is generally responsible for providing CIS connectivity to the highest level of command of all assigned, attached and supporting elements. The CJFSOCC is also responsible to ensure that CIS connectivity is provided to all liaison teams. Nations are responsible for providing their own internal CIS connectivity. Secure CIS connectivity for protection of sensitive information should be provided to the maximum extent possible. When secure CIS is provided within a national unit, secure (cryptoized) connectivity should be provided down to national levels for interface purposes. Secure CIS should include provisions for primary voice, data, and fax capability. Nations should consider tactical satellite communications as an invaluable means of establishing the secure connectivity. SOF requires a C2IS[8] network that allows timely C2 and implements the required security measures. All of these must be taken into consideration by the planners when the CIS planning process commences [8].

RULES AND REGULATIONS FOR ENABLING SOF CIS

With regard to SOF connectivity to host nations and the allied partners, no Hungarian CIS regulations are to be found, however NATO standardization agreements (STANAGs) are applicable for this purpose. The CIS planner in allied operations has to consider STANAG 5048 and STANAG 4637. STANAG 5048 provides the minimum scale of connectivity for communications and information systems for NATO land forces. It states that fully capable CIS connectivity is required to exchange C2 information and coordinating instructions on the battlefield between superior and subordinate headquarters at all levels, between the headquarters of a unit being supported and the supporting unit, and between adjacent formations on the battlefield. The responsibility for providing the required connectivity is governed by the general principles of higher formation to lower formation, supporting formation to supported formation, and left formation to right formation [9]. STANAG 4637 is

[7] C2 – Command and Control
[8] C2IS – Command , Control and Information System

a tactical communications regulation, which governs the tactical level means and procedures with regard to enabling CIS connectivity from tactical units to higher units. It defines the interoperability requirements for a federated network consisting of interconnected national elements, in such a way that it appears to the users as one network, fulfilling all defined requirements for user services and their defined Quality of Service (QoS), capacity, robustness, security, etc. In the long term, the concept aims to provide advanced interoperability capabilities (including e.g., mobility) for network-centric operations, but, due mainly to the capabilities of the present national tactical communication systems and the limited availability of advanced security solutions, an evolutionary approach will be used. The STANAG 4637 concept is service based, supports an extensive set of end-to-end user service, defines network services, permits an independent implementation of network elements (NE) by nations, where NE is an interconnection of communication assets, forming, e.g., any combination of a local area, wide area, or mobile networks, under the control of one nation, standardizes the IOP to provide connectivity between NEs. Interconnected NEs form STANAG 4637 Federated Network (TFN), allows multinational performance guarantees through Service Level Specifications (SLSs) and with corresponding instantiated Service Level Agreements (SLAs), and standardizes External Network Access Points (ENAPs) to provide connectivity between a NE and a civilian or non-tactical military network [10].

The only Hungarian joint regulation for CIS connectivity is the Joint Operational Doctrine of the Hungarian Defence Forces[9]. Under 4.2.4.3 are the requirements a CIS planner needs to consider when the planning process starts. This is the practical approach to the tactical and operational level CIS planning process, including the full spectrum of connectivity detailed in the above mentioned STANAGS [11].

TACTICAL LEVEL COMMUNICATIONS AND INFORMATION SERVICES

The smallest unit of SOF applications is the special operations task unit (SOTU). In the area of CIS connectivity, the following criteria need to be fulfilled. The CIS of SOTU is to be capable of supporting minimum one special operations forces command post, controlling 15 radio terminals in a common radio network and providing secure (classified) and unclassified services. The internal communications radio terminals of a SOTU need to be software defined radios that can provide Internet Protocol (IP) –based services and activate secure radio communications channels up to the level of NATO SECRET. They must provide wide bandwidth voice and data connection, keying and rekeying the radio terminals over the air (OTAR), and they have special waveforms, such as Soldier Radio Waveform (SRW) and secure wideband mode (ANW2) GPS[10] receivers. The terminals must be able to send and receive local positioning data and to operate both in open and secure channels using TYPE-I CCI[11] crypto keys. The radio terminals need to be compatible with high speed data networks and capable of sending and receiving imageries (jpeg, gif files) and video (mpeg4) signals in near real time. The radio devices must meet the requirements for high bandwidths and low weight so that they can be carried in soldiers' rucksacks.

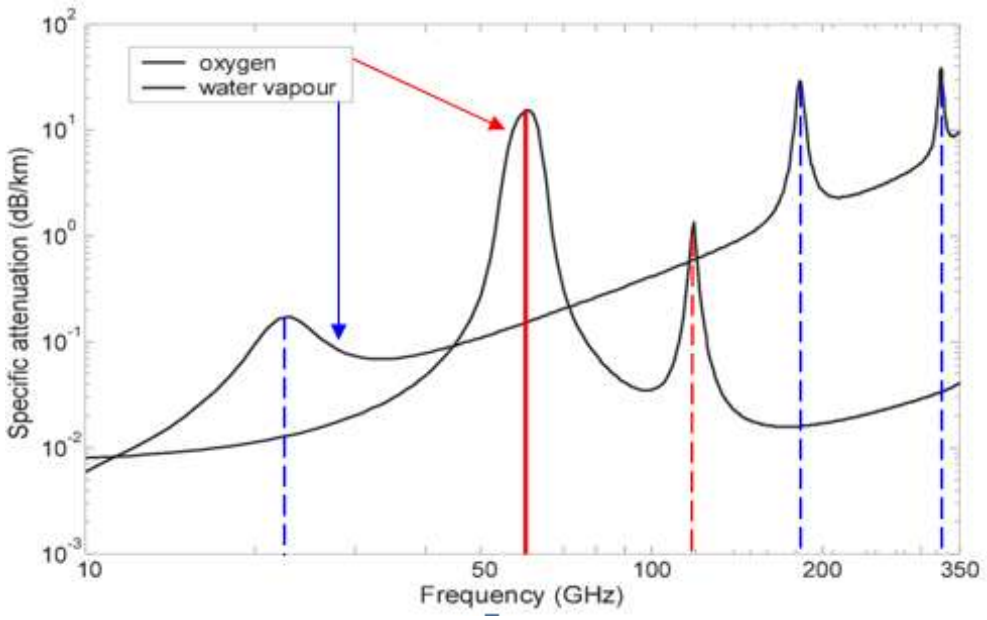
PROPERTIES OF THE RADIO CHANNELS

When planning radio frequency systems, one of the most important tasks is to examine those physical factors which affect the propagation of the radio waves and the possible services in that given frequency range. In the frequency range of millimetre waves – 60 GHz – the

[9] MH Összhaderőnemi Műveleti Doktrína v 1.0 ZMNE
[10] GPS – Global Positioning System
[11] CCI – Crypto Controlled Items

physical factors of radio propagation are considerably different than in lower frequency channels. The frequency band of 60 GHz is an umbrella-term for the frequency range from 54-67 GHz [12]. For civilian users, a part of the 60 GHz band is free for using (unlicensed) while other parts of the band are licensed. The narrowest band of the unlicensed part is in Australia (59.4 – 62.9 GHz). In Europe the average bandwidth is 9 GHz (57 - 66 GHz) [13].

In microwave channels the most significant difference between the specialties of frequencies originates from the attenuation by atmospheric gases (oxygen, water vapour and nitrogen). Since the nitrogen component's effect on the transmission is only significant in the 300 GHz frequency range and above, table 01 only shows the oxygen and the water vapour attenuations in that band.



1. figure. [14]

It can be seen that the peaks of attenuation are formed where the resonance of the polarized molecules is the highest. In the case of water vapour, the first maximum is at 23 GHz with 0,2 dB extra attenuation, the second and the third absorption line is at 183 GHz and 324 GHz with an attenuation of 30/40 dB/km. The resonance of oxygen molecules is 1,5 dB/km in the frequency of 119 GHz, however, it is 15 dB/km in the frequency of 60 GHz which is the maximum of the resonance level [15]. At the edges of the 60 GHz band attenuation can reach 10dB/km. In addition to this, it is necessary to take into consideration the normal open-air power loss (128dB/km) [16]. More attenuation can be caused by vapour (rain) in the air and terrain features, such as mountains, valleys and hills in the way of radiofrequency propagation.

As a result of the above mentioned factors, the 60 GHz frequency bandwidth is mostly used in indoor applications by civilian users. In order to use the frequency range in outdoor military applications, it is necessary to install, operate and maintain (IOM) high-gain beacons such as high directivity antennas and to use line of sight connections between the data transmitter and the receiver. These services often meet the military requirements because they help to accomplish the operational requirements of radio electronic counter-surveillance and the prevention of problems caused by frequency jamming or spoofing. Examining the adaptive antenna systems that may be used, one can find several stationary antennas, whose performance, however, is not suitable for military applications, since the tactical and operational use in the ever-changing battlefield is far from stationary. Military planners and designers should try to find mobile military applications to meet the dual requirement.

Another difficulty for communications planners arises from the fact that the wide bandwidth results in frequency-dependent attenuations, in other words the various parts of the propagated frequency spectrum can be attenuated in different manners. Most channel-models do not take this rule into consideration [17].

For planning and designing a civilian application, several channel models have been developed and are described in scientific essays and articles [18][19][20]. These developments are modelling the civilian office environment, taking into consideration the effect of reflexions and multipath. Special operations forces often fight in built-up areas so these civilian models are also applicable to these special situations. In outdoor operations the probability of line of sight communications is higher but the effects of the environment, such as terrain, vegetation, vehicles, mobility and fading cannot be ignored.

The international frequency allocation defines both the frequency channels and the maximum radiated antenna power. The following wide bandwidth systems are currently under research and development. In the 60 GHz-frequency-range the maximum output power level (EIRP[12]) is allowed due to the fact that attenuation is also the highest in this frequency range. The EIRP for IEEE 802.11n[13] systems is 25 dBmW, and when using UWB only 10 dBmW is approved. However in 60 GHz-channels, it is possible to achieve 57 dBmW [21].

We need to consider other channel attenuations in particular frequency bands. In the case of a radio connection of 1 kilometre, which is actually unreal but easy to visualize even for amateur readers, using maximum EIRP, the UWB system's receiving antenna can measure -122 dBmW signal level. In the case of 802.11n and 60 GHz, the signal level is - 81 dBmW. Because of the higher attenuation at 60 GHz, the increased EIRP compensates, thus the same received level. In order to choose between the 2 feasible solutions we need to examine further aspects. At 60 GHz a smaller amount of interference can be measured and the signal to noise ratio (SNR) is more favourable than when using Wi-Fi devices. This is primarily due to the increased channel attenuation, which enhances channel separation. However, it is more expensive than Wi-Fi technology (802.11n – 2.4 GHz – 5 GHz) [22].

To measure the data speed of frequency channels, the bit rate in radio communications systems is quantified using the bit per second (bit/s) unit, which corresponds to the radio spectrum bandwidth in Hertz (Hz). Using the expression ultra wide band can be deceptive because the bandwidth depends on the modulation techniques engineers use to design the frequency channels. The order of modulation determines how many information bits can be transported in the given bandwidth, in other words, what is the specific data speed in the channels. The higher modulation process we use the more data symbols can be transported in the frequency channel [23]. The more symbols are used the higher bandwidth efficiency can be achieved. Challenges can emerge when increasing the number of symbols, as the symbols' distinctness is reduced. This effect spoils the efficiency of power-consumption because at a given noise-level, the signal-level measured at the receiving antenna site needs to be increased. It will reduce signal range for a given quality of service. This effect is increased by section attenuations, and consequently the bit losses are also increased, which is a communications challenge (danger) for both conventional and SOF units.

Summarizing the facts, designers have quite a wide bandwidth at 60 GHz. At the same time, higher-order modulations are more complicated to produce and their implementation often requires complicated technologies and is not really cost-effective so they are not the best

[12] EIRP – Effective/Equivalent Isotropic Radiated Power. EIRP is the amount of power that a theoretical isotropic antenna would emit to produce the peak power density observed in the direction of maximum antenna gain.

[13] IEEE 802.11n (2009) is an amendment to the IEEE 802.11-2007 wireless networking standard to improve network throughput over the two previous standards - 802.11a and 802.11g - with a significant increase in the maximum net data rate from 54 Mb/s to 600 Mb/s.

solution for communications planners taking into the consideration the financial cuts in electrical and informatics engineering [24]. If the goal is to design/install a system with 1 Gbit/sec data speed at 40MHz, which is the available bandwidth for 802.11n, 25bit/sec/Hz channel efficiency should be achieved, which is very difficult to realize. However, using the 60 GHz-channels, where 1 communications channel can be broader than 1 gigahertz (in the case of well-constructed radio hardware), the most simple modulation schemes may be suitable. Despite all this, it is worth devoting time and energy to developing higher modulation schemes in the 60 GHz-channels in order to find optimal solutions enabling forward error correction (via redundant bits), robust systems and advanced information security.

The physical dimensions of hardware in 60 GHz are smaller than lower frequency channels, which are favourable for SOF applications. For this reason communications planners have a wide range of possibilities to design physical and electromagnetic defence capabilities that meet the new requirements of electronic counter-countermeasures (ECCM[14]).

From SOF point of view, it is obvious to use this frequency range for SOF wireless communications systems when the distance between the members of the radio network is not more that 100 meters because the ECCM-capability is much better than in the case of other Wi-Fi systems. It is possible, through compromises, to optimize systems for specific applications, which can be used effectively in military (both conventional and SOF) operations.

ANTENNA SYSTEMS

While the antenna systems are actually, part of the radio channel, because of their importance, they are discussed separately. In 60 GHz-systems the most significant challenge is to produce the received signal level for special radios operated in this frequency range. This challenge can be met by planning a special antenna system to compensate for the radio transmitter system's weaker capability and the increased attenuation. Using special high-gain antennas, the lower level of output power can be counterbalanced. The special antennas radically decrease the electromagnetic radiation, thus reducing the possibility of signal jamming or spoofing, which is a basic requirement in SOF operations.

Using guided (vectored) antennas requires further compromises and can also increase the complexity-level of the hardware. The end-points of civilian systems are stationary [25] but the end-points of military systems (soldiers, vehicles) are always in motion. It requires some kind of radio network topology, where the radios and the antennas need to cover a special polar pattern of electromagnetic signals [26]. In order to satisfy the needs, it is necessary to use adaptive antennas in the soldier's uniform, called body-worn antennas. The solution is to disperse the adaptive antenna sets in the uniform. A more practical solution is to divide the antenna system into subsystems (micro strip antennas), and thus the hardware's mathematical apparatus is responsible for establishing electromagnetic lobes by switching between the subsystems**.** This is the MIMO[15] adaptive antenna system in which the input/output (I/O) channels are phase-controlled antennas. There are 2 levels of channel vector management. On the one hand the system needs to specify the end-points of the I/O channels, and on the other hand it has to manage the electromagnetic radiation of the active antennas attached to the I/O channels. The electromagnetic field is depicted mathematically by vectors and antenna control

[14] ECCM - Electronic counter-countermeasures is a part of electronic warfare which includes a variety of practices which attempt to reduce or eliminate the effect of electronic countermeasures (ECM) on electronic sensors aboard vehicles, ships and aircraft and weapons such as missiles. ECCM is also known as electronic protective measures (EPM), chiefly in Europe. In practice, EPM often means resistance to jamming.

[15] MIMO – Multiple Input / Multiple Output

is based on phase-information, so the system needs to use electromagnetic vectors. To put it more simply, the manageable number of vectors determines the number of end-points and the complexity of control.

The end-point control tasks can be reduced by network interaction. If an end-point is in the centre of the radio network, it is likely to have to connect several end-points. If the storage of channel-vectors is full, a new end-point cannot connect to it. In that case a "third party", a new end-point is necessary, and a redesign in the adaptive communications network map. The "third party" is extremely important in SOF applications when – in case of operations – the line of sight connection between the SOF operators does not always exist. In that case active repeaters are important. The end-point can operate as a repeater or node centre, which is its intelligent function. This function reduces the possibility of connection fails (channel dropping, bit-loss).

The directional control of the antennas can be done in two different ways. The more simple but disadvantageous way is when the controller chooses the direction of propagation from an internal list and the resolution of the internal list determines the antenna's gain and loss level. In the case of real adaptive functioning (adaptive antennas) the polar-pattern of body-worn antennas is the result of special individual tuning. This is a time-consuming but more precise method, in which the covered range of antennas and the SNR can be maximized [27].

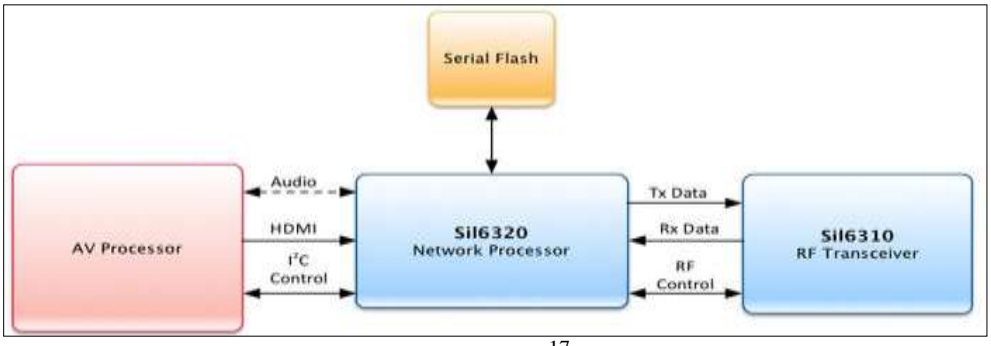
This assumes a special body-worn adaptive antenna system weaved into the uniform. This effort was published in the digital soldier model by the US Army [28].

CIVILIAN STANDARDS AND DEVELOPMENTS

The commercial exploitation of the 60GHz band is proceeding in two directions. Both the WirelessHD consortium and the Wireless Gigabit Alliance (WiGiG) are developing standards for high-definition (HD) video transmission for personal computers and home entertainment[29] [30]. Both companies are developing version 1.1 of their respective documents. The WiGiG published its brand-new innovation in June 2010 but the full system description is only available to the subscribers of the company. It is entirely based on the IEEE 802.11n standard (for media access control). The goals of the two 60-GHz standards are almost the same: 7 Gb/s data speed for uncompressed HD video transmission, minimum 10 meters transmission range with adaptive directed antennas and the possibility of securing the channels.

Based on these standards, implementation is possible even on a single chip because the dimension factors of 60 GHz circuits are much smaller than the circuits in 2.4 GHz. The WirelessHD is in advantage since its *Silicon Image Sil6300* chips are already on the market. The chipset consists of 2 chips, the *Sil6320* is the network processor which transforms the digital (HDMI[16]) signals for the 60 GHz transmission, while the *SIL6310* is the transmitter-receiver [31].

[16] HDMI – High Density Multimedia Interface



2. figure. [17]

Panasonic produces a new chipset by WiGiG standards. The *AR900TB* circuit by Qualcomm is a 3-band-chip, which consists of both the IEEE 802.11n and WiGiG standards. The WiGiG is more suitable for average radio applications, as it was even the basic development philosophy, while the WirelessHD integrates several application elements which are specifically for multimedia services [32].

3. figure. [18]

Taking into consideration the application of both standards, they are not directly applicable for military users in military radio devices because they ignore the special needs of military services. The best solution for developers is to use GaAS[19] or CMOS[20], based radio communications' chipsets and ICs[21]. These parts of integrated circuits would be cheaper and simpler to use and develop in military devices. The controlling algorithms and other basic-level signal processing units can be implemented within an FPGA[22] and attached to the 60 GHz radio communications devices to meet military (especially SOF) requirements.

In the course of development and manufacturing it is worth relying on national and international intellectual capital and practical experience represented by Hungarian manufacturers, engineers, enterprises and companies [33].

[17] http://www.totaltel.hu/content/03products/031_products.htm
[18] http://www.mwjournal.com/Article/Qualcomm_Acquire_Atheros/AR_10104/
[19] GaAs – Gallium-Arsenide
[20] CMOS – Complementary Metal Oxide Semiconductor
[21] IC – Integrated Circuit
[22] FPGA – Field-Programmable Gate Array

SUMMARY AND DEDUCTIONS

The special operations forces are specially trained and equipped to accomplish their tasks in the full spectrum of war and crisis response operations. They work mostly independently, in small units. They can be involved in indirect military action in crisis response operations or in providing military assistance and they can also be used in direct action. [34].

All levels of SOF need rapid, ready, reliable and interoperable communications and information systems (CIS) that provide interconnections to another CIS, improve the survivability of CCS and also provide the appropriate bandwidth for high speed communications and information transmission for reconnaissance and intelligence gathering purposes**.** Providing wider bandwidth with smaller devices is a manageable method for military applications especially in SOF applications. These types of devices primarily contribute to the extension of the communications range between SOF units by line of sight using ultra wide band channels to operate HD or HDMI special cameras and other high bandwidth data systems. The body-worn communications and information systems (adaptive directed antennas) increase the operational adaptation of the SOF operator (soldier) and provide a better chance to reach the common goal.

As a result of the development in the area of communications and information systems, the model of a digital soldier is appearing in the military services. The international SOF community will enjoy the benefits of this new development, which will make the SOF capable of adopting higher channel speed (bit speed) by using higher bandwidth, enhance IFF[23] capability and reduce the possibility of frequency jamming and spoofing.

The models described in this article are capable of providing communications and information support for SOF small units in built-up areas using high data speed wireless system applications for transporting voice, data, video signals by HD or HDMI resolutions applying line of sight (direct) communications channels. The aim is to use the systems described above for the transmission of HD video signals both in SOF and conventional operations. This method could be effectively used by explosive ordnance disposal (EOD) personnel. 60GHz is the most suitable frequency range for this purpose.

The current developments are aimed at the better utilization of the benefits of higher frequencies using high resolution video and extreme data speed provided by 60GHz digital channels [35]. National developers need to monitor the changes of the civilian electronic sector and adapt the innovations to military (conventional and special operations) applications.

References

[1] Kőszegvári Tibor: A különleges katonai műveletekről, Hadtudomány, 2006/1-2. p. 3. In: http://www.zmne.hu/kulso/mhtt/hadtudomany/2006/1_2/2006_1_2_3.html Letöltés ideje: 2012. március 26. 08:45

[2] Gácser Zoltán mk. őrnagy: A katona harci képességét növelő korszerű, hálózatba integrált egyéni felszerelésrendszerének kialakítási lehetőségei a Magyar Honvédségben, Doktori (PhD) értekezés, ZMNE KMDI 2008. p. 100-111. In: http://193.224.76.4/download/konyvtar/digitgy/phd/2008/gacser_zoltan.pdf Letöltés ideje: 2012. március 26 09:10

[3] Kőszegvári Tibor: A jövő század hadviselése és a különleges erők, Hadtudomány, 1994/4. p. 51-53.

[23] IFF – Identification Friend or Foe

[4] Gulyás Attila: Force tracking systems in SOF applications, AARMS Vol.8. (2009) pp. 604-605.

[5] AJP-3.5 Chapter II. 0202a. p. 2-1.

[6] AJP-3.5 Chapter II. 202b. p. 2-2.

[7] AJP-3.5 Chapter II. 202c. p. 2-3.

[8] AJP-3.5 Chapter V. 0509. p. 5-7.

[9] NATO STANAG 5048, C3 Edition No.5, Minimum scale of connectivity for Communications and Information Systems for NATO land forces: Principles p. 2.

[10] NATO STANAG 4637 Tactical Communications (TACOMs) edition 01. 18 June 2010. p. 11.

[11] MH Összhaderőnemi Műveleti Doktrína, verzió 1.0 2009. október 01. pp. 99-107.

[12] Su-Khiong (SK) Yong, Pengfei Xia, Alberto Valdes-Garcia: 60 GHz technology for Gbps WLAN and WPAN, John Wiley & Sons Ltd., 2011, p. 7.

[13] Su-Khiong (SK) Yong, Pengfei Xia, Alberto Valdes-Garcia: 60 GHz technology for Gbps WLAN and WPAN, John Wiley & Sons Ltd., 2011, p. 10.

[14] Babits László, Curgai-Horváth László, Héder Balázs, Bitó János, Frigyes István: Az 50-90 GHz frekvenciasávok alkalmazása ellátó hálózatokban, HTE Távközlési és Informatikai Hálózatok Szemináriuma, Zalakaros, 2008. október 15-17., p. 9. In: http://www.hte.hu/data/upload/file/Halozatok2008/14_Csurgai_L.pdf Letöltés ideje: 2012. március 26 08:21

[15] Ultra Wideband Communications: Novel trends – system, architecture and implementation, szerk. Mohammad A. Matin, InTech, 2011, p. 332.

[16] Su-Khiong (SK) Yong, Pengfei Xia, Alberto Valdes-Garcia: 60 GHz technology for Gbps WLAN and WPAN, John Wiley & Sons Ltd., 2011, p. 22.

[17] Ábel Dániel: Médiatechnológia és Kommunikáció I. Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Főiskolai Kar, Híradástechnikai Intézet, 2009, pp. 39-41.

[18] Trevor Manning: Microwave Radio Transmission Design Guide Second Edition, ARTECH HOUSE 2009, p. 153.

[19] Ismail Guvenc, Sinan Gezici, Zafer Sahinoglu és Ulas C. Kozat: Reliable Communications for Short-range Wireless Systems, Cambridge University Press 2011, p. 61.

[20] Su-Khiong (SK) Yong, Pengfei Xia, Alberto Valdes-Garcia: 60 GHz technology for Gbps WLAN and WPAN, John Wiley & Sons Ltd., 2011, pp. 24-27.

[21] IBCS Hungary Group: Ismerkedés IEEE 802.11n hálózatokkal, In: http://www.bcs.hu/letoltes.php?d_id=863 Letöltés ideje: 2011. november 20. 18:24

[22] ITU-R Terrestrial Services FAQ In: http://www.itu.int/ITU-R/terrestrial/faq/index.html G013. 5.150, Letöltés ideje: 2011. november 29. 00:09

[23] dr. Bozóki Sándor: Modulációs mérések a budapesti AM mikro rendszer digitális csatornájában, Antenna Hungária Rt, Multimédia Fejlesztési Osztály, In: http://www.omikk.bme.hu:8080/cikkadat/bitstream/123456789/472/1/2002_5bol2.pdf, Letöltés ideje: 2011. december 23. 18:09

[24] Su-Khiong (SK) Yong, Pengfei Xia, Alberto Valdes-Garcia: 60 GHz technology for Gbps WLAN and WPAN, John Wiley & Sons Ltd., 2011, p. 4.

[25] Simon L. Cotton, William G. Scanlon, Efstratios Skafidas, Bhopinder K. Madahar: Millimeter-wave stealth radio for special operations forces In: Military Microwaves Supplement, 2010. augusztus, p. 10.

[26] Simon L. Cotton, William G. Scanlon, Efstratios Skafidas, Bhopinder K. Madahar: Millimeter-wave stealth radio for special operations forces In: Military Microwaves Supplement, 2010. augusztus, p. 14.

[27] David Vye, Richard Mumford and Patrick Hindle: The spy who loved microwaves In: Microwave Journal, 2011. október, p. 30.

[28] http://www.armedforces-int.com/projects/future_force_warrior_system.html
Letöltés ideje: 2011. december 07. 22:13

[29] Overview of WirelessHD Specification Version 1.1 D1, p. 3 In:
http://www.wirelesshd.org/pdfs/WirelessHD-Specification-Overview-v1.1May2010.pdf
Letöltés ideje: 2011. december 23. 18:21

[30] WiGig white paper, p. 2 In: http://wirelessgigabitalliance.org/?getfile=1510
Letöltés ideje: 2011. december 23. 18:25

[31] SiI 6320/SiI6310 WirelessHD® HRTX Chipset
In: http://www.siliconimage.com/products/product.aspx?pid=206
Letöltés ideje: 2011. november 29. 00:54

[32] Panasonic Develops 60GHz Multi-Gigabit Wireless Circuit Technology for Mobile Devices Based on Major Wireless Standards,
In: http://panasonic.co.jp/corp/news/official.data/data.dir/en110602-3/en110602-3.html
Letöltés ideje: 2011. november 29. 01:12

[33] dr. Kazi Károly: Mikrohullámú fejlesztési irányelvek, Bonn Magyarország Elektronikai kft. In: http://www.bhe-mw.eu/?page=products&level=0
Letöltés ideje: 2011 december 23. 18:36

[34] MH Különleges Műveleti Erők alkalmazási irányelvei, Nyt. szám: 94/658, 2008. október, p. 14.

[35] Simon L. Cotton and William G. Scanlon: Millimeter-wave Stealth Radio for Special Operations Forces, Microwave Journal Vol.53. No. 8. August 2010. p. 6.

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Baráth Artur
magicman@mail.duf.hu

AZ ISO 27799:2008 SZABVÁNY AZ INFORMATIKAI BIZTONSÁG KEZELÉSE AZ EGÉSZSÉGÜGYBEN

I. RÉSZ

Absztrakt

Az informatikai rendszerek biztonságos, hatékony, megbízható működéshez elengedhetetlen a vonatkozó törvényi rendelkezések és szakmai normák beható ismerete. Ezen tudás elsajátításához ad segítséget jelen munkám, amelyben, a címben szereplő szabvány részletes ismertetésének első része olvasható.

The knowledge of professional norms and related laws are indispensable for the safe, reliable and effective work of informatics systems.For acquiring this knowledge my work provides help, in which the first part of the detailed presentation of the title standard is readable.

Kulcsszavak: *egészségügy, informatika, biztonság, ISO 27799:2008, szabvány ~ healthcare, informatics, safety, ISO 27799:2008 standard*

BEVEZETÉS

Ezen cikk első darabja egy háromrészes cikksorozatnak, melyben az ISO 27799:2008 számú szabványt dolgozom fel annak érdekében, hogy segítsek azoknak, akik Magyarországon kívánnak a témában dolgozni vagy kutatni. A vizsgált szabvány az egészségügyi informatikai rendszerek egységesítését és minőségének javítását hivatott segíteni, azáltal, hogy pontosan deklarált és megszabott környezetet biztosít a működéshez.

Magyarországon a napokban lehetett hallani az országos egészségügyi rendszerek átfogó modernizációjáról, egységesítéséről, a köztük szükséges átjárhatóságok megvalósításáról. A törekvés üdvözlendő és természetesen megkésett, ennek ellenére bizakodásra ad okot, hogy foglalkoznak a témával.

Egy biztonságos és nemzetközi szinten is kompatibilis, elismert rendszer kialakításához elengedhetetlen a vonatkozó szabványok és jogszabályok ismerete. Magyarországon sajnos még igen kezdetleges állapotok uralkodnak az egészségügyi informatikai rendszerek biztonsága területén, amit rövid időn belül orvosolni kell, hisz a társadalom és az ország érdeke egy stabil, hatékony, biztonságos ellátórendszer létesítése. Ezen folyamat elindulásához nyújt fontos segítséget cikksorozatom.

AZ ISO 27799:2008 SZABVÁNY

Az ISO 27799:2008 nemzetközi szabvány az egészségügyi informatika működését támogató iránymutatásokat határoz meg. A szabvány meghatározza egy sor részletes ellenőrzés irányítását az egészségügyi információs biztonság vizsgálatára, és a legjobb gyakorlati iránymutatásokat. Megvalósításával az egészségügyi szervezeteknek és egyéb egészségügyi információk kezelőinek képes biztosítani a minimálisan szükséges biztonsági szintet, amely megfelel saját szervezeti körülményeik között, és amely fenntartja a személyes egészségügyi adatok bizalmasságának, sértetlenségének és rendelkezésre állásának körülményeit. A szabvány minden egészségügyi információ vonatkozik, függetlenül a tárolásra használt eszközöktől és függetlenül a továbbítási csatornától.

Az ISO 27799:2008 nemzetközi szabvány az ISO/IEC 27002 nemzetközi szabvánnyal együtt alkalmazandó, és együtt határozzák meg, mire van szükség a biztonságos tájékoztatáshoz az egészségügyi ellátásban.

A szabvány technológia-semleges, mert a biztonsági technológiák gyorsan fejlődnek, miközben a szabvány előírásai hosszú távon is érvényben maradnak.

A szabvány szakkifejezései és meghatározásai

Jelen szabvány alkalmazásában az alábbi fogalom-meghatározásokat kell alkalmazni:

Az egészségügyi informatika egy tudományág, amely érinti a kognitív, az információ-feldolgozó és a kommunikációs feladatait az egészségügyi gyakorlatnak, oktatás és kutatás, beleértve az információs tudomány és a technológia támogatását.

Ennek kiszolgálására szolgál az egészségügyi információs rendszer, ami lényegében egészségügyi ellátással kapcsolatos információk tárolása számítógéppel feldolgozható formában, feladata kezelni és biztonságosan tárolni az adatokat, továbbá hozzáférést biztosítani azokhoz jogosult felhasználónak. E kettő terület összehangolt munkája is kell az egészségügyi ellátás működéséhez, ami bármilyen típusú szolgáltatás szakemberek részéről, akár paraprofessionálisan[1] rendszerben is.

Az egészségügyi ellátás működését biztosítja az egészségügyi szervezet, ami általános kifejező leírása többféle típusú szervezetnek, amelyek az egészségügyi szolgáltatásokat

[1] Állapot, mikor a professzionális képzettség és tudás a személy birtokában van, viszont a cím és jogosultság nincs. Mindig supervisori felügyeletet kíván meg a működése.

biztosítják. Ezen szervezeteken belül végeznek munkát az egészségügyi szakemberek, akik jogosult személyek, melyek hivatalos testület által elismert minősítéssel végeznek bizonyos egészségügyi feladatokat. Az egészségügyi szolgáltató, ami bármely személy vagy szervezet, aki részt vesz a nyújtott vagy kapcsolódó egészségügyi szolgáltatásokban az ügyfél részére, vagy jóléti gondozó biztosítja a körülményeket a munkavégzéshez

A felelősségre vonhatóság érdekében definiálni kell többek között azonosítható személyt, aki az a személy, aki azonosítható, közvetlen vagy közvetett módon. Különösen egy azonosító szám vagy több egyedi tényező és a személy fizikai, fiziológiai, mentális, gazdasági, kulturális vagy társadalmi jellemzői alapján.

Személyes egészségügyi adatok: Tájékoztatás az azonosítható személy részére, amely kapcsolódik az egyén fizikai vagy mentális egészségi állapotához, továbbá azon egészségügyi szolgáltatások adatai, amiket az egyénnek nyújtottak. Ezen adatok az alábbiak lehetnek:

- a) tájékoztatás a nyilvántartásba vételről az egyén számára;
- b) információ a kifizetések vagy jogosultság az egészségügyi ellátás tekintetében az egyén részére;
- c) egy számot, szimbólumot vagy különleges egyedi jelet, mely azonosítja az egyes egészségügyi célokra;
- d) származó információi vizsgálatnak, egy testrésznek vagy testi anyagnak;
- e) azonosítása egy személy (pl. egy egészségügyi szakember), mint az egészségügyi szolgáltató, az egyén számára.

További meghatározandó fogalom az ellátás tárgya: ez, egy vagy több személy beütemezése fogadására, illetve egészségügyi szolgáltatás nyújtására. Eközben szükséges használni vagyontárgyakat, ami bármi lehet, ami értéket jelent a szervezet részére. Ezen szolgáltatások biztosítóját és tárgyak felhasználóját felelősségre vonhatóvá kell tenni, ami egy tulajdonság, amely biztosítja, hogy a végrehajtott intézkedések hatásai egyénekhez legyenek köthetőek a gazdálkodó egység vezetői által. Szorosan ide kapcsolódik a biztosíték, ami egy sor megfelelési folyamat eredményein keresztül a szervezet részéről megvalósítja a bizalom státuszát az információbiztonsági irányítás területén. Mindezek mellett elérhetőséget is biztosítani kell, ami azon tulajdonság, hogy hozzáférhető és használható igény által a felhatalmazott szervezet vagy személy által.

Az egészségügyi informatikai biztonság

Az egészségügyi informatikai biztonság célja a szabvány szerint, hogy fenntartsa az információk titkosságát, hozzáférhetőségének és épségének állapotát, beleértve a hitelesség, elszámoltathatóság és auditálhatóság2 [1] területét is.

Titoktartási intézkedéseket kell tenni, hogy fennmaradjon az adatok integritása, ha másért nem, hogy ne férjenek hozzá a vezérlési adatokhoz, ellenőrzési nyomvonalakhoz és a rendszer egyéb adataihoz, oly módon, hogy lehetővé teszik a titoktartás sérülését. Ezen túlmenően, a betegbiztonság függ a titoktartás fenntartásától, a személyes egészségügyi adatok integritásától, ezek sérülése eredményezhet betegséget, sérülést vagy akár halált.

Hasonlóképpen, a magas szintű rendelkezésre állás különösen fontos tulajdonság az egészségügyi rendszereknél, ahol a kezelés gyakran idő-kritikus. Katasztrófahelyzetet jelenthet, amikor nem egészségügyi vonatkozású informatikai rendszerek megbénulnak, éppen akkor, amikor az érintett információkra az egészségügyi rendszernek a leginkább szüksége volna.

[2] vizsgálhatóság, ellenőrizhetőség, mérhetőség, minősíthetőség

Veszélyek az egészségügyi informatikai biztonságra nézve

Jelen részben sorra veszem azon eseményeket, állapotokat, melyek veszélyt jelenthetnek az egészségügyi informatikai rendszerekre. A legtöbb esetben konkrét nevet hordoz a probléma, de néha csak magát a jelenséget, eseményt írom le, egyfajta gyűjtőfogalomként.

Kezdjük az alapvető fogalmakkal. Az egészségügyi ellátást végző személyek rendszer-hozzáférési eljárásokat sértenek, amikor egymás autentikációs[3] adatait, rosszabb esetben egymás felhasználói profiljait használják a kijelentkezés-bejelentkezés vesződségének elkerülésére. A felelősségre vonást is ez nagyban megnehezíti. További gondokat okozhatnak a Masquerade szolgáltatók (ideértve a szerződött karbantartó személyzetet, a rendszer szoftvermérnökét, hardver javító személyzetet, akik lehet, hogy pro forma jogon hozzáférnek rendszerekhez és adatokhoz). Masquerade szolgáltatók szerződéses személyzet segítségével a kiváltságos hozzáférést igénylő rendszereknél (például a helyszíni vizsgálatok és berendezések üzemzavarának elhárítása során) illetéktelenek hozzáférhetnek az adatokhoz.

Mint ilyen, ez egy megsértése a biztonságos kiszervezési megállapodásoknak. Bár ritkább, de a bennfentesek is lehetnek forrása a súlyos szabályszegéseknek, amik veszélyeztetik a személyes egészségügyi adatok titkosságát. Léteznek még masquerade kívülállók (beleértve a hackerek-et is), akik kívülállók és masquerade esete akkor jelentkezik, ha illetéktelen harmadik fél hozzáfér a rendszer adatokhoz vagy erőforrásokhoz, akár felhatalmazott felhasználó megszemélyesítése módján. Az alábbi esetek a leggyakoribbak ezen területen:

- a felhasználó azonosítása;
- a felhasználói hitelesítést;
- a származási hitelesítés;
- beléptető és kiváltság irányítását.

Meglepően könnyű lehet hozzájutni jogosulatlanul egy egészségügyi információs rendszer hozzáféréséhez (például egy séta során egy felügyelet nélküli hagyott munkaállomás mellett).

Jogosult felhasználók is végezhetnek jogosulatlan műveleteket, mint rosszindulatú megváltoztatása az adatoknak. Kritikus fontosságú a helyesen azonosított ellátási témák, hogy az egészségügyi nyilvántartásokat vezető egészségügyi szervezetek részletes azonosító jellegű információkkal kezeljék betegeiket. Ezt azonosító adatok használatára való kötelezéssel érhetjük el. Általában véve, az egészségügyi információk jogosulatlan használata a következő esetekben lépnek életbe:

- munkacsoport beléptető hibás, jogtalan használata
- az elszámoltathatóság és pénzügyi ellenőrzés hibái esetén
- személyi biztonsági megsértése

Káros vagy romboló szoftverek bevezetésével (köztük a vírusok, férgek és egyéb "malware[4]" [2] programok) is érhetik a rendszert támadások. A legtöbb IT biztonsági esemény számítógépes vírusok által keletkezik. A káros és zavaró szoftverek rendszerint a vírusvédelm vagy a szoftver változás-frissítés rendszer működésének kudarcából adódik. A káros programok terjedésének megakadályozásának akadályai általában a védelmi rendszerek hatáskörein belül az e-mail férgek és vírusok működése és a szerver szoftverek hiányosságai. További gondot okozhat a rendszer erőforrásaival való visszaélés. Ez a fenyegetés magában a felhasználókkal él, jellemzően akkor, amikor az egészségügyi dolgozó nem rendeltetés-szerűen használja az egészségügyi informatikai rendszer eszközeit, adatbázisait, személyes adatait. Például munkaidő alatt az őt foglalkoztató szervezet számítógépein zenét, filmeket, videókat hallgat és néz, rosszabb esetben az egészségügyi adatbázisokat használja személyes célokra. Kommunikációs beszivárgással végrehajtott támadásról beszélünk, amikor a normál

[3] Autentikáció: egy adott személy, eljárás hitelesítése különböző adatok által.

[4] Rosszindulatú szoftverek, melyek zavarják vagy akadályozzák a működést eközben esetlegesen illegális adatgyűjtést folytatnak.

adatáramlás folyamába egy kívülálló személy vagy szervezet becsatlakozik. A leggyakoribb esemény egy denial-of-service[5] támadás, amelyben szervert vagy hálózati erőforrásokat

hatékonyan off-line állapotba taszítják. Más beszűrődési kommunikációs formák is lehetségesek (például visszajátszás támadás, amelyben egy érvényes, de out-of-date üzenetet újraadnak egy valamilyen módon, ami normálisnak tűnik. Kommunikációs beszűrődésnek minősül a behatolásjelző károsítása és / vagy a hálózati hozzáférés-vezérlés károsítása.

Kommunikációs lehallgatás az, amikor nem titkosított a csatorna az átvitel alatt, a bizalmas információkat igen könnyen lehallgathatják. Ez egyszerűbb, mint amilyennek hangzik, bárki a helyi hálózatban potenciálisan telepíthet egy úgynevezett "csomag szippantás" alkalmazást,ami nyomon követi a hálózati forgalmat a saját helyi hálózaton, beleértve az olvasott e-maileket is az átvitel során. Erre szolgáló hacker eszközök könnyen hozzáférhetőek, amik automatizálják és egyszerűsítik ezt a folyamatot. Kommunikációs lehallgatásnak minősülő hiba, ha egy rendszer nem biztosítja a biztonságos kommunikációt.

Utóbbi támadás kapcsán fordul elő leginkább a megtagadás, amely fenyegetés az, amikor a felhasználók tagadják, hogy küldtek egy üzenetet (elállás eredet) vagy kaptak egy üzenetet (elállás kézhezvétel). Megtagadás jelenthet az ellenőrző alkalmazások használatának elmulasztását, mint például a digitális aláírás az e-receptek esetében (például: eredetmegjelölés), vagy az e-mail üzenetek olvasási visszaigazolásainak elhagyását.

Eltérő gondot okozhat a csatlakozási hiba, ami a következő: minden hálózatnak van egy rendelkezésre állási szintje, amikor ez nem elégséges és nem teljesíti a kívánt szintet, csatlakozási hibát eredményezhet. Ezen hiba előidézhető a hálózati rendszereszközök – elsősorban forgalomirányítók – káros befolyásolásával, vagy az autentikációs eljárások megzavarásával. Eredménye, hogy a felhasználók kevésbé biztonságos rendszereken kénytelenek kommunikálni, ami könnyűvé teszi a lehallgatást. Kiterelésnek is szokták nevezni, a biztonságos hálózatból való kiterelés nyomán. Ezen állapot egyik kivitelezési módja, a rosszindulatú kódok beágyazása. Ez a fenyegetés magában foglalja az e-mail vírusokat és a rosszindulatú mobil kódokat. A vezeték nélküli és mobil technológiák egészségügyi szolgáltatók általi növekvő használata emeli ennek a fenyegetésnek a potenciálját. A rosszindulatú kód beágyazása eredményezheti az antivírus szoftver alkalmazásának elmulasztását vagy bénítását, vagy a behatolásvédelmi ellenőrzések elmaradását, vagy elégtelen működését.,

A hálózati hibák sorában az első, amit sorra veszünk a véletlen misrouting[6]. Ez a fenyegetés magában foglalja annak lehetőségét, hogy az információ egy hibás címre kerül kézbesítésre a hálózaton keresztül. Véletlen misrouting hiba adódhat a felhasználó oktatásának hiányából, vagy az integritás fönntartásának elmulasztásából. További ilyen területű gond a műszaki hiba a fogadó, tároló és hálózati infrastruktúrában. Ezen fenyegetések közé tartoznak hardverhibák, hálózati meghibásodások vagy adattároló létesítmények hibái. Sajnos egyáltalán nem egyedi az egészségügyi információs rendszereknél, hogy ezen hibáknak életveszélyes következményei vannak a betegek számára. További speciális hiba a környezetvédelmi támogatás hiánya (beleértve áramkimaradás és hálózati zavarok, szolgáltatásból származó természetes vagy ember által okozott katasztrófák). Egészségügyi információs rendszerek működése kritikus lehet a természeti katasztrófák közben és egyéb események ideje alatt. A megfelelő veszély-és kockázatértékelést az egészségügyi információk tartalmazzák. Annak felmérése, hogy természeti katasztrófák idején létfontosságúak-e az ilyen rendszerek működése elengedhetetlen.

Továbblépünk a szoftveres érintettségű hibákra. Az első értelemszerűen a rendszer vagy hálózati szoftver hiba. Denial-of-service támadásokat nagyban elősegítik ezen hiányosságok,

[5] Denial-of-service: informatikai szolgáltatás temporális használhatatlansága valamely ártó beavatkozás eredményeként.
[6] Téves irányítás

vagy a helytelen működésű operációs rendszer vagy hálózati operációs rendszer szoftver. A rendszer vagy hálózati szoftver hiba megelőzésének minősül a szoftver integritásának ellenőrzése, a rendszer tesztelése, illetve szoftver-karbantartásának ellenőrzése. Magyarországon sajnos roppant gyakori a szoftver hibás alkalmazása (pl. egy egészségügyi információs alkalmazás), amikor egy szoftvert nem a rendeltetésének vagy céljának megfelelő módon használunk. További gyakori gond az operátor hiba. Ez azon anomáliák összessége, mely az informatikai rendszer felhasználójának hibájából adódnak. Jellemzően az alábbi hiányosságokból adódhatnak: [3]

- műveletek ellenőrzései
- személyi biztonság (beleértve a hatékony képzés)
- a katasztrófa-elhárítás (beleértve az adatok biztonsági mentését és visszaállítását.)

További emberi mulasztásra visszavezethető probléma a karbantartási hiba. Minden olyan hiba, mely megelőzhető lett volna azon tevékenységek elvégzésével, amik az informatikai-rendszer karbantartására irányulnak és a karbantartási terv előír. Lehet ez szoftver oldali (például: frissítések elmulasztása) vagy hardwer oldali (hibás eszközök javításának vagy cseréjének elmulasztása)

Egyik leggyakoribb eset - az egész világ tekintetében is - a felhasználói hiba: Jelen anomália akkor állhat fenn, ha a felhasználó követ el hibát, például figyelmetlenségből rossz címzettnek küld bizalmas információkat. Felhasználói hibát eredményezhet:

- a felhasználói kezelőszervek rossz kialakítása
- személyi biztonság hiánya (hiányos képzés)

Speciális – e Magyarországon gyakori gond – a személyzet alacsony száma. A személyzet hiányból adódó fenyegetés lehetőségét tartalmazza, ha a kulcsfontosságú személyzet hiányos, vagy létszáma szűken szabott. E fenyegetés nagysága attól függ, hogy milyen mértékben küzdenek munkaerőhiánnyal az üzleti folyamatok. Az egészségügyi járvány nagymértékben növeli a keresletet a szakszemélyzetre.

Nagyon sötét terület a bennfentesek általi lopás (ideértve a berendezések vagy adatok eltulajdonítását). Bennfentesek általában jobban hozzáférnek a bizalmas információkhoz, mint a kívülállók, ezért kedvező helyzetben vannak, hogy ellopjanak információkat annak érdekében, hogy eladják vagy nyilvánosságra hozzák azt másoknak.

Egy fokkal kevésbé kellemetlen és szégyenteljes ügy a kívülállók általi lopás (ideértve a berendezések vagy adatok eltulajdonítását). Kívülállók általi adatok és berendezések eltulajdonítása egy komoly probléma egyes kórházakban. Sok ellenőrzés, beleértve a mobil számítástechnika ellenőrzések, biztonságos média szállítás, incidenskezelés, compliance[7] ellenőrzések vagy fizikai lopás elleni védelem segíthet megelőzni ezen eseményeket.

Jellemzően elégedetlen alkalmazottak követi kel a szándékos károkozás bennfentesek által nevű cselekményt. Akkor beszélhetünk ilyen eseményről, ha az alkalmazott személyzet szánt szándékkal károsítja a reá bízott, vagy használatra átadott eszközöket. Ez vonatkozik mind hardware, mind software eszközökre. Ennek is van külsős párja, a Szándékos károkozás külsősök által kategória. Akkor beszélhetünk ilyen eseményről, ha kívülálló személyek (nem a szolgáltató vagy annak megbízott alvállalkozóinak szerződéses munkavállalói) kárt okoznak azon rendszerekben vagy eszközökben, amelyekhez hozzáféréshez jutnak.

Kórházaknál, klinikáknál és egyéb egészségügyi szervezeteknél sokkal nehezebb megakadályozni, mint a legtöbb más működési környezetekben, elsősorban a nagyszámú rokonok, látogatók, barátok, járó betegek által generált embermennyiség miatt.

Sok magyarázatot nem kíván a terrorizmus által jelentett veszély. A terrorizmus fenyegetése, hogy szélsőséges csoportok szándékosan károsítják vagy megzavarják egészségügyi szervezetek munkáját vagy veszélyeztetik az egészségügyi szolgáltatók

[7] Szolgáltatás-készség

működését az egészségügyi információs rendszerek zavarása által. Az egészségügyi rendszerek tervezésénél komoly figyelmet kell fordítani a terrorizmus elleni védelemre, mert egyre komolyabb fenyegetést jelent. [4]

Mint az látható, elég száraz és nehézkes egy szabvány olvasata, értelmezése. Ennek ellenére igyekeztem minél inkább olvasó és felhasználóbaráttá tenni. A forma természetesen eltér a megszokott cikkek kinézetétől, de sajnos egy szabvány lényegében meghatározásokból áll, így azok formája erősen köti a lehetőségeket. Esetünkben a funkcionalitás elsőbbséget élvezett a külalaknál, remélem elnézi nekem a Tisztelt olvasó ezt a kompromisszumot.

ÖSSZEGZÉS

Jól látható, hogy elsősorban az emberi eredetű hiányosságokkal foglalkozik a szabvány eddigi része. Az egész világon nagy probléma, hogy a munkáját végző egészségügyi személyt nehéz rábírni a felelős adminisztrációs tevékenységre. Ennek érdekében olyan rendszereket kell kifejleszteni, amik nem teszik lehetővé a hanyagságot és minimalizálják a lehetséges hibákat.

Másik fontos terület, a fizikai környezet biztosítása. Hisz hiába érjük el, hogy mindenki tartsa be a biztonsági előírásokat, ha rendszerünk sebezhető és könnyen korrumpálható.

Az eddig taglalt ismeretek alapján ezen két fontos területen szükséges a mielőbbi előrelépés, hisz ezek alapokat képezhetnek egy további, magas színvonalú rendszer felépítéséhez.

Felhasznált irodalom

[1] Angol-Magyar Műszaki és tudományos szótár könyv és CD - Akadémiai Kiadó 1993.

[2] Webster's Encyclopedic Unabridged Dictionary of the English Language. – Gramercy Books, New Work/Avenel, 1996.

[3] Útmutató az IT biztonsági szintek meghatározásához BME IK, 2008

[4] Európai Bizottság, Zöld Könyv egy Kritikus Infrastruktúra Védelmi Európai Programról, COM(2005) 576, 2005. november 17. (Commission of the European Communities: Green Paper on a European Programme for Critical Infrastructure Protection, Brussels, 17.11.2005 COM(2005) 576 final

A cikk alapjául szolgáló szabvány:

Az ISO 27799:2008 szabvány angol nyelvű kiadása – ICS: 35.240.80 Első kiadás 1998.

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Baráth Artur
magicman@mail.duf.hu

AZ ISO 27799:2008 SZABVÁNY AZ INFORMATIKAI BIZTONSÁG KEZELÉSE AZ EGÉSZSÉGÜGYBEN

I. RÉSZ

Absztrakt

Az informatikai rendszerek biztonságos, hatékony, megbízható működéshez elengedhetetlen a vonatkozó törvényi rendelkezések és szakmai normák beható ismerete. Ezen tudás elsajátításához ad segítséget jelen munkám, amelyben, a címben szereplő szabvány részletes ismertetésének első része olvasható.

The knowledge of professional norms and related laws are indispensable for the safe, reliable and effective work of informatics systems.For acquiring this knowledge my work provides help, in which the first part of the detailed presentation of the title standard is readable.

Kulcsszavak: *egészségügy, informatika, biztonság, ISO 27799:2008, szabvány ~ healthcare, informatics, safety, ISO 27799:2008 standard*

BEVEZETÉS

Ezen cikk első darabja egy háromrészes cikksorozatnak, melyben az ISO 27799:2008 számú szabványt dolgozom fel annak érdekében, hogy segítsek azoknak, akik Magyarországon kívánnak a témában dolgozni vagy kutatni. A vizsgált szabvány az egészségügyi informatikai rendszerek egységesítését és minőségének javítását hivatott segíteni, azáltal, hogy pontosan deklarált és megszabott környezetet biztosít a működéshez.

Magyarországon a napokban lehetett hallani az országos egészségügyi rendszerek átfogó modernizációjáról, egységesítéséről, a köztük szükséges átjárhatóságok megvalósításáról. A törekvés üdvözlendő és természetesen megkésett, ennek ellenére bizakodásra ad okot, hogy foglalkoznak a témával.

Egy biztonságos és nemzetközi szinten is kompatibilis, elismert rendszer kialakításához elengedhetetlen a vonatkozó szabványok és jogszabályok ismerete. Magyarországon sajnos még igen kezdetleges állapotok uralkodnak az egészségügyi informatikai rendszerek biztonsága területén, amit rövid időn belül orvosolni kell, hisz a társadalom és az ország érdeke egy stabil, hatékony, biztonságos ellátórendszer létesítése. Ezen folyamat elindulásához nyújt fontos segítséget cikksorozatom.

AZ ISO 27799:2008 SZABVÁNY

Az ISO 27799:2008 nemzetközi szabvány az egészségügyi informatika működését támogató iránymutatásokat határoz meg. A szabvány meghatározza egy sor részletes ellenőrzés irányítását az egészségügyi információs biztonság vizsgálatára, és a legjobb gyakorlati iránymutatásokat. Megvalósításával az egészségügyi szervezeteknek és egyéb egészségügyi információk kezelőinek képes biztosítani a minimálisan szükséges biztonsági szintet, amely megfelel saját szervezeti körülményeik között, és amely fenntartja a személyes egészségügyi adatok bizalmasságának, sértetlenségének és rendelkezésre állásának körülményeit. A szabvány minden egészségügyi információ vonatkozik, függetlenül a tárolásra használt eszközöktől és függetlenül a továbbítási csatornától.

Az ISO 27799:2008 nemzetközi szabvány az ISO/IEC 27002 nemzetközi szabvánnyal együtt alkalmazandó, és együtt határozzák meg, mire van szükség a biztonságos tájékoztatáshoz az egészségügyi ellátásban.

A szabvány technológia-semleges, mert a biztonsági technológiák gyorsan fejlődnek, miközben a szabvány előírásai hosszú távon is érvényben maradnak.

A szabvány szakkifejezései és meghatározásai

Jelen szabvány alkalmazásában az alábbi fogalom-meghatározásokat kell alkalmazni:

Az egészségügyi informatika egy tudományág, amely érinti a kognitív, az információ-feldolgozó és a kommunikációs feladatait az egészségügyi gyakorlatnak, oktatás és kutatás, beleértve az információs tudomány és a technológia támogatását.

Ennek kiszolgálására szolgál az egészségügyi információs rendszer, ami lényegében egészségügyi ellátással kapcsolatos információk tárolása számítógéppel feldolgozható formában, feladata kezelni és biztonságosan tárolni az adatokat, továbbá hozzáférést biztosítani azokhoz jogosult felhasználónak. E kettő terület összehangolt munkája is kell az egészségügyi ellátás működéséhez, ami bármilyen típusú szolgáltatás szakemberek részéről, akár paraprofessionálisan[1] rendszerben is.

Az egészségügyi ellátás működését biztosítja az egészségügyi szervezet, ami általános kifejező leírása többféle típusú szervezetnek, amelyek az egészségügyi szolgáltatásokat

[1] Állapot, mikor a professzionális képzettség és tudás a személy birtokában van, viszont a cím és jogosultság nincs. Mindig supervisori felügyeletet kíván meg a működése.

biztosítják. Ezen szervezeteken belül végeznek munkát az egészségügyi szakemberek, akik jogosult személyek, melyek hivatalos testület által elismert minősítéssel végeznek bizonyos egészségügyi feladatokat. Az egészségügyi szolgáltató, ami bármely személy vagy szervezet, aki részt vesz a nyújtott vagy kapcsolódó egészségügyi szolgáltatásokban az ügyfél részére, vagy jóléti gondozó biztosítja a körülményeket a munkavégzéshez

A felelősségre vonhatóság érdekében definiálni kell többek között azonosítható személyt, aki az a személy, aki azonosítható, közvetlen vagy közvetett módon. Különösen egy azonosító szám vagy több egyedi tényező és a személy fizikai, fiziológiai, mentális, gazdasági, kulturális vagy társadalmi jellemzői alapján.

Személyes egészségügyi adatok: Tájékoztatás az azonosítható személy részére, amely kapcsolódik az egyén fizikai vagy mentális egészségi állapotához, továbbá azon egészségügyi szolgáltatások adatai, amiket az egyénnek nyújtottak. Ezen adatok az alábbiak lehetnek:

- a) tájékoztatás a nyilvántartásba vételről az egyén számára;
- b) információ a kifizetések vagy jogosultság az egészségügyi ellátás tekintetében az egyén részére;
- c) egy számot, szimbólumot vagy különleges egyedi jelet, mely azonosítja az egyes egészségügyi célokra;
- d) származó információi vizsgálatnak, egy testrésznek vagy testi anyagnak;
- e) azonosítása egy személy (pl. egy egészségügyi szakember), mint az egészségügyi szolgáltató, az egyén számára.

További meghatározandó fogalom az ellátás tárgya: ez, egy vagy több személy beütemezése fogadására, illetve egészségügyi szolgáltatás nyújtására. Eközben szükséges használni vagyontárgyakat, ami bármi lehet, ami értéket jelent a szervezet részére. Ezen szolgáltatások biztosítóját és tárgyak felhasználóját felelősségre vonhatóvá kell tenni, ami egy tulajdonság, amely biztosítja, hogy a végrehajtott intézkedések hatásai egyénekhez legyenek köthetőek a gazdálkodó egység vezetői által. Szorosan ide kapcsolódik a biztosíték, ami egy sor megfelelési folyamat eredményein keresztül a szervezet részéről megvalósítja a bizalom státuszát az információbiztonsági irányítás területén. Mindezek mellett elérhetőséget is biztosítani kell, ami azon tulajdonság, hogy hozzáférhető és használható igény által a felhatalmazott szervezet vagy személy által.

Az egészségügyi informatikai biztonság

Az egészségügyi informatikai biztonság célja a szabvány szerint, hogy fenntartsa az információk titkosságát, hozzáférhetőségének és épségének állapotát, beleértve a hitelesség, elszámoltathatóság és auditálhatóság2 [1] területét is.

Titoktartási intézkedéseket kell tenni, hogy fennmaradjon az adatok integritása, ha másért nem, hogy ne férjenek hozzá a vezérlési adatokhoz, ellenőrzési nyomvonalakhoz és a rendszer egyéb adataihoz, oly módon, hogy lehetővé teszik a titoktartás sérülését. Ezen túlmenően, a betegbiztonság függ a titoktartás fenntartásától, a személyes egészségügyi adatok integritásától, ezek sérülése eredményezhet betegséget, sérülést vagy akár halált.

Hasonlóképpen, a magas szintű rendelkezésre állás különösen fontos tulajdonság az egészségügyi rendszereknél, ahol a kezelés gyakran idő-kritikus. Katasztrófahelyzetet jelenthet, amikor nem egészségügyi vonatkozású informatikai rendszerek megbénulnak, éppen akkor, amikor az érintett információkra az egészségügyi rendszernek a leginkább szüksége volna.

[2] vizsgálhatóság, ellenőrizhetőség, mérhetőség, minősíthetőség

Veszélyek az egészségügyi informatikai biztonságra nézve

Jelen részben sorra veszem azon eseményeket, állapotokat, melyek veszélyt jelenthetnek az egészségügyi informatikai rendszerekre. A legtöbb esetben konkrét nevet hordoz a probléma, de néha csak magát a jelenséget, eseményt írom le, egyfajta gyűjtőfogalomként.

Kezdjük az alapvető fogalmakkal. Az egészségügyi ellátást végző személyek rendszer-hozzáférési eljárásokat sértenek, amikor egymás autentikációs[3] adatait, rosszabb esetben egymás felhasználói profiljait használják a kijelentkezés-bejelentkezés vesződségének elkerülésére. A felelősségre vonást is ez nagyban megnehezíti. További gondokat okozhatnak a Masquerade szolgáltatók (ideértve a szerződött karbantartó személyzetet, a rendszer szoftvermérnökét, hardver javító személyzetet, akik lehet, hogy pro forma jogon hozzáférnek rendszerekhez és adatokhoz). Masquerade szolgáltatók szerződéses személyzet segítségével a kiváltságos hozzáférést igénylő rendszereknél (például a helyszíni vizsgálatok és berendezések üzemzavarának elhárítása során) illetéktelenek hozzáférhetnek az adatokhoz.

Mint ilyen, ez egy megsértése a biztonságos kiszervezési megállapodásoknak. Bár ritkább, de a bennfentesek is lehetnek forrása a súlyos szabályszegéseknek, amik veszélyeztetik a személyes egészségügyi adatok titkosságát. Léteznek még masquerade kívülállók (beleértve a hackerek-et is), akik kívülállók és masquerade esete akkor jelentkezik, ha illetéktelen harmadik fél hozzáfér a rendszer adatokhoz vagy erőforrásokhoz, akár felhatalmazott felhasználó megszemélyesítése módján. Az alábbi esetek a leggyakoribbak ezen területen:

- a felhasználó azonosítása;
- a felhasználói hitelesítést;
- a származási hitelesítés;
- beléptető és kiváltság irányítását.

Meglepően könnyű lehet hozzájutni jogosulatlanul egy egészségügyi információs rendszer hozzáféréséhez (például egy séta során egy felügyelet nélküli hagyott munkaállomás mellett).

Jogosult felhasználók is végezhetnek jogosulatlan műveleteket, mint rosszindulatú megváltoztatása az adatoknak. Kritikus fontosságú a helyesen azonosított ellátási témák, hogy az egészségügyi nyilvántartásokat vezető egészségügyi szervezetek részletes azonosító jellegű információkkal kezeljék betegeiket. Ezt azonosító adatok használatára való kötelezéssel érhetjük el. Általában véve, az egészségügyi információk jogosulatlan használata a következő esetekben lépnek életbe:

- munkacsoport beléptető hibás, jogtalan használata
- az elszámoltathatóság és pénzügyi ellenőrzés hibái esetén
- személyi biztonsági megsértése

Káros vagy romboló szoftverek bevezetésével (köztük a vírusok, férgek és egyéb "malware[4]" [2] programok) is érhetik a rendszert támadások. A legtöbb IT biztonsági esemény számítógépes vírusok által keletkezik. A káros és zavaró szoftverek rendszerint a vírusvédelm vagy a szoftver változás-frissítés rendszer működésének kudarcából adódik. A káros programok terjedésének megakadályozásának akadályai általában a védelmi rendszerek hatáskörein belül az e-mail férgek és vírusok működése és a szerver szoftverek hiányosságai. További gondot okozhat a rendszer erőforrásaival való visszaélés. Ez a fenyegetés magában a felhasználókkal él, jellemzően akkor, amikor az egészségügyi dolgozó nem rendeltetés-szerűen használja az egészségügyi informatikai rendszer eszközeit, adatbázisait, személyes adatait. Például munkaidő alatt az őt foglalkoztató szervezet számítógépein zenét, filmeket, videókat hallgat és néz, rosszabb esetben az egészségügyi adatbázisokat használja személyes célokra. Kommunikációs beszivárgással végrehajtott támadásról beszélünk, amikor a normál

[3] Autentikáció: egy adott személy, eljárás hitelesítése különböző adatok által.

[4] Rosszindulatú szoftverek, melyek zavarják vagy akadályozzák a működést eközben esetlegesen illegális adatgyűjtést folytatnak.

adatáramlás folyamába egy kívülálló személy vagy szervezet becsatlakozik. A leggyakoribb esemény egy denial-of-service[5] támadás, amelyben szervert vagy hálózati erőforrásokat

hatékonyan off-line állapotba taszítják. Más beszűrődési kommunikációs formák is lehetségesek (például visszajátszás támadás, amelyben egy érvényes, de out-of-date üzenetet újraadnak egy valamilyen módon, ami normálisnak tűnik. Kommunikációs beszűrődésnek minősül a behatolásjelző károsítása és / vagy a hálózati hozzáférés-vezérlés károsítása.

Kommunikációs lehallgatás az, amikor nem titkosított a csatorna az átvitel alatt, a bizalmas információkat igen könnyen lehallgathatják. Ez egyszerűbb, mint amilyennek hangzik, bárki a helyi hálózatban potenciálisan telepíthet egy úgynevezett "csomag szippantás" alkalmazást,ami nyomon követi a hálózati forgalmat a saját helyi hálózaton, beleértve az olvasott e-maileket is az átvitel során. Erre szolgáló hacker eszközök könnyen hozzáférhetőek, amik automatizálják és egyszerűsítik ezt a folyamatot. Kommunikációs lehallgatásnak minősülő hiba, ha egy rendszer nem biztosítja a biztonságos kommunikációt.

Utóbbi támadás kapcsán fordul elő leginkább a megtagadás, amely fenyegetés az, amikor a felhasználók tagadják, hogy küldtek egy üzenetet (elállás eredet) vagy kaptak egy üzenetet (elállás kézhezvétel). Megtagadás jelenthet az ellenőrző alkalmazások használatának elmulasztását, mint például a digitális aláírás az e-receptek esetében (például: eredetmegjelölés), vagy az e-mail üzenetek olvasási visszaigazolásainak elhagyását.

Eltérő gondot okozhat a csatlakozási hiba, ami a következő: minden hálózatnak van egy rendelkezésre állási szintje, amikor ez nem elégséges és nem teljesíti a kívánt szintet, csatlakozási hibát eredményezhet. Ezen hiba előidézhető a hálózati rendszereszközök – elsősorban forgalomirányítók – káros befolyásolásával, vagy az autentikációs eljárások megzavarásával. Eredménye, hogy a felhasználók kevésbé biztonságos rendszereken kénytelenek kommunikálni, ami könnyűvé teszi a lehallgatást. Kiterelésnek is szokták nevezni, a biztonságos hálózatból való kiterelés nyomán. Ezen állapot egyik kivitelezési módja, a rosszindulatú kódok beágyazása. Ez a fenyegetés magában foglalja az e-mail vírusokat és a rosszindulatú mobil kódokat. A vezeték nélküli és mobil technológiák egészségügyi szolgáltatók általi növekvő használata emeli ennek a fenyegetésnek a potenciálját. A rosszindulatú kód beágyazása eredményezheti az antivírus szoftver alkalmazásának elmulasztását vagy bénítását, vagy a behatolásvédelmi ellenőrzések elmaradását, vagy elégtelen működését.,

A hálózati hibák sorában az első, amit sorra veszünk a véletlen misrouting[6]. Ez a fenyegetés magában foglalja annak lehetőségét, hogy az információ egy hibás címre kerül kézbesítésre a hálózaton keresztül. Véletlen misrouting hiba adódhat a felhasználó oktatásának hiányából, vagy az integritás fönntartásának elmulasztásából. További ilyen területű gond a műszaki hiba a fogadó, tároló és hálózati infrastruktúrában. Ezen fenyegetések közé tartoznak hardverhibák, hálózati meghibásodások vagy adattároló létesítmények hibái. Sajnos egyáltalán nem egyedi az egészségügyi információs rendszereknél, hogy ezen hibáknak életveszélyes következményei vannak a betegek számára. További speciális hiba a környezetvédelmi támogatás hiánya (beleértve áramkimaradás és hálózati zavarok, szolgáltatásból származó természetes vagy ember által okozott katasztrófák). Egészségügyi információs rendszerek működése kritikus lehet a természeti katasztrófák közben és egyéb események ideje alatt. A megfelelő veszély-és kockázatértékelést az egészségügyi információk tartalmazzák. Annak felmérése, hogy természeti katasztrófák idején létfontosságúak-e az ilyen rendszerek működése elengedhetetlen.

Továbblépünk a szoftveres érintettségű hibákra. Az első értelemszerűen a rendszer vagy hálózati szoftver hiba. Denial-of-service támadásokat nagyban elősegítik ezen hiányosságok,

[5] Denial-of-service: informatikai szolgáltatás temporális használhatatlansága valamely ártó beavatkozás eredményeként.
[6] Téves irányítás

vagy a helytelen működésű operációs rendszer vagy hálózati operációs rendszer szoftver. A rendszer vagy hálózati szoftver hiba megelőzésének minősül a szoftver integritásának ellenőrzése, a rendszer tesztelése, illetve szoftver-karbantartásának ellenőrzése. Magyarországon sajnos roppant gyakori a szoftver hibás alkalmazása (pl. egy egészségügyi információs alkalmazás), amikor egy szoftvert nem a rendeltetésének vagy céljának megfelelő módon használunk. További gyakori gond az operátor hiba. Ez azon anomáliák összessége, mely az informatikai rendszer felhasználójának hibájából adódnak. Jellemzően az alábbi hiányosságokból adódhatnak: [3]

- műveletek ellenőrzései
- személyi biztonság (beleértve a hatékony képzés)
- a katasztrófa-elhárítás (beleértve az adatok biztonsági mentését és visszaállítását.)

További emberi mulasztásra visszavezethető probléma a karbantartási hiba. Minden olyan hiba, mely megelőzhető lett volna azon tevékenységek elvégzésével, amik az informatikai-rendszer karbantartására irányulnak és a karbantartási terv előír. Lehet ez szoftver oldali (például: frissítések elmulasztása) vagy hardwer oldali (hibás eszközök javításának vagy cseréjének elmulasztása)

Egyik leggyakoribb eset - az egész világ tekintetében is - a felhasználói hiba: Jelen anomália akkor állhat fenn, ha a felhasználó követ el hibát, például figyelmetlenségből rossz címzettnek küld bizalmas információkat. Felhasználói hibát eredményezhet:

- a felhasználói kezelőszervek rossz kialakítása
- személyi biztonság hiánya (hiányos képzés)

Speciális – e Magyarországon gyakori gond – a személyzet alacsony száma. A személyzet hiányból adódó fenyegetés lehetőségét tartalmazza, ha a kulcsfontosságú személyzet hiányos, vagy létszáma szűken szabott. E fenyegetés nagysága attól függ, hogy milyen mértékben küzdenek munkaerőhiánnyal az üzleti folyamatok. Az egészségügyi járvány nagymértékben növeli a keresletet a szakszemélyzetre.

Nagyon sötét terület a bennfentesek általi lopás (ideértve a berendezések vagy adatok eltulajdonítását). Bennfentesek általában jobban hozzáférnek a bizalmas információkhoz, mint a kívülállók, ezért kedvező helyzetben vannak, hogy ellopjanak információkat annak érdekében, hogy eladják vagy nyilvánosságra hozzák azt másoknak.

Egy fokkal kevésbé kellemetlen és szégyenteljes ügy a kívülállók általi lopás (ideértve a berendezések vagy adatok eltulajdonítását). Kívülállók általi adatok és berendezések eltulajdonítása egy komoly probléma egyes kórházakban. Sok ellenőrzés, beleértve a mobil számítástechnika ellenőrzések, biztonságos média szállítás, incidenskezelés, compliance[7] ellenőrzések vagy fizikai lopás elleni védelem segíthet megelőzni ezen eseményeket.

Jellemzően elégedetlen alkalmazottak követi kel a szándékos károkozás bennfentesek által nevű cselekményt. Akkor beszélhetünk ilyen eseményről, ha az alkalmazott személyzet szánt szándékkal károsítja a reá bízott, vagy használatra átadott eszközöket. Ez vonatkozik mind hardware, mind software eszközökre. Ennek is van külsős párja, a Szándékos károkozás külsősök által kategória. Akkor beszélhetünk ilyen eseményről, ha kívülálló személyek (nem a szolgáltató vagy annak megbízott alvállalkozóinak szerződéses munkavállalói) kárt okoznak azon rendszerekben vagy eszközökben, amelyekhez hozzáféréshez jutnak.

Kórházaknál, klinikáknál és egyéb egészségügyi szervezeteknél sokkal nehezebb megakadályozni, mint a legtöbb más működési környezetekben, elsősorban a nagyszámú rokonok, látogatók, barátok, járó betegek által generált embermennyiség miatt.

Sok magyarázatot nem kíván a terrorizmus által jelentett veszély. A terrorizmus fenyegetése, hogy szélsőséges csoportok szándékosan károsítják vagy megzavarják egészségügyi szervezetek munkáját vagy veszélyeztetik az egészségügyi szolgáltatók

[7] Szolgáltatás-készség

működését az egészségügyi információs rendszerek zavarása által. Az egészségügyi rendszerek tervezésénél komoly figyelmet kell fordítani a terrorizmus elleni védelemre, mert egyre komolyabb fenyegetést jelent. [4]

Mint az látható, elég száraz és nehézkes egy szabvány olvasata, értelmezése. Ennek ellenére igyekeztem minél inkább olvasó és felhasználóbaráttá tenni. A forma természetesen eltér a megszokott cikkek kinézetétől, de sajnos egy szabvány lényegében meghatározásokból áll, így azok formája erősen köti a lehetőségeket. Esetünkben a funkcionalitás elsőbbséget élvezett a külalaknál, remélem elnézi nekem a Tisztelt olvasó ezt a kompromisszumot.

ÖSSZEGZÉS

Jól látható, hogy elsősorban az emberi eredetű hiányosságokkal foglalkozik a szabvány eddigi része. Az egész világon nagy probléma, hogy a munkáját végző egészségügyi személyt nehéz rábírni a felelős adminisztrációs tevékenységre. Ennek érdekében olyan rendszereket kell kifejleszteni, amik nem teszik lehetővé a hanyagságot és minimalizálják a lehetséges hibákat.

Másik fontos terület, a fizikai környezet biztosítása. Hisz hiába érjük el, hogy mindenki tartsa be a biztonsági előírásokat, ha rendszerünk sebezhető és könnyen korrumpálható.

Az eddig taglalt ismeretek alapján ezen két fontos területen szükséges a mielőbbi előrelépés, hisz ezek alapokat képezhetnek egy további, magas színvonalú rendszer felépítéséhez.

Felhasznált irodalom

[1] Angol-Magyar Műszaki és tudományos szótár könyv és CD - Akadémiai Kiadó 1993.

[2] Webster's Encyclopedic Unabridged Dictionary of the English Language. – Gramercy Books, New Work/Avenel, 1996.

[3] Útmutató az IT biztonsági szintek meghatározásához BME IK, 2008

[4] Európai Bizottság, Zöld Könyv egy Kritikus Infrastruktúra Védelmi Európai Programról, COM(2005) 576, 2005. november 17. (Commission of the European Communities: Green Paper on a European Programme for Critical Infrastructure Protection, Brussels, 17.11.2005 COM(2005) 576 final

A cikk alapjául szolgáló szabvány:

Az ISO 27799:2008 szabvány angol nyelvű kiadása – ICS: 35.240.80 Első kiadás 1998.

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Berki Gábor
berkigabor@t-online.hu

A KIBERTÉRI KONFLIKTUSOK VÁLTOZÁSAI

Absztrakt

Az utóbbi néhány évben egyre több hírt hallunk számítógép-hálózati támadásokról. A célpontok között szerepelnek nemzetközi nagyvállalatok, kormányzati szervek, pénzügyi vállalatok és kritikus infrastruktúrák is. A támadók bevallott céljai nagyon különbözőek, a kíváncsiságtól, az anyagi haszonszerzésen át a politikai, vallási célok eléréséig. Ha azonban összességében tekintünk ezekre az eseményekre, megláthatjuk azokat a tendenciákat, amelyek világunkat fenyegetik, ha nem teszünk megfelelő lépéseket a védekezésre.

In recent years there have been growing reports of attacks on computer network. Targets include international corporations, government agencies, financial firms and critical infrastucture. The attackers' declared goals range from simple cuoriousity through to financial gain and political and religious aims. Unless adequate protective measures are put in place, such developments will continue to threaten today's world.

Kulcsszavak: *kiberhadviselés, hackerek, rosszindulatú programok, információbiztonság, folyamatirányítás ~ cyberwar, hackers, malewares, information security, process controll*

BEVEZETÉS

Az Internet elterjedésével egyszerűbbé vált az élet, a hivatalos ügyintézésektől kezdve, a banki átutalásokon át a webes vásárlások lebonyolításáig. Ám a számítógép-hálózatokkal átszőtt világunk sosem volt olyan sebezhető, mint napjainkban. Ez a sebezhetőség a bonyolult technikai, infokommunikációs rendszerektől való függésnek, illetve az egymással összekapcsolódó létfontosságú infrastruktúráknak köszönhető. A telekommunikációs hálózatok, energiaszállítási útvonalak, vízutánpótlási rendszerek, szállítási hálózatok, banki és pénzügyi szolgáltatások, állami szolgáltatások és vészhelyzeti szolgáltatások működésképtelenné tételének lehetősége komoly fenyegetést jelent. [1] Az ártó szándékú támadók kihasználva a sebezhetőségeket, a saját céljaik – legyen az ideológiai, vallási vagy pénzszerzési - elérése érdekében korlátozni, bénítani igyekeznek az információs társadalom részegységeinek működését. A nagy sajtóvisszhangot kiváltó támadások azonban csak a jéghegy csúcsát jelentik, véleményem szerint a háttérben igen intenzív felderítő munkát végeznek bizonyos csoportok, országok, hogy a jövőben esetleg kialakuló konfliktusok során előnyös pozícióból tudják támadni az ellenfél informatikai, folyamatirányító rendszereit, kritikus infrastruktúráit. Az alábbiakban – a nagyobb kibertámadások mellett - az erre utaló tevékenységeket is bemutatom. A közelmúltban nagy visszhangot kiváltó Stuxnet és a magyar CrySyS labor által felfedezett Duqu, Flamer és egyéb, a közelmúltban detektált vírusok bemutatásával rávilágítok a célzott informatikai támadások lehetőségeire. Az Anonymous hackercsoport kampányszerű támadásaiban is megpróbálok logikus rendszert találni.

AZ ELSŐ INFORMATIKAI TÁMADÁSOK

Habár a szakirodalom szerint a legelső dokumentált kibertámadást 1997-ben egy sri lanka-i terrorszervezet, a tamil tigrisek követték el, úgy gondolom, nem mehetünk el szó nélkül az 1982-es szibériai gázvezeték-robbanás mellett sem. Thomas C. Reed, az amerikai Nemzetbiztonsági Hivatal egykori munkatársa 2004-ben megjelent könyvében[1] leírja, hogy a robbanás nem a véletlen műve volt, hanem a szovjetek elleni gazdasági hadviselés része. A Szovjetunió megpróbált embargós nyugati technológiához jutni, az Egyesült Államok viszont meg akarta akadályozni, hogy a szovjetek valutabevételhez jussanak a nyersanyagszállításokból. [2]

Egy, a KGB-be beépült ügynök juttatta el a CIA-hoz azt a listát, amelyen a szovjetek által beszerezni kívánt technológia szerepelt. Ezen találták azt a bizonyos szoftvert, amelyet a nyersanyagvezetékek irányítási rendszereihez használtak volna. Egy kanadai vállalaton keresztül a CIA adta el a szovjeteknek a szoftvert, amelybe azonban olyan hibákat építettek, hogy néhány hónapos kifogástalan működés után összezavarta a szállítási folyamatokat. Ezt a vezeték irányítószelepeinek precízen megtervezett fals működtetésével érték el. Ennek eredménye volt az eddigi legnagyobb, nem nukleáris eredetű robbanás, amely a szovjet gazdaságot is megrázta 1982 nyarán.

Ez az emberéletet nem követelő, de hatalmas kárt okozó robbanás indította el a hidegháború utolsó felvonását - állítja a könyv szerzője. Mert noha a szovjetek rájöttek, hogy manipulált technológiát vettek, innentől kezdve nem bízhattak meg egyetlen beszállítójukban sem.[3]

Ez az akció előrevetítette a számítógép vezérelte rendszerek sebezhetőségét is.

1999-ben szerb hackerek – a NATO szerbiai bombázásaira válaszul - támadták meg a szövetség szervereit és néhányat DDoS2 módszerrel tettek átmenetileg elérhetetlenné, valamint feltörtek néhány weboldalt és propaganda üzeneteket helyeztek el rajtuk.

---

[1] At the Abyss: An Insider's History of the Cold War New York 2004. ISBN 0-89141-821-0

[2] Distributed Denial of Service – elosztott szolgáltatás-megtagadással járó támadás

A 2000-es évek elején kezdődtek azok a támadások, amelyek célja nem a károkozás vagy a figyelemfelkeltés, hanem az amerikai ipari és katonai infrastruktúra feltérképezése volt. A támadásokat orosz illetve kínai számítógépekre vezették vissza, de ezen országok vezetői hevesen tagadták, hogy kormányaiknak bármi közük is lenne hozzájuk. A leghíresebb támadássorozat a Titan Rain fedőnevet kapta és egyértelműen Kínához volt kapcsolható.[4] A legkülönbözőbb célpontok támadása során a védelmi rendszerek hatékonyságát és működését tesztelték. Természetesen nem tudható, hogy ezek a támadások milyen eredménnyel jártak, de nem járunk messze a valóságtól, ha azt feltételezzük, hogy a támadók igen pontos információkkal rendelkeznek ezen rendszerekről és egy komolyabb konfliktusban nagyszerűen ki tudnák használni a feltérképezett hibákat és komoly csapást tudnának mérni célpontjaikra.

Az első kibertámadás, amelyet egy ország ellen indítottak, 2007-ben következett be. Az igen fejlett informatikai kultúrával rendelkező Észtországban 2007. április 27-én zavargások törtek ki a tallinni szovjet hősi emlékmű eltávolítása miatt. Az első túlterheléses támadások jelei néhány nappal az első tüntetések után jelentkeztek a parlament, kormányhivatalok, minisztériumok, bankok, telefontársaságok és médiacégek szerverei ellen. A célpontok kiválasztása, a támadások összehangoltsága, precíz kivitelezése és hatékonysága arra mutatott, hogy e támadások hátterében szervezett erők állnak. Néhány esetben szakértők megállapították, hogy a támadások orosz szerverektől indultak, amit az orosz hatóságok természetesen tagadtak. Ugyanakkor a megtámadott szerverek jellegéből adódóan nyilvánvaló, hogy a támadások célja egyértelműen a balti állam kritikus információs infrastruktúrájának bénítása volt. Az ország online adatforgalmát irányító kulcsfontosságú szerverek naponta omlottak össze, sok állami intézmény hálózatát kénytelenek voltak ideiglenesen leválasztani az internetről. Az elektronikus banki forgalom és kereskedelem részint megszűnt, részint erősen akadozott. Egyes szakértők szerint a kibertámadás sokkal súlyosabb gazdasági károkat okozott Észtországnak, mint amit azok a kereskedelmi szankciók okoztak volna, amikkel Oroszország a krízis első heteiben fenyegetőzött.

Bár kezdetben NATO-szakértők is részt vettek a támadások felderítésében, azok jellegéből adódóan a támadók azonosítása szinte lehetetlen volt. Számos támadót lehetett ugyan azonosítani orosz területen, de annak egyértelmű igazolása, hogy kormányzati szerverek voltak, sikertelennek bizonyult. Általánosan elterjedt nézet szerint orosz hazafias érzelmű hackerek olyan botnet hálózatot hoztak létre, amelybe orosz gépeken kívül számos más ország területén lévő számítógépeket is beszerveztek a tudtuk nélkül (zombi gépek), és ezeken keresztül hajtották végre a támadásokat.[2]

A 2008 augusztusában kitört orosz-grúz háborúnak is volt kiber aspektusa. Mint az köztudott, a hosszú évek óta tartó grúz-oszét és a grúz-abház konfliktust a grúz elnök 2008. augusztus 8-án katonai úton próbálta megoldani az említett területek megtámadásával. Rosszul mérte fel azonban az erőviszonyokat, amikor nem számolt azzal, hogy Oroszország nem fogja szó nélkül hagyni a támadást, már csak azért sem, mivel csapatai ENSZ felhatalmazással békefenntartó missziót teljesítettek Dél-Oszétiában. Az orosz csapatok erőteljes válaszcsapásokat mértek a grúz erőkre és öt napig tartó heves harcok után a grúzok kénytelenek voltak fegyverszünetet kérni.[5]

A fegyveres konfliktussal egy időben megindult Grúzia ellen egy kiber hadjárat is. Az internet-forgalmat ellenőrzése alá vonta Oroszország - vagy legalábbis valakik Oroszországból, állította a grúz kormány, amely valóságos kiber-emigrációba kényszerült, és a hadi jelentések mellett sorra jelentette meg a virtuális támadásokról szóló közleményeit.3

A leglátványosabb hacker-akciók ugyanis az ország kormányzati weboldalai ellen indultak, amelyeket kívülről megbénítottak, illetve a tartalmukat kicserélték4. Az orosz földről érkezett

[3] http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html
[4] Ezt nevezi az internetes szaknyelv defacementnek

hackerek Mihail Szakasvili elnök portréjával vandálkodtak. Az államfő képére Hitler-bajuszt rajzoltak, és egy sor olyan képet tettek ki róla az oldalra, ahol a náci diktátor pózaiban ábrázolták, vagy a történelem nagy gonosztevői közé kopírozták be az arcmását.

A megtámadott oldalak között volt az elnök saját weblapja mellett a grúz külügy- és hadügyminisztérium is. Szakasvili elnök erre válaszul a hazája ügyét nyíltan támogató Lengyelország vezetőjétől kért és kapott segítséget: az államfő, illetve stábja Lech Kaczynski hivatalos, angol nyelvű oldalán is lehetőséget kapott arra, hogy tájékoztatást adjon a háborús eseményekről. Még ezt a hivatalos, nagyban gesztusértékű lépést megelőzően a honlap nélkül maradt grúz külügyminisztérium blogot indított a Google által birtokolt Blogspot blogszolgáltatónál.

Mindezekkel egy időben megindultak az ország lejáratását célzó, dezinformációs céllal indított weboldalak is - a hiteles forrásokat a konfliktusról percről percre-bontásban beszámoló blog a linkek között listázta. A kaukázusi országban a .ru végződésű webcímek is elérhetetlenné váltak, amelyeket egyes források szerint maga a grúz kormányzat tilttatott le, hogy útját állja az orosz propagandának, és a Tbilisziben lévő orosz nagykövetség munkatársai szerint a mobil- és vezetékes telefonszolgáltatásban is fennakadások voltak a túlterhelés miatt (igaz, ennek inkább a katonai offenzívához lehetett köze). [6]

Véleményem szerint a grúz kormány erősen eltúlozta az ellene indított kiber támadásokat, hisz korántsem rendelkezett olyan infrastruktúrával, mint például Észtország, így a támadásoknak sem volt olyan hatása, nem bénult meg a bankrendszer, illetve a kormányzat. Az interneten keresztül zajló nagyszabású támadások akkor különösen hatékonyak, ha egy olyan ország ellen irányulnak, amely erőteljesen támaszkodik információs technológiára és annak infrastruktúrájára. Grúzia esetében ez nem mondható el: az interneten keresztül a támadók nem tudtak nagyobb károkat okozni, mint az ország földjére lépő orosz katonák. Hétköznapi ésszel érthetetlen, hogy a kormány miért foglalkozott olyan erőteljesen a kiber-támadásokkal, miközben városait, infrastruktúráját lőtte és bombázta az orosz hadsereg.

Mind az orosz-észt, mind az orosz-grúz konfliktus vonatkozásában elmondhatjuk, az orosz hivatalos szervek kategorikusan tagadták, hogy közük lenne a támadásokhoz. A konfliktusok lezárulta utáni elemzések csupán azt tudták kimutatni, hogy orosz nacionalista érzések vezérelték a támadókat, ám az orosz állam közreműködését nem sikerült bebizonyítani.

A ROSSZINDULATÚ PROGRAMOK ÚJ GENERÁCIÓJA

Az első vírusokat még a 70-es években készítették, a világ legelső ismert vírusa a Creeper volt amely a Tenex operációs rendszert használó számítógépek hálózatán terjedt. A Creeper kiirtására hozták létre a Reaper nevű programot, ez az első ismert vírusirtó.[7] A "számítógépes vírus" kifejezést először a neves elméleti víruskutató Fred Cohen használta 1983-ban egy tudományos munkában. Az első kifejezetten PC-re írt vírus 1986 januárjában tűnt fel. A floppy lemezen terjedő Brain nem okozott semmi kárt, de ezzel elindult az a folyamat ami, még napjainkban is mérgezi az informatika világát.

A vírusokkal, férgekkel és egyéb rosszindulatú programokkal folytatott több évtizedes harc azonban új, jelentős mérföldkőhöz érkezett 2010 júniusában, amikor a fehérorosz VirusBlokAda cég felfedezett egy új férget, amelyet Stuxnetnek neveztek el.

Az új féreg Microsoft operációs rendszereken terjed és kizárólag ipari folyamatirányító rendszerek ellen lett kifejlesztve. A Stuxnet kivételes mivoltát és specializáltságát erősíti az a tény is, hogy az említett ipari felügyeleti, vezérlő és adatgyűjtő rendszereket egyetlen cég a *német Siemens gyártja (SIMATIC WinCC HMI és WIMATIC STEP 7)* és alapvetően a nehézipari szektorban, illetve az energiatermelés és szállítás területén használják, azaz

fenyegetést alapvetően csak olyan létesítményekre jelent, melyek egy része kritikus infrastruktúrának minősül.[8]

A Stuxnet végső célja ipari vezérlő rendszerek automatikus folyamatainak újraprogramozása volt. Elsősorban PLC[5] szoftvereket támadja. A WinCC/Step 7 szoftver volt mindezek közül az elsődleges, amelyet a Stuxnet megcélzott. Ez a szoftver adatkábelen keresztül kapcsolódik a PLC-hez és eléri a memória tartalmat, képes folyamatokat újrakonfigurálni, programokat feltölteni és a végrehajtás során rendelkezik bizonyos nyomkövetési funkciókkal is. Ha a PLC már programozásra került, akkor lekapcsolható róla, és a PLC már önmagában is képes a működésre. A Stuxnet e szoftver segítségével juttatta be kódblokkjait a PLC-be, majd ezeket el is rejtette. [10]

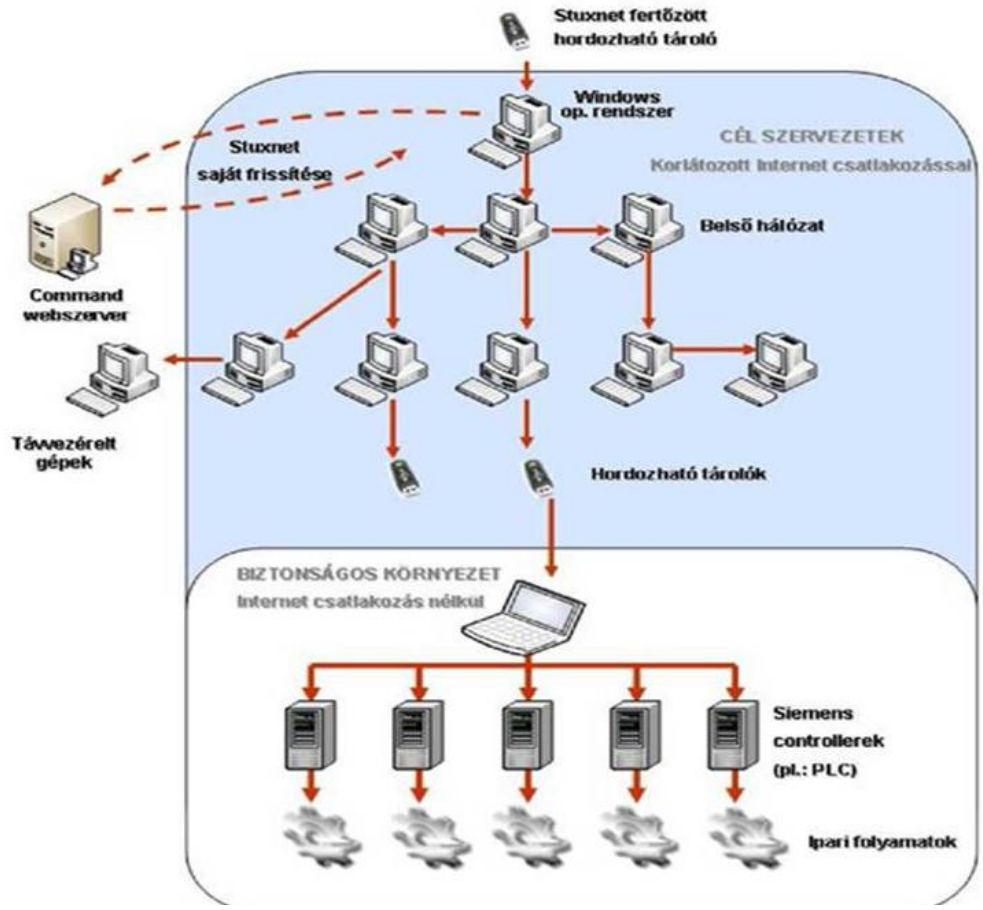
A Stuxnet a PLC-ken bizonyos konkrét ipari eszközök, nevezetesen nagy sebességű motorok frekvencia átalakítói után kutat és csak akkor lép akcióba, ha a finn Vacon és az iráni Fararo Paya készülékeire talál, valamint a felügyelt eszköz 807 és 1210 Hz között működik. Ilyen frekvencia átalakítók és motorok szinte kizárólag az iráni urándúsítókban használatosak.[10]

A vírus egyértelmű célja az urándúsító centrifugák észrevétlen tönkretétele és a dúsítási folyamat megzavarása volt. Ezt a célt sikeresen el is érte, hisz legalább 1000 centrifugát tett használhatatlanná a Natanzban lévő dúsítóban és mértékadó vélekedések szerint legalább két évvel vetette vissza az iráni atomprogramot.

A támadó kód megírásának profizmusára utal, hogy egyszerre négy zero-day[6] fenyegetést is kihasznált a terjedéséhez és két lopott digitális aláírással is tudta igazolni legitimitását. Terjedését az alábbi ábra mutatja be.

[5] A PLC - Programmable Logic Controller, azaz programozható logikai vezérlő. PLC-ket nagy számban az ipari szabályozástechnikában, a különböző villamos, illetve az ilyen módon működtetett folyamatok irányításában használják.

[6] A *zero-day/zero-hour*, vagyis *nulladik napi támadás* kifejezést azokra a számítógépes biztonsági fenyegetésekre használják a szakemberek, amelyek egy adott számítógépes alkalmazás még felfedezetlen, nem publikált sebezhetőségét használják ki. A támadó a sebezhetőség felfedezését követően úgynevezett *zero-day exploit*ot készít, amely az a tényleges számítógépes kód, ami képes a sérülékenység kiaknázására. Azonban a sérülékenységek nehéz és bonyolult detektálhatósága miatt a kártékony programok készítői számára jelentős értéket képvisel egy újonnan felfedezett sérülékenység, ezért egy program általában csak egy sérülékenység kihasználására épül. Ezen támadások idején a megtámadott alkalmazás fejlesztőjének még többnyire nincs tudomása a sérülékenységről, vagy még nem tudott javítást készíteni hozzá.



1. ábra. A Stuxnet terjedése a belső hálózaton [9]

Származásáról nincsenek pontos adatok, de mindenki rögtön az Egyesült Államokra és Izraelre gondolt, mint olyan országokra, amelyeknek érdekében és módjában is állhatott az iráni atomprogram elleni akció. Ralph Langner hamburgi vírusbiztonsági szakértő blogjában mélyrehatóan foglalkozott a Stuxnettel és a 2010. december 31-i bejegyzésében az alábbiakat írta:

„Egy ilyen nagy horderejű támadás mögött feszülő hatalmas erőket elég könnyű érzékelni. A Stuxnet kártevő kifejlesztéséhez extrém mennyiségű hírszerzési adat kellett a dúsító mű elrendezéséről teljesen meg kellett érteni az IR-1[7] *működését (amihez feltehetően rendelkezésre állt egy üzemképes tesztelő rendszer is), valamint a Siemens érintett termékeiről rengeteg bennfentes tudásra volt szükség. Mindez igen kevés szervezetre szűkíti le a világon azt a kört, amely a feladat megoldására vállalkozhatott.”[11]*

Egy amerikai IT biztonsági szakértő azonban arra is rámutatott, hogy Oroszországnak is fűződhettek érdekei az iráni centrifugák elleni támadáshoz.[12]

Politikai szempontból nem tűnik logikai bakugrásnak, ha az iráni atomprogramba amúgy besegítő orosz tudósok révén Moszkva lassítani próbálja a teheráni eredményeket – amíg a program eredménytelen, az áttételes támogatás nem okoz az eddigieknél is súlyosabb problémát az orosz-amerikai diplomáciai kapcsolatokban, ráadásul a közreműködés során szerzett belső információk lehetővé teszik a Stuxnethez hasonlóan célirányos eszköz kifejlesztését.

Nem szabad elfelejteni azt sem, hogy a terrorfenyegetéssel nemcsak a nyugati világnak kell számolnia. Moszkva és Washington erőfeszítéseinek köszönhetően mára a két szuperhatalom készleteiből csak nagyon nehezen kerülhet atomfegyver készítésére alkalmas

[7] A pakisztáni P-1 urándúsító centrifuga iráni változatának a külvilág által adott neve

alapanyag szélsőséges csoportok kezére, azonban Irán egy sikeres atomprogrammal a lehetséges források közé emelkedhet, márpedig a csecsen felkelők, és szélsőséges iszlám csoportok az orosz nemzetbiztonságra is veszélyt jelentenek.

A cikk írója egyúttal arra is emlékeztet, hogy szimpla gazdasági érdekek is állhatnak az iráni atomlétesítmények elleni támadás mögött – amíg szükség van az orosz szakértelemre, a megrendelések is folyamatosan érkeznek majd. A szakértő szerint áttételesen az is ezt a forgatókönyvet igazolja, hogy a rosszindulatú kód visszafejtése közben kizárólag olyan nyomokat és utalásokat találtak, amik amerikai és izraeli fejlesztőket sejtetnek. Ráadásul orosz szempontból meglehetősen kényelmes volt, hogy még a végzetes atomkatasztrófa előtt egy fehérorosz cég felfedezte a Stuxnetet, ezzel időt adva az iráni mérnököknek a védekezésre.[12]

Minden esetre a Stuxnet elkészítéséhez szükséges tudás Oroszországban is rendelkezésre állt.

Még nem is sikerült teljesen megfejteni a Stuxnet minden részletét, amikor 2011 szeptemberében egy újabb rosszindulatú program vált ismertté. Felfedezése a Budapesti Műszaki Egyetem Híradástechnikai Tanszékén működő CrySyS Adat- és Rendszerbiztonság labor munkatársaihoz fűződik. A magyar szakemberek Duqu-nak nevezték el az új kártevőt, amely nagyon sok hasonlóságot mutat a Stuxnettel. Az elemzések szerint valószínűsíthető, hogy a Duqu készítői hozzáfértek a Stuxnet forráskódjához. Az nem tisztázódott, hogy a két program közül melyik volt előbb, vagy csupán egy közös tőről származó, azonban függetlenül fejlesztett kártevőkről van-e szó. Persze lehetséges az is, hogy a Duqu készítői csupán visszafejtették a Stuxnet kódját és egy ahhoz nagyon hasonlót írtak, hogy ezzel a gyanút másfelé tereljék. Még nem sikerült pontosan kideríteni, hogy mi is lehet az új kártevő feladata, de hála a gyors felismerésnek, már elkészült rá a védelem. Az eddig elfogott példányok feladata a megfigyelés volt, a központtól a kártevő letöltötte a megfelelő adatgyűjtő alkalmazást, majd az adatokat visszaküldte. A felfedezett esetekben az adatgyűjtés a számítógépen futó folyamatok listájára, képernyőmentésekre, hálózati felderítésre és billentyűzetfigyelésre terjedt ki.[13]

2012. májusában a budapesti CrySyS labor és vele egy időben a Kaspersky Lab felfedezett egy újabb rosszindulatú kódot, amelyet a magyarok sKyWipernek, a Kaspersky Flamernek nevezett el. Szintén felfedezhető volt a hasonlatosság a Stuxnet kódjával. Ez a malware is modul rendszerű, nagyon kifinomult eszköz, mely a moduloknak köszönhetően tevékenységét rendkívül széles skálán képes kifejteni. Néhány figyelemre méltó káros tevékenység:

- hálózat figyelés, hálózat felderítés, sérülékeny jelszavak gyűjtése
- a fertőzött rendszerek lemezeit átvizsgálja meghatározott programok és egyéb tartalmak után kutatva
- képernyőmentéseket készít, amikor bizonyos folyamatok vagy ablakok aktívak
- a számítógéphez csatlakoztatott mikrofonnal fel tudja venni a környezetben elhangzott zajokat
- a mentett adatokat az irányító szerverekre menti
- tíznél több C&C[8] szervert azonosítottak
- SSH és HTTPS protokollok segítségével kapcsolódik a C&C szerverekhez
- megkerüli a széles körben használt víruskeresőket és egyéb biztonsági szoftvereket
- Windows XP, Vista és Windows 7 operációs rendszereket támad
- képes nagyméretű helyi hálózatokat megfertőzni [14]

[8] Command & Control – olyan szerver, amely irányítja a kártevő tevékenységét

A CrySys Lab jelentésében kiemeli, hogy ez az eddig talált legkifinomultabb kártevő és kifejlesztése nagyon jelentős anyagi és szellemi ráfordítást igényelt, ami állami részvételre utalhat.[15]

2012 augusztusában egy újabb rosszindulatú szoftver tűnt fel. A Gauss névre keresztelt vírus elsősorban banki és egyéb hozzáférési adatokat gyűjt a fertőzött rendszerből, majd továbbítja azokat a Command and Control (C&C) szerverek felé. Egy biztonsági cég szerint a Gauss jelenleg elsősorban Libanonban, Izraelben és a Palesztin területeken aktív, de az Egyesült Államokból is jelentettek fertőzést. A káros szoftver elemzése során a szakemberek számos hasonlóságot fedeztek fel a Gauss és a Duqu, a Flame valamint a Stuxnet férgek között. A moduljait beilleszti különböző böngészőkbe, hogy lehallgassa a felhasználó munkamenetét, valamint, hogy onnan ellopja a tárolt jelszavakat, sütiket valamint a böngésző előzményeket. A jelentések szerint a hordozható adattárolókat fertőző információgyűjtő modul tartalmaz egy titkosított ”payload”-ot is, amely funkciója egyelőre ismeretlen. [16]

2013 januárjában a Kaspersky jelentette be, hogy leleplezett egy nagyarányú online kémkedési akciót. A vírusirtó cég által Vörös októbernek nevezett kártékony kód már 2007 óta volt aktív, főképp Kelet-Európában, a volt szovjet tagköztársaságokban, illetve Kelet-Ázsiában, de találtak fertőzött gépeket szerte a világon kormányszervezetekben, nagykövetségeken, kutatóközpontokban is. A vírus fő célja titkos dokumentumok megszerzése volt, de ezen kívül információkat gyűjtött a megfertőzött hálózatokról is. Ez a vírus is, akárcsak az előzőekben ismertetett kártevők, igen kifinomult és több, eddig ismeretlen metódust alkalmaz működése során. A terjedéséhez viszont régi, bevált módszereket, adathalász emaileket, fertőzött weboldalakat, a Word- és Excel sérülékenységeket használ. A program moduláris felépítésű, több mint ezer modult fejtettek vissza eddig. Az egyik érdekes modul például a fertőzött számítógépre csatlakoztatott okostelefonokról, illetve a gépre dugott pendrive-okról le tudja menteni az érdekesnek tűnő tartalmat, még a törölt fájlokat is vissza tudja állítani ezekről. A forráskód, illetve az ahhoz fűzött megjegyzések orosz programozók munkájára engednek következtetni. Persze az is elképzelhető, hogy ez csak az álcázás része, és az orosz, illetve programozói szlengben elterjedt kifejezésekkel csak félrevezetésből szórták meg az angol nyelvű megjegyzéseket a programsorok mellett.[17]

2013 februárjában a CrySys Lab és a Kaspersky közösen azonosított egy újabb kártevőt, amely 23 ország 59 célpontját támadta, főleg a diplomáciai körökben. A Miniduke-nak elnevezett program az Adobe Reader azóta már javított sérülékenységét használta ki, a kódot egy fertőzött pdf dokumentummal juttatták a kiszemelt számítógépre. Az egyik ilyen anyag például Ukrajna NATO csatlakozásának terveiről szól. A fertőzés után a vezérlőszerverekkel történő kommunikációra a Twittert használja a program. A szakemberek szerint a Miniduke egyedülálló alkotás. Még nem tudni, milyen adatokat sikerült a támadóknak megszerezniük.[18]

A fentebb említett kártevők megjelenése is mutatja, hogy a vírusok és különböző rosszindulatú programok készítői már nem kamaszok, vagy sértett informatikusok, akik a szobájuk mélyén gyártják ezeket a kódokat, mint régen. Ezen kódok írói komoly anyagi és szellemi háttérrel rendelkező fejlesztők, akik a szervezett bűnözés megbízásából dolgoznak vagy állami támogatással a jövő háborúinak fegyvereit készítik.

AZ ANONYMOUS CSOPORT

Az elmúlt időszakban szinte naponta lehetett olvasni az Anonymous csoport támadásairól. Ez a laza szerveződésű internetes közösség vélt, vagy valós sérelmek megtorlásául vagy egyszerűen valamely ügyet felkarolva indít támadásokat internetes tartalmak, cégek, kormányzatok ellen.

2. ábra. Az Anonymous logója
(forrás: http://en.wikipedia.org/wiki/Anonymous_(group) letöltve: 2011. december 02.)

Az Anonymous logója egy fej nélküli, babérkoszorúba foglalt öltönyös figura, tagjai pedig, ha utcára mennek vagy képet tesznek ki magukról a netre, akkor a *V, mint vérbosszú* című filmből ismert mosolygó Guy Fawkes maszkot viselik, amelyet annak főhőse hordott.

A közösség a 2003-ban alakult 4chan nevű képmegosztó oldal felhasználóiból verbuválódott. A kezdetben a japán képregények rajongóinak szóló oldal hamar nagy népszerűségre tett szert, tartalmában és stílusában azonban az internet sötét oldalához tartozik. A beszélgetések úgy általában a tizen-huszonéves internet, online pornó és videojáték-mániás amerikai fiatalok szellemi színvonalán zajlik, akik ebből ítélve az oldal törzsközönségét alkotják. Az obszcén tartalmairól és féktelen szabadosságáról ismert fórum, vagyis képes üzenő fala már kevesebb látogató számára érdekes és vállalható, de így is az internet egyik legnagyobb hatású oldala. Jellemző, hogy felhasználói a kortárs online popkultúra rengeteg fontos elemét termelték, termelik ki és dolgozzák fel újra folyamatosan. A 4chan mindezek ellenére, vagy talán épp ezért, az online tömegkultúra egyik termékeny alkotóműhelyévé vált, amelynek látogatói saját elvetemült humoruk és a Photoshop segítségével rengeteg internetes mémet, vagyis egy adott témára épülő, továbbküldés útján terjedő, folyamatosan remixelt műalkotást dobnak be a köztudatba. A 4chanról származnak például a lolmacskák, vagyis az internetes szlengben feliratozott vicces macskás képek. [19]

Ebből a közegből származik az Anonymus, melynek fontos eszköze a weboldalakat automatikus lekérdezésekkel megbénító túlterheléses támadás, amire magasztos hangnemben megfogalmazott webes szórólapjain toborozza a résztvevőket, rendszerint nem csak a 4chanon, hanem más csevegő szobákban és fórumokon is. A szaknyelven dosolásnak nevezett támadásokban való részvételhez nem is kell más, csak pár ingyenesen letölthető szoftver, amelyek beszerzéséhez, használatához a felhasználók rendszerint már a szórólapokon megkapják a szükséges instrukciókat. 2007-ben először így bénították meg a rasszista kijelentéseiről elhíresült amerikai rádiós, Hal Turner műsorát, noha a 4chanon mindennapos dolog a niggerezés vagy más népek, országok alpári stílusú pocskondiázása. A következő nagy támadás, amely hellyel-közzel a mai napig tart, a szcientológiai egyház ellen indult

2008-ban. Tiltakozásul az egyház által véleményük szerint elkövetett csalások, illegális tevékenységek, személyes szabadságok korlátozása miatt, kiterjedt támadásba kezdtek ellenük. [20] A szolgáltatásmegtagadásos támadásokon kívül nyilvánosságra hoztak több száz iratot és dokumentumot, amelyeket számítógépes betörések útján szereztek.

Saját meghatározásuk alapján tiltakoznak és fellépnek minden olyan jelenség ellen, amely a szólásszabadságot és az Internet szabadságát veszélyeztetik.

Ebbe belefért a Sony ellen indított támadás is, mely során több millió felhasználó adatait, köztük bankkártya számait lopták el és tették nyilvánossá azért, mert a Sony perbe fogta azt a hackert, aki feltörte a PlayStation védelmét.

A legnagyobb port felvert támadássorozatuk a Wikileaks támogatását megakadályozó amerikai intézkedések miatt következett be. Mint az ismeretes, 2010-ben a Wikileaks több ezer titkos amerikai diplomáciai és katonai iratot jelentetett meg az Interneten a szólásszabadság jegyében. Ez komoly diplomáciai feszültséget és még komolyabb biztonsági problémákat okozott, elsősorban az amerikai hadsereg műveleti területein. Az amerikai kormány komoly politikai nyomást fejtett ki az oldal ellehetetlenítésére, többek között a finanszírozásával kapcsolatban. A PayPal, a Visa vagy a MasterCard e nyomás hatására nem engedélyezte a Wikileaks számláira történő utalásokat. Ennek hatására hirdette meg az Anonymous a fenti pénzintézetek elleni támadássorozatát, amelyben sikerült is kisebb fennakadásokat okozni.

Létezik az Anonymous csoportnak magyar szárnya is, Facebook oldaluk is van, ahol a hitvallásukat is közzétették:

Anonymous vagyunk. Egy eszme vagyunk. A pénzügyi és politikai zsarnokság ellen küzdünk itthon és globális szinten, Egy emberibb világot akarunk, ahol nem a profit, a hatalom, az erőszak számít, hanem az igazság, a szabadság, az egyenlőség. Változást szeretnénk elérni: a tudás, az információ nyílt áramlását, a cenzúra eltörlését, a szűk, kapzsi elit uralmának a végét és a 99% valódi hatalmát. Közvetlen demokráciát, igazi beleszólást akarunk. A jelenlegi rendszer igazságtalan, embertelen és végpusztulás felé sodorja a civilizációt. Nincsenek vezetőink, nincsenek rendszabályaink, nincsenek bombáink, Sokan vagyunk, napról-napra egyre többen vagyunk. Légiót alkotunk. Nem felejtünk, nem bocsájtunk meg. Számolj velünk és számíts ránk! Csatlakozz hozzánk és legyél részese egy győztes forradalomnak![21]

Magyarországi tevékenységük weboldalak feltörésével kezdődött, 2012. március 4-én feltörték az Alkotmánybíróság honlapját és átírták az Alaptörvény szövegét, április 8-án a Nemzeti Rehabilitációs és Szociális Hivatal következett. Augusztus 28-án túlterheléses támadást intéztek a Közgép Zrt. honlapja ellen, amelyet sikerült is egy rövid időre megbénítani. Ennek az ügynek a kapcsán a rendőrség őrizetbe vett öt személyt, akik el is ismerték azt, hogy részt vettek a támadásban. Ellenük számítástechnikai rendszer és adatok elleni bűncselekmény megalapozott gyanúja miatt indítottak eljárást.[22]

A magyar Anonymous saját csoportjának méretét 50-60 aktív főre tesz, akik állandóan akcióra készek, valamint további 150-200 fő elkötelezett követőre.

Hosszan sorolhatnánk a csoport által elkövetett támadásokat, a világ szerzői jogvédő hivatalaitól az arab tavasz támogatásán át a világméretű pedofilhálózat feltöréséig.

Céljaik néhány esetben támogathatók ugyan, de a módszereik veszélyesek és egyértelműen törvénytelenek. Nincsenek nevesített vezetőik, szervezetük decentralizált és tagjaik a világ minden részén megtalálhatók. Az, hogy milyen célpontot támadnak sikeresen, attól is függ, hogy mennyi támogatót tudnak megnyerni maguknak.

Ha a dolgok mögé nézünk, az a víziónk támadhat, hogy ha valaki a megfelelő időben, megfelelő módon tudná befolyásolni ez a világméretű közösséget, akkor nagyon komoly károkozásra lehetne képes, legyen az akár terrorista, akár egy ország.

KÖVETKEZTETÉSEK

Cikkemben be kívántam mutatni, hogy az elmúlt néhány évben milyen fejlődésen ment keresztül az informatikai támadások metodikája.

Mint azt a fenti példák mutatják, az számítógép-hálózatok elleni támadások egyre jobban beépülnek a hagyományos konfliktusok eszköztárába. Az, hogy a konfliktusokban részt vevő felek még nem ismerik el a felelősségüket a kibertámadásokban, az annak köszönhető, hogy nem akarják az ilyen irányú képességeiket a világ elé tárni. Mindenki számára nyilvánvaló, hogy például Oroszország rendelkezik azokkal a képességekkel, amelyekkel az észtországi vagy a grúziai támadásokat kivitelezhették, azonban a „hazafias hacker-csoport" teória remek fedőtörténet az események magyarázatára. Kínában, ahol nagy súlyt fektetnek a hadsereg számítógép-hálózati műveleti képességének fejlesztésére, szintén az országban működő hacker csoportok tevékenységével magyarázzák az amerikai és európai kormányzati, katonai célpontok elleni kínai szerverekről érkező támadásokat. Nehéz azonban elképzelni, hogy a több ezer kiképzett katonai hacker csak gyakorlatozik a laktanyákban, miközben néhány fekete kalapos támadó ilyen kiemelt fontosságú célpontokat támad. Tisztában kell lennünk azzal, hogy a világ számos hadseregében lázasan készülnek a kiberhadviselésre és nem csak a védekezésre, hanem a támadásra is.

A rosszindulatú programok készítésében is megfigyelhető az ilyen irányú fejlődés. A fent bemutatott programok kifejlesztése már olyan infrastruktúrát és magasan képzett programozók összmunkáját feltételezi, amely mögött kormányzatokat kell sejtenünk. Felvethető még a szervezett bűnözés tevékenysége is, azonban számukra a pénzszerzés a fő motívum, vélhetően nem keveredtének olyan ingoványos talajra, mint a katonai titkok fürkészése, főleg nem az Egyesült Államok kárára. Az utóbbi idők történései azt látszanak bizonyítani, hogy a hírszerzés egyre jobban kiterjed a kibertérre, mindenki igyekszik kifürkészni a riválisországok kritikus informatikai infrastruktúráját, megismerni a számítógépeken őrzött katonai, diplomáciai, pénzügyi, ipari titkait. A Stuxnet-tel pedig már a kiberfegyver is elkészült, amellyel fizikai károk is okozhatók. Úgy vélem, nem nehéz a jövőt sem megjósolni. Egyre kifinomultabb rosszindulatú szoftverek fognak születni és ezek egy jelentős részét csak akkor fogja megismerni a világ, amikor már egy éles, háborús helyzetben használták őket. Nincs kétségem afelől, hogy számos ország rendelkezik már ilyen fegyverrel és egy adott helyzetben használni is fogják őket.

Néhány évvel ezelőtt egy konferencián az egyik előadó azt mondta, hogy a kiberháború nem fog kitörni, hanem már folyik. Az elmúlt idők eseményeit nézve ez bizony nagy igazság. Az igazi kérdés az, hogy az egyes országok mennyire tudják majd megvédeni magukat az interneten keresztül érkező támadásokkal szemben.

Nem szabad félvállról venni a különböző hacktivista csoportokat sem, amelyek bizonyos célok mellé felsorakozva nagyon komoly erőt jelenthetnek. Ha például az Anonymous tagjait sikerülne meggyőzni érvekkel vagy akár megtévesztéssel egy kibertámadás támogatására valamely kormányzatnak vagy érdekcsoportnak, komoly segítséget jelentenének a sikerhez. Természetesen ez fordítva is igaz lehet, ha a célpont ország tudná segítségül hívni őket, jelentősen javíthatna az esélyein.

Ezek ellen a fenyegetések ellen ki kell építeni a megfelelő védelmi rendszereket minden olyan országnak, amely fejlett információtechnológiával rendelkezik, így hazánknak is. Az ilyen védelem kiépítésénél számításba kell venni a köz és magánszféra erőforrásait is. A kritikus infrastruktúrák védelme mellett azonban létre kellene hozni egy ütőképes, jól felkészült egységet is, amely sikerrel tudna számítógép-hálózati műveleteket bonyolítani, legyen szó védekezésről vagy megelőző csapásról. A nemzetközi példákat alapul véve ezt a szervezetet a Magyar Honvédség kötelékében lenne célszerű kialakítani. Ezáltal hadseregünk egy újabb, akár a NATO számára felajánlható képességgel is gyarapodhatna.

Felhasznált irodalom

[1] A hálózati társadalom sérülékenysége
http://www.nato.int/docu/review/2002/issue2/hungarian/features2.html
(letöltve: 2012. október 12.)

[2] Haig Zsolt – Kovács László: Fenyegetések a cybertérből, Nemzet és biztonság. I. évfolyam, 5. szám. Budapest, 2008. május, pp.: 61-69 ISSN 1789-5286

[3] Steve Kettmann: Soviets Burned By CIA Hackers?
http://www.wired.com/culture/lifestyle/news/2004/03/62806
(letöltve: 2012. október 12.)

[4] Kovács László: Információs hadviselés kínai módra, Nemzet és biztonság II. évfolyam 7. szám. Budapest 2009. szeptember pp.: 35-44, ISSN 1789-5286

[5] Németh József, Hajzer Tamás: Az orosz-grúz háború néhány jellemző vonása
http://www.biztonsagpolitika.hu/?id=16&aid=709&title=Az_orosz-grúz_háború_néhány_jellemző_vonása, (letöltve: 2012. október 12)

[6] Az Interneten kis zajlik az orosz-grúz összecsapás
http://www.origo.hu/techbazis/internet/20080811-az-interneten-is-zajlik-az-oroszgruz-osszecsapas.html (letöltve: 2012. október 12.)

[7] Jeremy Norman: The First Computer Virus
http://www.historyofinformation.com/expanded.php?id=2860
(letöltve: 2013. január 25.)

[8] Berzsenyi Dániel, Szentgáli Gergely: STUXNET: a virtuális háború hajnala
http://www.biztonsagpolitika.hu/index.php?id=16&aid=932
(letöltve: 2012. október 12.)

[9] Kovács László, Sipos Mariann: A stuxnet és ami mögötte van
Hadmérnök V. évfolyam 4. szám Budapest, 2010. december pp.:163-172,
ISSN 1788-1919

[10] Cserháti András: A Stuxnet vírus és az iráni atomprogram, Nukleon IV. évfolyam 1. szám Budapest 2011 március p.:85, ISSN 1789-9613

[11] Ralph Langner hamburgi vírusbiztonsági szakértő blogja,
http://www.langner.com/en/blog/page/5/

[12] Panayotis A. Yannakogeorgos: Was Russia Behind Stuxnet?
http://the-diplomat.com/2011/12/10/was-russia-behind-stuxnet/?all=true
(letöltve: 2012. október 12.)

[13] Symantec Security Response: W32.Duqu The precursor to the next Stuxnet
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdff (letöltve: 2012. október 22.)

[14] Flamer/sKyWIper – egy újabb veszélyes kiberfegyver bukkant fel,
http://tech.cert-hungary.hu/tech-blog/120529/flamerskywiper-egy-ujabb-veszelyes-kiberfegyver-bukkant-fef (letöltve: 2012. október 22.)

[15] sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks
http://www.crysys.hu/skywiper/skywiper.pdf (letöltve: 2012. október 22.)

[16] Újabb taggal bővült a Stuxnet család
http://tech.cert-hungary.hu/tech-blog/120810/ujabb-taggal-bovult-a-stuxnet-csalad (letöltve: 2012. október 22.)

[17] „Red October" Diplomatic Cyber Attack Investigation
http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation (letöltve: 2013. január 20.)

[18] The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor,
https://www.securelist.com/en/blog/208194129%20The_MiniDuke_Mystery_PDF_0_day_Government_Spy_Assembler_Micro_Backdoor (letöltve: 2013. február 28.)

[19] Vámosi Gergő: A kretének háborúja zajlott az Interneten,
http://www.origo.hu/techbazis/20101117-a-4chan-a-tumblr-ellen-a-kretenek-haboruja-zajlott-az.html (letöltve: 2012. október 22.)

[20] Anonymous vs. scientology,
https://whyweprotest.net/anonymous-scientology/ (letöltve: 2012. október 22.)

[21] Az Anonymous Operation Hungary adatlapja a Facebook-on,
https://www.facebook.com/OpHunAnon/info (letöltve: 2012. október 22.)

[22] Dajkó Pál: Elfogták a Közgépet megtámadó Anonymous-szimpatizánsokat,
http://itcafe.hu/hir/orfk_anonymous_kozgep.html (letöltve: 2012. október 22.)

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Fleiner Rita
fleiner.rita@nik.uni-obuda.hu

KÖZIGAZGATÁSI ADATBÁZISOK ÖSSZEKAPCSOLÁSÁNAK TECHNIKAI MEGVALÓSÍTÁSA

Absztrakt

Az államigazgatási szerveknek kötelessége a gazdaságra és a társadalmi folyamatokra kiható döntéseiket előzetesen mérlegelni és eredményeiket utólagosan vizsgálni. A költségvetési szervek által létrehozott adatbázisok nem csak adminisztratív célokra, hanem elemzések, hatásvizsgálatok és döntés előkészítés céljára is alkalmazandók. A vizsgálatokhoz szükség lehet a különböző adatbázisokból származó adatok együttes kezelésére, az adatbázisok összekapcsolására. A publikációban a közigazgatási adatbázisok összekapcsolásának technikai megvalósítását vizsgáljuk. Ennek keretében elemezzük az összekapcsolás alapját képező anonim kapcsolati kód fogalmát és képzési módját, feltárjuk az adatbázisok összekapcsolásának biztonsági elvárásait, követelményeit és bemutatjuk az összekapcsolás folyamatát.

It is the duty of the government to consider their decisions influencing the economy and the social processes beforehand and to examine their results posteriorly. Databases created by government agencies can be used not only for administrative purposes, but also for analyses, impact assessments and decision making processes. These examinations may need joint data from different databases, so the connection of databases must be performed. In the publication we examine the technical implementation aspects of connecting administrative databases. In this framework we analyse the concept and construction of the anonym connection code providing the basis of the connection, we reveal the security requirements of the database connection, and we present the steps of the connection process.

Kulcsszavak: *adatbázis, adatbázis összekapcsolás, elektronikus közigazgatás, biztonsági elvárás, hash függvény ~ database, connecting databases, electronic government, security requirement, hash function*

BEVEZETÉS

A közigazgatás elektronikus nyilvántartásai az elsődleges adminisztratív célok mellett adat alapú döntéshozás, statisztikai számítások, társadalomkutatási feladatok számára is felhasználhatók. *Közigazgatási adatbázison* a továbbiakban olyan, a magyar közigazgatásban fellelhető adatbázist értünk, melyet valamely államigazgatási szerv a saját feladatai ellátása során hozott létre. A közigazgatási adatvagyon felhasználásának előmozdítása érdekében született meg az Európai Parlament és a Tanács 2003/98/EK számú irányelve [1]. Az irányelv minimum szabályokat állapít meg a tagállamok közigazgatási szervei birtokában lévő dokumentumok (ideértve az adatokat is) további felhasználására.

Magyarországon az irányelv céljainak elérését a döntés előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló 2007. évi CI. törvény [2] teszi lehetővé. A törvény kimondja, hogy az államnak és az államigazgatási szerveknek kötelessége, hogy a gazdaságra és a társadalmi folyamatokra kiható döntéseiket előzetesen mérlegeljék, eredményüket utólagosan vizsgálják, és ehhez adminisztratív céllal gyűjtött adatokat is felhasználjanak. Ez a törvény szabályozza a közigazgatási adatok összekapcsolásának lehetőségeit is. A szabályozásra az európai uniós irányelv mellett jelentősen hatottak a hazai adatvédelmi előírások, melyek európai szinten kifejezetten szigorúnak számítanak.

A kormányzati döntés-előkészítéshez és hatásvizsgálatához szükség lehet természetes személyekre vagy gazdasági szervezetekre vonatkozó mikroszintű adatokra. A mikroszintű adatok kezelésének feltételeit különböző jogszabályok - méghozzá az adatvédelmi törvény [3], az adózás rendjéről szóló törvény [4] és a statisztikáról szóló törvény [5] - írják le. A személyes adatokat is tartalmazó adatbázisok közérdekű, vagy más jogszerű célra való felhasználásának jogi feltétele az *adatok személyességének megszüntetése*, az ún. *anonimizálás*. Az anonimizálás egy olyan eljárás, melynek során az egyes személyeket beazonosító adatokat törölni vagy visszafordíthatatlan módon módosítani kell úgy, hogy a tárolt adatok az érintettel a továbbiakban ne legyenek kapcsolatba hozhatók.

Az elemzések során felmerülhetnek olyan kérdések, melyek megválaszolásához szükség lehet több adatbázis összetartozó sorainak összekapcsolására. *Adatbázisok összekapcsolása* technikai értelemben azt jelenti, hogy különböző adatbázisok adataiból – fizikailag, vagy virtuálisan – egy új adatbázist hozunk létre. Relációs adatbázisok esetében ez különböző adattáblák sorainak összekapcsolását jelenti, amely megfelelő oszlopokban szereplő adatértékek egyezésére épül. Az adatbáziskezelés fogalomrendszerében ez ún. elsődleges kulcsok és idegen kulcsok segítségével történhet.

A közigazgatási adatbázisok összekapcsolásának vizsgálatát a [6] publikációban leírtakra alapozva végezzük el. A publikáció

- elemzi az összekapcsolás alapját képező anonim kapcsolati kód fogalmát és képzési módját;
- feltárja az adatbázisok összekapcsolásának biztonsági elvárásait, követelményeit;
- bemutatja az összekapcsolás folyamatát.

ANONIM KAPCSOLATI KÓD FOGALMA ÉS KÉPZÉSE

A kutatásokban, elemzésekben szükség lehet a különböző adatbázisok sorainak összekapcsolására, ami az adatbázis azonosítók (egyedi kulcsok) egymáshoz rendelésén keresztül valósítható meg. Ma Magyarországon az adatvédelmi törvény nem teszi lehetővé a különböző nyilvántartásokban található személyes adatok összekapcsolását. Személyes adatnak minősülnek a természetes személlyel kapcsolatba hozható adatok, mint például név, születési év, lakcím, életkor. Külön törvény [7] véd egyes mesterséges személyes azonosítókat, mint adószám, TAJ szám, személyi szám, ezeket még korlátozottabban lehet

kiadni, összekapcsolásra felhasználni. Az adatvédelmi törvény szerint személyes adatokat akkor lehet kezelni, továbbadni, összekapcsolni, ha ehhez az érintett hozzájárul, vagy törvény megengedi.

Az univerzális azonosításra alkalmas személyazonosító jel használatát Magyarországon az Alkotmánybíróság 1991-es döntése [8] a személyes adatok védelme érdekében megtiltotta. Az univerzális személyazonosító helyett ma Magyarországon természetes személyazonosítóként a (név, anyja neve, születési hely és idő) hármast, illetve a személyiadat- és lakcímnyilvántartásban a személyazonosító jelet, az adózással kapcsolatos nyilvántartásokban az adóazonosítót, a társadalombiztosítási rendszerben pedig a társadalombiztosítási azonosító jelet (TAJ) használjuk. Ez utóbbi három mesterséges azonosítót a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény [7] hozta létre, továbbá rendelkezett arról, hogy ezek az azonosítók személyes adatok, valamint arról, hogy mely szervek és hogyan használhatják ezeket az azonosítókat.

Az adatbázisok összekapcsolásának folyamata kapcsán adatkérő szervnek nevezzük azt, aki az adatok átadását igényeli, vagyis aki számára az összekapcsolt adatok átadásra kerülnek. Az adatkezelő szerv vezeti az adott nyilvántartást, adatbázist. Az adatbázis létrehozásáért felelős szerv végzi el a különböző adatkezelőktől megkapott adatok összekapcsolását és adja át az összekapcsolt adatokat az adatkérő szerv számára.

Magyarországon a kormány az adatbázis létrehozásáért felelős szervként a Neumann János Digitális Könyvtár és Multimédia Központ Kht.-t (továbbiakban: NKHT) jelölte ki. A különböző adatbázisok összetartozó sorainak összekapcsolására a 2007. évi CI. törvény az anonim kapcsolati kód használatát írja elő. A törvény szerint *anonim kapcsolati kódnak* nevezzük az ugyanazon személyre vonatkozó személyazonosító adatokból véletlenszerű elemet is tartalmazó módszerrel képzett karaktersort, amellyel ugyanazokból az adatokból mindig ugyanaz a karaktersor jön létre, de amely eredményeképpen létrejött karaktersorból a személyazonosító adatok nem állíthatók helyre. Az adatok összekapcsolását az adatbázis létrehozásáért felelős szerv végzi úgy, hogy a különböző adatkezelőktől azonos módszerrel képzett anonim kapcsolati kóddal veszi át és kapcsolja össze a különböző forrású adatokat. A törvény előírja, hogy az adatbázis létrehozásáért felelős szerv feladata az anonim kapcsolati kód képzésének módszerének meghatározása. A törvény szerint a kódképzés módszerének a következő kriptográfiai biztonsággal is kapcsolatos tulajdonságokkal kell bírnia:

- olyan személyazonosító adatok alapján kell képezni, melyek kezelésére valamennyi érintett adatkezelő jogosult,
- a kódképzés alapját nem képezhetik olyan személyazonosító adatok, amelyek kezelésére az adatkérő vagy az adatbázis létrehozásáért felelős szerv jogosult,
- az adatkezelőnek a kezelésében lévő személyes adatról, adótitokról, vagy egyedi statisztikai adatról készített másolatot visszafordíthatatlan módon kell módosítania úgy, hogy az az érintettel a továbbiakban ne legyen kapcsolatba hozható,
- a kódképzés konkrét módszere tartalmazzon egyedi, véletlenszerűen megállapított elemet,
- egy adott adatkérés esetén ugyanazokból az adatokból mindig ugyanaz a karaktersor jöjjön létre,
- az összekapcsolást anonim kapcsolati kód segítségével kell végrehajtani.

Az anonim kapcsolati kód képzésének alapjául az NKHT hash függvény használatát választotta. A hash függvények fő tulajdonsága, hogy tetszőleges hosszúságú bemenetet (bitsorozatot) egy véges hosszúságú kimenetre képeznek le. Hash függvény esetén a bemenetet gyakran üzenetnek, a kimenetet pedig lenyomatnak vagy hash értéknek nevezzük. A leképezés több-az-egyhez típusú, azaz egy hash értéket sokféle lehetséges bemenet előállíthat.

Hash függvény definíciója a következő: Legyen X a lehetséges bemenetek halmaza, Y pedig a lehetséges kimenetek véges halmaza és teljesüljön rájuk, hogy $|X| \geq |Y|$. Ekkor a $h:X \rightarrow Y$ függvényt hash függvénynek nevezzük.

A hash függvények szoros kapcsolatban állnak az egyirányú függvényekkel. Egy $f: X \rightarrow Y$ függvény egyirányú, ha a minden lehetséges bemenethez tartozó függvényérték könnyen kiszámítható (legfeljebb polinom idejű algoritmussal), azonban a kimenetek inverzeit nehéz kiszámítani (legalább exponenciális idejű algoritmust igényel). Egy hash függvénnyel szemben a következő biztonsági kritériumokat szokták megfogalmazni. Nagyon nehéz (gyakorlatilag lehetetlen):

- adott h(m) hash értékhez egy megfelelő m bemenetet találni (egyirányúság, őskép-ellenállás),
- adott m-hez olyan m'-t találni, hogy h(m) = h(m') (gyenge ütközésmentesség, 2. őskép-ellenállás),
- két olyan tetszőleges m-et és m'-t találni, hogy h(m) = h(m') (erős ütközésmentesség),
- illetve a bemenet bármely bitjének megváltozása a kimenet bitjeinek mindig átlagosan felét változtassa meg (lavinatulajdonság).

A hash függvények fontos alkotórészei különböző kriptográfiai probléma megoldásának. A kriptográfiai hash függvények egyik elsődleges felhasználási területe az adatintegritás biztosítása. Tetszőleges hosszúságú adatról fix hosszúságú lenyomatot, ellenőrző összeget készítenek hash függvénnyel és azt tárolják el. Később az adat változatlanságáról úgy győződhetnek meg, hogy ismét elkészítik az adat lenyomatát, és ha ez nem egyezik az eredetivel, akkor biztos, hogy változás történt. A kriptográfiai hash függvények fontos szerepet játszanak a digitális aláírás folyamatában. A digitális aláíró algoritmusok először lenyomatot készítenek az aláírandó adatról, és csak a lenyomatot írják alá. Szinten gyakori, hogy a jelszavas azonosítást használó rendszerek nem a jelszavakat tároljak, hanem a jelszavak lenyomatait és a jelszavak ellenőrzése is a lenyomatok alapján történik.

A kapcsolati kód képzéséhez ki kell jelölni azon adatbázis attribútumokat, melyek alapján történik a lenyomat képzése, másrészt meg kell adni a lenyomatképző algoritmust, amely egy, az adott adatkérésre vélelenszerű elemet is felhasznál. Az anonim kapcsolati kód képzésére az NKHT a Kripto Kft. által készített és kereskedelmi forgalomba hozott, Codefish nevű hash függvényre [9] alapuló algoritmust választotta. A Codefish hash függvény kriptoanalízisét vizsgálták tudományos kutatások [10], [11], melyek kimutatták, hogy a függvény gyenge és erős ütközésmentesség tulajdonságai támadhatóak, a függvény ezeket biztonsági kritériumokat nem teljesíti.

ADATBÁZISOK ÖSSZEKAPCSOLÁSÁNAK BIZTONSÁGI ELVÁRÁSAI

A következőkben a törvényből és a kormányrendeletből levezethető, az összekapcsolás rendszerére vonatkozó biztonsági elvárásokat vizsgáljuk. A biztonsági elvárások pontos megfogalmazása segíti a megvalósítandó rendszer tervezését, érékelését és ellenőrzését. Mivel az összekapcsolást informatikai rendszer valósítja meg, továbbiakban az összekapcsolás informatikai rendszerének biztonsági elvárásait keressük.

A megvalósított feladat alapján az adatbázisok összekapcsolását végző informatikai rendszert fokozott biztonsági kategóriába sorolták be [12]. A [13] dokumentumban ismertetett biztonsági kategorizálás módszere szerint az informatikai rendszer által kezelt adatok sérülésének következményét alacsony, fokozott és kiemelt osztályokba sorolják be. Az adatbázisok összekapcsolását végző rendszer esetében az adatok bizalmasságának és sértetlenségének sérülését fokozott szintbe sorolták, míg a rendelkezésre állását alacsony kategóriába. A biztonsági kategóriát a három biztonsági célra (bizalmasság, sértetlenség,

rendelkezésre állás) kapott legnagyobb szint határozza meg, ez pedig az adatbázisok összekapcsolása esetén a fokozott.

A fokozott biztonsági kategória meghatározza a rendszer által felvállalt általános informatikai biztonsági követelményeket. Ezek vonatkoznak például az azonosítás és hitelesítés, hozzáférés ellenőrzés, rendszer és kommunikáció védelem, naplózás, konfiguráció kezelés folyamataira. Azonban az összekapcsolást szabályozó törvényből és kormányrendeletből levezethetőek a rendszerre vonatkozó speciális biztonsági elvárások is. Ezeket az elvárásokat meg kell fogalmazni az informatikai biztonság fogalomrendszerével, ami a rendszer helyes megvalósítása, értékelése és ellenőrzése kapcsán elengedhetetlen. Ez konkrétan azt jelenti, hogy meg kell határozni a rendszer specifikus biztonsági célokat és ezek teljesüléséhez szükséges biztonsági követelményeket.

A törvényből és a kormányrendeletből egyértelműen levezethető a következő két speciális biztonsági cél:

1. Szükséges az összekapcsolt adatok alanyának védelme. Biztosítani kell, hogy az összekapcsolt adatokból ne tudjon senki következtetni az adatok alanyára (sem kívülálló, sem adatkérő, sem adatkezelő, sem az adatbázis létrehozásáért felelős szerv).
2. Szükséges a különböző összekapcsolások ismételt összekapcsolásának megakadályozása. Ez azt jelenti, hogy a különböző adat összekapcsolásokból származó eredményeket ismételten ne tudja összekapcsolni senki. Ez abból következik, hogy adatbázis összekapcsolást csakis konkrét, előre definiált célhoz kötötten lehet végrehajtani, amit miniszter vagy kormányhivatal vezetője rendelhet el, és ennek kapcsán az átadandó adatok körét és az átadás konkrét célját meg kell határozni.

A törvény előírja, hogy az összekapcsolást anonim kapcsolati kód képzésén keresztül kell megvalósítani. Az anonim kapcsolati kód képzését úgy kell meghatározni, hogy ugyanazokból az adatokból mindig ugyanannak a kimenetnek, azaz karaktersornak kell előállnia (egy adott lekérdezés esetén a különböző adatbázisok), de a létrejött karaktersorból a személyazonosító adatok ne legyenek előállíthatók. Ez a követelmény a kriptográfiai algoritmusok közül az egyirányú függvények csoportjára jellemző. Az adatbázis létrehozásáért felelős szerv a kódképző algoritmus alapjául hash függvényt választott. A következőkben azokat a kriptográfiai tulajdonságokat (követelményeket) soroljuk fel, melyekkel a kódképző szolgáló algoritmusnak, azon belül hash függvénynek rendelkeznie kell ahhoz, hogy a törvény előírásai teljesüljenek.

- A hash függvénynek egyirányúnak kell lennie
- E tulajdonság teljesülése szükséges ahhoz, hogy a kommunikációban átadott hash értékekből a védendő információk ne legyenek visszaállíthatóak, az anonimitás biztosítható legyen.
- A hash függvénynek rendelkeznie kell lavina-hatással
- E tulajdonság teljesítésülése szükséges ahhoz, hogy néhány karakter, vagy bit becslése nem vigyen közelebb a védendő információhoz. Azaz egy bit eltérés az inputban teljesen véletlenszerű változást okozzon a hash képben. Szintén ez a tulajdonság szükséges, hogy közeli bemenő adatok (például csak kevés karakterben eltérő adószámok) ne legyenek felismerhetők a hash értékek sokaságában.
- A hash függvénynek erősen ütközésmentesnek kell lenni
- E tulajdonság teljesítése szükséges ahhoz, hogy ne lehessen reális időben találni két azonos védendő adatot, melynek ugyanaz a hash képe. Az ütközés (két bemenő adat hash képének egyezése) zavart okozhatna a különböző adatbázisokból származó adatok párosításában.
- Rövid bemenő adatsor biztonsága

- A hash függvény előzőekben felsorolt kriptográfiai tulajdonságainak teljesülnie kell a feladatkörből adódó rövid bemenő adatsorra is, mivel Magyarországon a statisztikai minta kiindulási alapja eléggé kicsi. Rövid bemenő adatsor mellett is garantálni kell a megfelelő biztonságot.
- A kódképző algoritmus véletlenszerűségét biztosítani kell
- A törvény előírja, hogy az eljárásnak tartalmazni kell véletlenszerű (azaz tikos) kulcselemeket. Ezen elemek kellő szabadsági fokú véletlenszerűségét garantálni kell azért, hogy az eljárás ismeretében se legyenek kipróbálhatóak, megszüntetve ezáltal a véletlenszerűséget. A szabadsági foknak 100 bitnek kell lennie.

A különböző összekapcsolások ismételt összekapcsolásának megakadályozása teljesüléséhez közvetlenül hozzájárul a véletlenített hash függvény azáltal, hogy az anonim kapcsolati kód képzési módszerében véletlenszerű elemeket is használnak, így több adatkérést nem lehet ugyanazzal a kóddal megvalósítani, ezáltal ezek eredményeit még az adatkérő és az adatkezelő sem képes összevonni.

A Codefish hash függvény nem ütközésmentes és a gyakorlati támadások különösen érvényesek rövid bemenő adatsorra [10], ezért ennek kiküszöbölésére az összekapcsolást elvégző algoritmust megvalósító programot a következő tulajdonságokkal ruházták fel:

- Egy véletlenszerű, 1024 bites S, illetve egy véletlenszerű 3*1024 bites V paramétert generál, melyeket a kódképzési módszer adatkérésenkénti módosítására használnak. Ezt az S és V paramétert állítja elő az NKHT minden adatkéréskor egyszer, és küldi el az érintett adatkezelőknek. Az S paramétert modulusnak, a V paramétert maszk-vektornak hívják.
- A program a célkörnyezetben képes arra, hogy egy adott, 1024 bites bemenő adatra, valamint az adott modulusra és maszk vektorra válaszul egy 256 bites, hexadecimális számrendszerben ábrázolt számsorozatot adjon. Ez lesz a kapott anonim kapcsolati kód.

Az NKHT kérésére a Hunguard kft. elvégezte az adatbázisok anonimizált összekapcsolását megvalósító rendszer biztonsági értékelését [14]. A minősítők a tanúsítványban kijelentik, hogy az összekapcsolást elvégző algoritmus és program megfelel a rendszer biztonsági előirányzatában [12] megfogalmazott funkcionális és garanciális biztonsági követelményeknek.

AZ ÖSSZEKAPCSOLÁS FOLYAMATA

Az összekapcsolás folyamatának lépéseit az NKHT eljárásrendjét leíró dokumentum alapján tárgyaljuk [15]. Adatbázisok összekapcsolását miniszter vagy kormányhivatal vezetője rendelheti el. Az adatbázisok összekapcsolásának folyamatában az adatbázis létrehozásáért felelős szervnek az adatkezelőkkel egyeztetve ki kell választania az anonim kapcsolati kód képzésére felhasználható személyi azonosító mezőket. Ezeket a törvény [2] szerint úgy kell meghatározni, hogy kezelésükre minden érintett adatkezelő jogosult legyen, ugyanakkor sem az adatkérő, sem az adatbázis létrehozásáért felelős szerv nem. Ezután az adatbázis létrehozásáért felelős szervnek elő kell előállítania az anonim kapcsolati kód képzéséhez szükséges véletlenszerű paramétert és továbbítania kell a programot, a futtatásához szükséges információkat és a paramétert a mintaképzésért felelős adatkezelőhöz és a kapcsolódó adatkezelőkhöz. A sikeres továbbítás után az adatbázis létrehozásáért felelős szerv törli az anonim kapcsolati kód képzésére szolgáló véletlen paramétert.

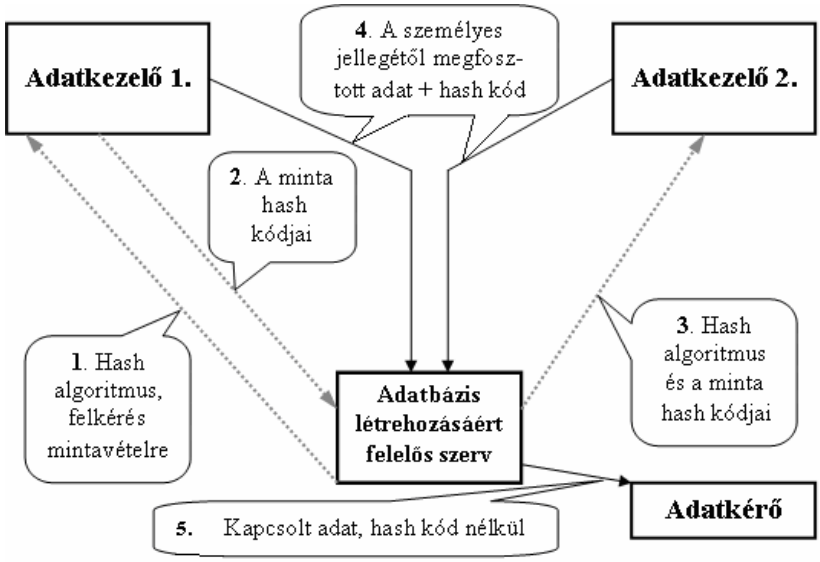
Az adatbázis létrehozásáért felelős szerv kérésére az egyik adatkezelő szerv (a továbbiakban mintaképzésért felelős adatkezelő) mintát vesz az általa kezelt adatbázisból. Mintaképzésnek nevezzük azt a folyamatot, amikor a mintaképzésért felelős adatkezelő az adatkérés paramétereinek megfelelően kialakítja az igényelt mintát, azaz leválogatja az

adatbázisaiból a kiválasztási és mintaképzési szempontoknak megfelelő tételeket. Ezután a minta tételeiben a kiválasztott azonosító adatokra alkalmazza a kapott anonim kapcsolati kód előállító programot. Végül az előállított kapcsolati kódokat és a hozzájuk tartozó, igényelt adatokat az adatkezelő átadja az NKHT-nak.

Az adatbázis létrehozásáért felelős szerv az anonim kapcsolati kódokat, az ehhez tartozó adatok nélkül átadja az adatkérésben megjelölt többi adatkezelőnek. Az érintett adatkezelők saját adatbázisaikból leválogatják az eredeti kérés kiválasztási szempontjainak megfelelő tételeket, alkalmazzák rájuk a kapott anonim kapcsolati kód előállító programot, és kiválasztják azokat, amelyek megfelelnek a kapott kapcsolati kódoknak. Ezután elvégzik az anonimizálást, majd az adatkezelők átadják az NKHT-nak az eredményül kapott adatokat a kapcsolati kódokkal. Az adatkezelő szervek a kódképzéshez kapott véletlenszerűséget biztosító paramétert és a kapcsolati kódokat az adatok átadása után törlik.

Az összekapcsolás folyamatában az NKHT átveszi a leválogatott és anonimizált adatokat tartalmazó állományokat és a kapcsolati kódok segítségével összekapcsolja ezeket. Amennyiben ismétlődő tételek is előfordulnak vagy keletkeznek, és az adatkérő igényli az azonos alanyhoz tartozó adatok jelzését, a kapcsolati kódokat az összekapcsolás után futó sorszámmal helyettesíti úgy, hogy azonos kódhoz tartozók azonos sorszámot kapjanak. Ellenőrzi - szükség esetén az adatkezelők bevonásával -, hogy az eredmény továbbra is megfelel az anonimizálás feltételeinek. Törli a kapcsolati kódokat az eredményből és átadja az adatkérő kapcsolattartójának a leválogatott és összekapcsolt adatokat.

A döntés-előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló törvény indoklásában [16] megtalálható ábra jól szemlélteti az összekapcsolás folyamatát:



1. ábra. Az összekapcsolás folyamata [16]

Előfordulhat, hogy az eredményezett minta túl kevés adatot tartalmaz, vagy a reprezentativitási mutatói az igényeknek nem felelnek meg (például olyan esetekben, amikor a mintaképző adatkezelő nem rendelkezett minden szükséges adattal). Ebben az esetben a kapcsolódó adatkezelő jelezheti a hibát, és kérheti a mintaképzésért felelős adatkezelőt, hogy készítsen bővebb, több tételből álló mintát. Ilyenkor az első lépéstől kezdve ismétlődik ez a folyamat. Amennyiben a minta megfelelő, az adatkezelők elkezdhetik a leválogatást és anonimizálást.

Egyének esetén a kódolás legtöbbször a személyek természetes azonosítóin alapul. Ekkor a lenyomatképzés felveti az adatok különböző adatkezelőknél lévő szinkronizáltságának kérdését. Elvileg ez a probléma rendezett, mert a természetes azonosító adatok tekintetében a

személyiadat-nyilvántartás a hitelesnek elfogadott, és [17] törvény rendelkezik a személyiadat- és lakcímnyilvántartásból történő rendszeres adatátadásról. Ugyanakkor a gyakorlat szerint jelentős eltérések vannak az egyes adatkezelőknél tárolt természetes azonosító adatok tekintetében. Ezért ilyen esetben meg kell vizsgálni az adatkezelőknél tárolt természetes azonosító adatok szinkronizáltságnak mértékét és meg kell határozni ezek közös formátumát. Ki kell térni a több elemből álló azonosító helyes összefűzésére, a megfelelő karakterkódolásra, az eltérő formátumokból adódó egyéb konverziós lépésekre.

Az adatbázis létrehozásáért felelős szervnek az adatok átadása előtt a polgárok lakcímére vonatkozó adatokat úgy kell módosítania, hogy azokból az érintettek lakóhelye a kistérségnél pontosabban ne legyen megállapítható, továbbá adatkezelőnként legalább száz főt eredményező mintát kell venni. A teljes népességre vonatkozó adatbázisok esetében a minta nem haladhatja meg a teljes sokaság 50%-át. A [2] törvényben foglaltak nem alkalmazhatóak a külön törvény által szabályozott minősített adatokra, illetve azokra a közérdekű adatokra, amelyeknek megismerhetőségét nemzetbiztonsági érdekből szintén külön törvény korlátozza.

KÖVETKEZTETÉSEK

A közigazgatási adatvagyon felhasználásának segítése céljából született meg az Európai Parlament és a Tanács 2003/98/EK számú irányelve. Az irányelv minimum szabályokat állapít meg a tagállamok közigazgatási szervei birtokában lévő dokumentumok (ideértve az adatokat is) további felhasználására. Az irányelv céljainak elérését Magyarországon a döntés előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló 2007. évi CI. törvény teszi lehetővé. Ez a törvény és a hozzá kapcsolódó kormányrendelet [18] szabályozza a közigazgatási adatok összekapcsolásának lehetőségeit is. Az adatbázis összekapcsolás folyamatának bonyolultsága mögött – mely az adatkezelőktől független újabb szereplő bevonását és erős kriptográfiai algoritmusok alkalmazását is igényli – elsősorban az európai szinten is kifejezetten szigorúnak számító hazai adatvédelmi előírások állnak.

Hazánkban az adatbázisok összekapcsolására vonatkozó jogi korlátozások a személyes adatok védelméhez kapcsolódnak. Magyarországon a személyes adatok védelmét információs önrendelkezési jogként értelmezik, eszerint személyes adatot felvenni és felhasználni csakis az érintett beleegyezésével szabad. Személyes adat kötelező kiszolgáltatását és felhasználását csak kivételesen és törvényben lehet elrendelni. A személyes adatok védelmére érvényes a célhoz kötöttség elve, miszerint személyes adatot feldolgozni csak pontosan meghatározott és jogszerű célból szabad. Személyes adatot harmadik személy számára hozzáférhetővé tenni csak akkor szabad, ha az erre konkrét törvényi felhatalmazással rendelkezik, vagy az érintett ehhez hozzájárulását adta.

Az adatbázisok összekapcsolása a kért adatok más számára történő rendelkezésre bocsátását jelenti. Az összekapcsolás lehetősége kizárná az érintettet az adatáramlásból, korlátozná abban, hogy adatai útját és felhasználását ellenőrizze. A személyes adatokat is tartalmazó adatbázisok összekapcsolásának jogi feltétele az adatok személyességének megszüntetése (anonimizálása). Az anonimizálás egy olyan eljárás, amelynek eredményeként az egyes adatsorok már nem kapcsolhatóak adott személyhez.

A magyarországi szabályozás az adatkezelőket (még ha kormányzati szervezetekről van is szó!) nem megbízható szereplőnek tekinti. Az összekapcsolás folyamatára megfogalmazott két biztonsági cél (1. az összekapcsolt adatok alanyának védelme, 2. összekapcsolások ismételt összekapcsolásának megakadályozása) megvalósítása érdekében Magyarországon az adatkezelők a tárolt adataikon kívül más adatkezelőktől nem kérhetnek adatokat összekapcsolás céljára. A hazai szabályozás nem engedélyezi azt a szenáriót, miszerint egy adatkezelő a saját személyes adatait összekapcsolja egy másik féltől kapott adatokkal, majd anonimizálja a kapott adathalmazt, amellett, hogy törli az adatbázisából az „illegális”

személyes adatokat. A jelenleginél egyszerűbb - azaz plusz szereplő bevonását nem igénylő rendszer - úgy lenne elképzelhető, ha a személyes adatok védelme tekintetében a közigazgatási szervek megbízhatóbb szereplőnek számítanának (nem az lenne a feltételezés, hogy az elképzelhető legrosszabbat fogják megtenni) és a visszaélés elkerülését, a törvénytelen használatot és a szabályos működést rájuk vonatkozó jogi előírásokkal és megfelelő ellenőrzéssel biztosítanák.

Felhasznált irodalom

[1] Az Európai Parlament és a Tanács 2003/98/EK irányelve (2003. november 17.) a közszféra információinak további felhasználásáról.

[2] 2007. évi CI. törvény a döntés-előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról

[3] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[4] 2003. évi XCII. törvény az adózás rendjéről

[5] 1993. évi XLVI. törvény a statisztikáról

[6] Fleiner Rita – Munk Sándor: Közigazgatási adatbázisok összekapcsolásának biztonsági kérdései. Hadmérnök, VII. Évfolyam 4. szám - 2012. december

[7] 1996. évi XX. törvény a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról

[8] 15/1991. (IV. 13.) AB határozat.

[9] Bérczes A., Ködmön J., and Pethő A. A one-way function based on norm form equations. Periodica Mathematica Hungarica 49, 1 (2004), 1–13.

[10] Jean-Philippe Aumasson: Cryptanalysis of a hash function based on norm form equations. Cryptologia, 33. évf. (2009. Január), 12–15. p. ISSN 0161-1194.

[11] Folláth János: Kriptográfiai hash függvények és álvéletlenszám generátorok. Egyetemi doktori (PhD) értekezés. Debreceni Egyetem, 2011.

[12] Adatbázisok anonimizált összekapcsolását megvalósító rendszer (DBCS) Rendszer biztonsági előirányzat 2009.01.23. www.hunguard.hu/fileok/m003_bizt_eloiranyzat.pdf (2012.11.30.)

[13] Útmutató az IT biztonsági szintek meghatározásához BME IK, 2008.

[14] Adatbázisok anonimizált összekapcsolását megvalósító rendszer (DBCS v1.0) biztonsági minősítése http://www.hunguard.hu/fileok/m003.pdf (2012.11.30.)

[15] Eljárásrend a döntés-előkészítéshez szükséges adatok hozzáférhetőségének biztosítására Verzió: 1.00 Készítette: NKHT 2009.03.10.

[16] MAGYAR KÖZTÁRSASÁG KORMÁNYA T/3029. számú törvényjavaslat a döntés előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról www.parlament.hu/irom38/03029/03029.pdf (2012.11.30.)

[17] 1992. évi LXVI. Törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról

[18] 335/2007. (XII. 13.) Korm. Rendelete a döntés előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló 2007. évi CI. törvény végrehajtásáról

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Jéri Tamás
jeri.tamas@bv.gov.hu

KRITIKUS INTERNETES SZOLGÁLTATÁSOK

Absztrakt

A kritikus internetes szolgáltatások a kritikus infrastruktúrákkal és a kritikus információs infrastruktúrákkal szorosan összefüggő, a világhálón megjelenő szolgáltatások rendszere. Jelen közlemény célja definiálni a kritikus internetes szolgáltatás fogalmát és bemutatni felépítését, továbbá megvizsgálni működésének aspektusait, áttekinteni az általános és a hazai rendvédelmi alkalmazásának lehetőségeit.

The critical internet services are systems of services that appeared on the internet, being connected closely with critical infrastructures and critical information infrastructures. This publication aims to define and describe the concept of critical internet services, and examines aspects of the operation, and a general overview of the possibilities of applying in general and domestic law enforcement.

Kulcsszavak: *Internet, szolgáltatás, információ, infrastruktúra, kommunikáció ~ Internet, service, information, infrastructure, communication*

BEVEZETÉS

Információs társadalomban élünk. A napi gazdasági folyamatokhoz, életvitelünkhöz, hétköznapjainkhoz, munkánkhoz kapcsolódó - információkat hordozó - adatok, valahol a kibertérben, folyamatos elérhetőség biztosítása mellett szervereken tárolódnak. Az informatikai hálózatok előnyeit kiaknázva, mind a költségvetési, mind a piaci szegmensnek érdeke az elektronikus adattárolás, továbbá a már elektronikusan tárolt adatok centralizálása. A kialakult helyzet eredményeként többek között a "pénz/értékpapír forgalom", "levelezés", "repülőjegy", "ügyintézés" szavak jelentése napjainkra átértékelődött és még hosszasan lehetne sorolni azokat a fogalmakat melyek informatikai szolgáltatásként jelennek meg.

A világháló használóinak növekedésével, mindenkinek érdeke olyan, interneten elérhető szolgáltatások működtetése, melyek használatával az emberi energia és idő ráfordítás csökkenthető, ugyanakkor a rendelkezésre állás növelhető és összességében valamilyen profit képezhető.

1. A KRITIKUS INTERNETES SZOLGÁLTATÁS ÉRTELMEZÉSE

Kritikus infrastruktúrák (továbbiakban: KI):

„Kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek *meghibásodása, kiesése vagy megsemmisítése, működésük megzavarása közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon* súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, a közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére." [1]

Információs rendeltetésű Infrastruktúrák (továbbiakban: II):

„Olyan állandóhelyű vagy mobil létesítmények, eszközök, rendszerek, hálózatok, illetve az általuk nyújtott szolgáltatások összessége, melyek az információs társadalom működéséhez szükséges *információk megszerzését, előállítását, tárolását, elosztását, szállítását és felhasználását* teszik lehetővé. Az információs infrastruktúra a fizikai építményekből, berendezésekből, illetve az azokat szakszerűen működtetni tudó szakszemélyzetből áll, mely egy tudatosan tervezett, szervezett és megépített mesterséges környezet az információk feldolgozására, továbbítására vagy felhasználására." [2]

Kritikus Információs Infrastruktúrák (továbbiakban: KII):

„A kritikus infrastruktúrák védelmére vonatkozó európai programról szóló *zöld könyv* szerint: kritikus információs infrastruktúrák közé azokat kell sorolni, amelyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlési hálózat, számítógép hardver/szoftver, internet, műholdak stb.)." [2]

Az Európai Bizottság 2005. novemberében közreadott anyaga [3] és a Zrínyi Miklós Nemzetvédelmi Egyetem Információs Műveletek és. Elektronikai Hadviselés Tanszék kutatói és szakemberei által készített tanulmány szerint:

„A kritikus információs infrastruktúra azokat az infokommunikációs rendszereket jelenti, amelyek önmagukban is kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából (távközlés, számítógépek és szoftver, internet, műholdak stb.)" [4]

Az információs infrastruktúrák a definíciójukban megfogalmazott funkcióikat gyakran internethez kapcsolással érik el, mely részben a végfelhasználók részben pedig az azokat működtető apparátus jól felfogott gazdasági vagy társadalmi érdeke. A nagy távolságok, az utazással járó költségek, s a technika adta lehetőségek a védelmi szféra szereplőinek is

indokolják a valamilyen szintű internethez történő kapcsolódást, melynek egyenes következménye, az úgynevezett kritikus internetes szolgáltatások létrehozása, melyek a szerver-kliens modell alapján, különböző hálózati protokollok segítségével biztosítják a zavartalan információáramlást.

Kritikus Internetes Szolgáltatás (a továbbiakban: KRISZ) minden olyan, a világhálón elérhető informatikai szolgáltatás, mely a fenntartó vagy az igénybe vevő működéséhez szükséges információk megszerzését, előállítását, tárolását, elosztását, szállítását és felhasználását teszi lehetővé és *meghibásodása, kiesése* vagy *megsemmisítése,* működése *megzavarása közvetlenül* vagy *közvetetten, átmenetileg* vagy *hosszútávon* súlyos hatást gyakorolhat a fenntartó működésére, kihathat az állampolgárok gazdasági, szociális jólétére, a közegészségre, a közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.

A hálózati szolgáltatás olyan, az informatikai hálózat valamely dedikált pontján működő tevékenység, mely a hálózat aktív elemei között közvetlenül vagy közvetetten adatcserét tesz lehetővé.

"Az angol „service” szó magyarra fordítva egyaránt jelent kiszolgálást és szolgáltatást. Egymással rokon értelmű szavak, van is közöttük átfedés, azonban főleg az informatikában mégiscsak markánsan eltér a jelentésük. A kiszolgálás egy állandó, ingyenes rendelkezésre állás, míg a szolgáltatás olyan rendelkezésre állás, melynek teljesítése - általában - valamilyen feltétel függvénye." [5]

Egy interneten megjelenő hálózati szolgáltatásból akkor lesz KRISZ, ha a funkciójában megfogalmazott célt folyamatosan biztosítja, tehát kiszolgál, továbbá a szolgáltatás igénybevételére igény mutatkozik. A KRISZ tehát olyan szolgáltatás, amely az elvárt állandó rendelkezésre állás következtében egyben kiszolgálás is.

2. A KRISZ FELÉPÍTÉSE

Tekintettel arra, hogy interneten megjelenő szolgáltatás(ok)ról van szó - a definícióból adódóan - fontos leszögezni, hogy a szolgáltatás igénybevételekor közvetve, vagy közvetlenül információ-, adatcsere történik, melynek egyenes következménye, hogy a kommunikációban felek működnek közre.

A számítógép-hálózatban csak a dedikált aktív eszközök képesek egymással kommunikálni, mely a sikeres kapcsolatfelvétel után valósul meg és a kapcsolat lezárásával végződik. Az eszközök közötti kommunikáció alapfeltételei:

- egymás azonosításának képessége (felismerés),
- kapcsolatteremtő képesség (kérés, válasz),
- közös nyelv ismerete

Ahhoz azonban, hogy a szolgáltatást nyújtó és az azt igénybe vevő fél egységesen reagáljon a kommunikáció során, viselkedési kultúrára, azaz protokollra van szükség.

„Az informatikában a *protokoll* egy egyezmény, vagy szabvány, amely leírja, hogy a hálózat résztvevői miképp tudnak egymással kommunikálni. Ez többnyire a kapcsolat felvételét, kommunikációt, adat továbbítást jelent.” [6]

A „hivatalos szabványos internet protokollok” [7] listája megtalálható a világhálón, melyek nagyrészt lefedik az általános internetes kommunikáció protokolljait, ugyanakkor természetesen lehetnek egyedileg kifejlesztett kapcsolatteremtési és viselkedési formák.

A hálózati protokollokat ismerő és megvalósító szoftverek az úgynevezett szerverprogramok. A szerverprogram hálózati portot nyit a kiszolgáló számítógépen, ezáltal biztosítja a hálózati kapcsolódás lehetőségét, melyhez az ügyfél számítógépére telepített, a szerverprogrammal kommunikálni képes kliens program kapcsolódhat.

Az interneten elérhető, a KRISZ körébe tartozó szolgáltatások jellemzően felhasználó orientáltak, mert alapvető cél az egyszerű kezelhetőség biztosítása. Az igénybe vett szolgáltatás megjelenése számtalan formában előfordul, melyet a szerverprogram és az ahhoz kapcsolódó kliens program együttese határoz meg.

Ahhoz azonban, hogy egyáltalán interneten megjelenő szolgáltatásról beszéljünk, megkerülhetetlen a működéshez szükséges összetevők számba vétele:

1. infrastruktúra
    a) támogató információs infrastruktúra: „Létrehozzák, és folyamatosan biztosítják a funkcionális információs infrastruktúrák nagy halmazainak zavartalan működéséhez és fejlődéséhez szükséges anyagi és szellemi alapokat valamint támogatási háttereket.” [8]
    b) funkcionális információs infrastruktúra: „Fizikailag lehetővé teszik a társadalom valamilyen információs funkciójának zavartalan működését, vagyis infrastrukturális alapon információs alapszolgáltatásokat végeznek.„ [4]
2. hardver
    a) számítógép,
    b) hálózati eszköz(ök)
3. szoftver
    a) kiszolgáló operációs rendszere,
    b) háttér-program(ok),
    c) szerverprogram
    d) kliens program

A hardverre telepített operációs rendszer, háttér-programok és szerverprogram együttesen biztosítják a szolgáltatás szoftver oldali működését. A szerverprogram gyakran csak a jéghegy csúcsa, hisz az alkalmazott protokollhoz igazodó működéssel, csak az igénybe vevő számára fontos végeredményt biztosítja, ugyanakkor az információ előállításához további háttér-program(ok) működését veszi igénybe. A háttér-programok lehetnek saját hálózati port-tal rendelkező - önálló - szerverprogramok, szorosan együttműködő csatolt modulként működő komponens programok, vagy "tényleges hálózati port-tal nem rendelkező TCP-socket primitívvel" [6] működő kiegészítő programok.

Gyakran a végfelhasználást biztosító kliens programok működéséhez is kiegészítő modulok alkalmazására van szükség, mely adott esetben a KRISZ igénybevételének elengedhetetlen kelléke (JAVA futtató modul).

A KRISZ működtetése és igénybevétele összetett és bonyolult, infrastruktúrák, hardverek és szoftverek összehangolt működésének következménye. Fontos kiemelni, hogy egy KRISZ működéséhez szükséges összetevők bármelyikének kiesése a szolgáltatás használhatatlanságához vezet.

3. A KRISZ ASPEKTUSAI

A KRISZ megvalósulása szubjektív. A társadalom szereplőinek igényei, szokásai, kötelezettségei, vagy érdekei egyénileg határozzák meg, hogy egy internetes szolgáltatás beletartozik-e a KRISZ körébe, vagy sem. A működés létfontossága a szolgáltató, vagy az igénybe vevő oldalán egyaránt megjelenhet.

KRISZ fenntartója és igénybe vevője egyaránt lehet:

1. állam-kormányzat;
2. vállalkozás;
3. magánszemély.

A KRISZ előfordulásának lehetséges esetei:

1. állam-kormányzat
    a) szolgáltatóként (magyarorszag.hu)
    b) felhasználóként (e-ügyintézés, e bank)
2. vállalkozás
    a) szolgáltatóként: (e-kereskedelem)
    b) felhasználóként: (e-ügyintézés, e-bank)
3. magánszemély
    a) "szolgáltatóként": (VPN[1] home office)
    b) felhasználóként: (SMTP[2], e-bank)

A KRISZ álláspontom szerint akkor tartozik bele a KI, vagy KII körébe, ha arra felhasználói oldalon a társadalom egészére kiható igény mutatkozik (pld e-ügyintézés), illetve szolgáltatói oldalon közvetve, vagy közvetetten társadalmi érdek a működés (pld. kormányzati email). Egyes esetekben a KRISZ egyformán fenntartói és felhasználói érdek (pld. e-bank), mely nagy valószínűséggel deklarálja, hogy a szolgáltatás a KI/KII körébe tartozik.

KRISZ számos cél érdekében működhet, ugyanakkor a végeredmény mindig ugyanaz, mégpedig az információcsere biztosítása.

Általános rendszerezés szerint, - néhány példa feltüntetésével - KRISZ működhet:

1. hálózati összeköttetés megvalósítása céljából:
    a) létező hálózati szegmens használatára (VPN),
    b) új hálózati szegmens kialakítására (WLAN[3], PPP[4]),
2. hálózati szolgáltatást biztosító szerver szoftveres karbantartása céljából:
    a) WinRM[5] alkalmazására,
    b) SSH[6] használatára,
    c) Apple Remote Desktop[7] elérésére,
3. adatcsere biztosítása céljából:
    a) elektronikus levelek küldésére és fogadására – SMTP,
    b) állományok továbbítására - FTP[8],
    c) szövegek, képek, videók, multimédia objektumok megjelenítésére - W3[9] / HTTP[10]

KRISZ lehetséges funkciói:

1. információs társadalom kiszolgálása;
2. II biztonságos elérhetőségének biztosítása;
3. kormányzati kommunikáció biztosítása;
4. internetes összeköttetéssel működő kommunikációs rendszerek működtetése.

[1] Virtual Private Network - virtuális magánhálózat
[2] Simple Mail Transfer Protocol - levéltovábbító protokoll
[3] Wireless LAN - vezeték nélküli hálózat
[4] Point-To-Point Protocol - pont-pont kapcsolati protokoll
[5] Windows Remote Managment - Windows távoli menedzsment
[6] Secure Shell - biztonságos parancsfuttató környezet
[7] Apple távoli munkaasztal
[8] File Transfer Protocol - állománytovábbító protokoll
[9] Wolrd Wide Web
[10] HyperText Transfer Protocol

4. KRISZ A RENDVÉDELEMBEN

Ahogy Magyarország közigazgatásának működésében is egyre nagyobb hangsúlyt kap az elektronikus szolgáltatások kiterjesztése, úgy a védelmi szférában is folyamatos a tolódás az információs infrastruktúrák használata felé és kimondva- kimondatlanul a jövő feladata békeidőben is a papírmentes információfeldolgozás. Az információtechnológia fejlődése a rendvédelem minden ágában kivétel nélkül kikényszeríttette a gyors és kényelmes eszközök és alkalmazások használatát (pld. email, web, okos-telefon), melyek beivódtak a napi munkavégzésbe, létfontosságú adatok hordozóivá váltak és észrevétlenül lettek internethez kapcsolódó kritikus információs infrastruktúrák

Elektronikus levelezés

A centralizált levelező szolgáltatás a rendvédelem – akár teljes - személyi állománya részére internetes, azaz valós, egyénre szóló levelező postafiókot biztosíthat, lehetővé téve az arra jogosultak számára, hogy - biztonsági megoldások használata mellett - a világhálón küldjenek, vagy fogadjanak elektronikus leveleket, csatolmányokat.

Az email alkalmazásával rendkívül dinamikus irányító rendszer működtethető, a feladatok, utasítások rövid időn belül a legmagasabb szintekről is képesek eljutni a végrehajtókhoz. Az utasítások csatolmányban elhelyezett elektronikus dokumentumba, kézzel aláírt és újradigitalizált esetleg elektronikusan aláírt állományba, vagy az email tartalmi részébe egyaránt elhelyezésre kerülhetnek.

A gyors és kényelmes email használata a hagyományos levelezéshez képest az alábbi változásokat eredményezheti:

- a határidős feladatok (adatszolgáltatások) száma növekedhet;
- a feladatok végrehajtására rendelkezésre álló idő csökkenhet;
- az adatszolgáltatásokban a redundáns adatok száma növekedhet;
- a kommunikációs csatornák száma növekedhet, a szakmai irányítás nagyobb hangsúlyt kaphat.

Az elektronikus levelezés alkalmazása létfontosságúvá vált. Amikor az egyik rendvédelmi szerv levelező rendszere - hardveres meghibásodás következtében – néhány napra használhatatlanná vált, az információáramlás teljesen leállt, a jelentési-, adatszolgáltatási kötelezettségek szinte végrehajthatatlanná váltak, a szervezet működésében információhiány alakult ki.

Web hozzáférés

Ma a rendvédelemben dolgozó irodai alkalmazottak munkaköréhez szinte elengedhetetlen az internet használata. A szolgáltatást általában az információ-technológiával foglalkozó szakterületek web-proxy[11] szerver alkalmazásával biztosítják.

A proxy megoldások több szolgáltatási funkcióra is rendelkezésre állnak, de a legelterjedtebb a web-proxy, mellyel egy belső hálózatból biztosítható, hogy a felhasználók:

- közvetlen web kéréseket ne tudjanak az internet felé indítani;
- a gyakrabban látogatott oldalak tartalmát gyorsabban elérjék;
- csak a munkájukhoz szükséges oldalakat látogathassák;
- nem kívánt adattartalmat ne tudjanak a munkaállomásukra letölteni.

[11] proxy - helyettesítő

A web-proxy alkalmazásának egyik szerepe, hogy a belső hálózatot ne tudják kitenni támadásnak a felhasználók, ugyanakkor használata KRISZ-nek tekinthető, hisz a szolgáltatás leállásával a web használata szünetel az adott szervezeti egységnél.

Web szolgáltatás

Az államigazgatásnak, így a rendvédelmi szerveknek is számtalan tájékoztatási kötelezettsége van a társadalom felé, így többek között a közérdekű adatok ismertetése, melynek legkézenfekvőbb módja az információk saját honlapon történő megjelenítése. A tájékoztatás egy egyirányú folyamat, ha azonban az államigazgatási vagy rendvédelmi szervnek interaktivitást kell biztosítania adott társadalmi csoport részére, akkor a web és a programozott weboldalak megoldást jelentenek.

Például a felsőoktatási intézetek tanulmányi rendszerei az interneten keresztül - is - biztosítják az oktatók és a diákok adminisztrációit, így a tantárgyakkal, vizsgákkal, pénzügyekkel és egyéb tanulmányokkal kapcsolatos ügyintézését. A tanulmányi rendszer elérhetőségét biztosító weblap bevezetését követően beletartozik a KRISZ körébe, hisz leállása komoly károkat okoz(hat).

ÖSSZEGZÉS

A kritikus internetes szolgáltatások, a kritikus információs infrastruktúrák egyik - egyre bővülő - szegmensén megjelenő, létfontosságú kiszolgálások köre. Dolgozatomban elsők között tettem kísérletet a KRISZ definiálására és röviden áttekintettem a működés hátterét. Bemutattam, hogy milyen egymásra épülő, további szolgáltatásoknak kell működniük egy internetes kiszolgálás megvalósításához és rávilágítottam, hogy milyen szubjektív szempontok alapján kerülhet egy szolgáltatás a KRISZ körébe. A hálózati kommunikációt alapjaiban meghatározó protokolloktól kiindulva, áttekintettem a jellemző szolgáltatások körét, valamint azok hétköznapi és rendvédelmi alkalmazását.

Egy-egy szolgáltatást kiragadva, gondolatébresztő szándékkal tértem ki a KRISZ leállásának ismert, vagy vélt következményeire.

Felhasznált irodalom

[1] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

[2] Haig Zsolt–Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005. ISBN 963 327 391 9

[3] Európai Bizottság, *Zöld Könyv egy Kritikus Infrastruktúra Védelmi Európai Programról*, COM(2005) 576, 2005. november 17. (Commission of the European Communities: Green Paper on a European Programme for Critical Infrastructure Protection, Brussels, 17.11.2005 COM(2005) 576 final)

[4] Haig Zsolt, Hajnal Béla, Kovács László, Muha Lajos, Sik Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana http://www.cert-hungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf; (2012.11.05)

[5] Jéri Tamás, Pándi Erik, Jobbágy Szabolcs: A hálózatok világa, Hírvillám, I. évf. 1. szám, Budapest, ISSN 2061-9499 http://193.224.76.4/download/hirado/kiadvanyok/hirvill_1evf_1sz.pdf; (2012.11.05)

[6] Andrew S. Tanenbaum: Számítógép-hálózatok, Panem Kiadó Kft., Budapest 2003.

[7] Official Internet Protocol Standards
http://www.rfc-editor.org/rfcxx00.html; (2012.11.05)

[8] Munk Sándor: Információs színtér, információs környezet, információs infrastruktúra
Nemzetvédelmi Egyetemi Közlemények 2002. 2. sz. ZMNE
http://193.224.76.4/download/konyvtar/digitgy/nek/2002_2/12_munk.pdf; (2012.11.05)

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Kassai Károly
kassai.karoly@hm.gov.hu

AZ ELEKTRONIKUS INFORMÁCIÓVÉDELEM SZABÁLYOZÁSI KÉRDÉSEI A KÖZELMÚLTBAN[1]

Absztrakt

A kommunikációs szolgáltatások gyorsuló ütemű fejlődése szükségessé teszi az elektronikus információvédelmi rendszabályok fejlesztését is. A biztonsági célkitűzések, biztonsági követelmények, védelmi rendszabályok és mechanizmusok rugalmas, naprakész szabályozása kulcskérdés a szükséges mértékű biztonsági szint kialakítása és fenntartása érdekében. A cikk a katonai híradó és informatikai rendszerek elektronikus információbiztonságával kapcsolatos szabályozási kérdések támogatását célozza az utolsó évtizedek szabályozási lépéseinek áttekintésével és a hadtudományi publikációk eredményeinek összefoglalásával.

The accelerated development of communication services requires communication and information system (CIS) security regulations development as well. The flexible and updated security goals, security requirements, protection methods and mechanisms are key issues in order to develop and maintain the appropriate level of security. This article aims the support of regulation the military CIS security by review the main regulation steps in last decades and summarization of military studies about this topic.

Kulcsszavak: *információbiztonság, elektronikus információvédelem, kiberbiztonság, szabályozás ~ information security, electronic information security (INFOSEC, Information Assurance) cyber security, regulation*

[1] A cikk a szerző Nemzeti Közszolgálati Egyetem, felső vezetői katonai tanfolyam évfolyamdolgozatának (2013) felhasználásával készült.

BEVEZETÉS

A Magyar Honvédség bonyolult feladatokat végző szervezetek összessége, mely szervezetek specializált elektronikus adatkezelésének biztonságát egy szabályozóval nem lehet megoldani. A Magyar Honvédségnél a híradó és informatikai szolgáltatások biztonságához szükséges követelmények, feladatok először a híradó, ügyviteli, rejtjelző és informatikai szabályozókban jelentek meg, majd a szolgáltatások bonyolultságot követve az önálló központi szabályozók irányába kezdenek fejlődni.

A növekvő számú szakmai feladatok miatt logikus követelmény, hogy a szabályozókat az érthetőség, nyomon követhetőség érdekében valamilyen rendbe kell rendezni, tartalmilag egymáshoz kell illeszteni, figyelemmel arra, hogy közöttük átfedések ne legyenek, illetve közöttük hiányzó területek ne maradjanak.

A katonai szabályozóknak illeszkedniük kell a nemzeti, NATO és EU szabályozási környezethez, az alkalmazott híradó és informatikai szolgáltatásokhoz, így a szabályozási témák kiválasztásakor figyelembe kell venni a kapcsolódásokat és függőségeket.

E gondolatok mentén a cikk célja a hasznosítható értékek feltárása érdekében az elektronikus információbiztonságra vonatkozó korábbi alapvető követelmények azonosítása, a szabályozási gondolkodás előzményeinek tanulmányozása.

ÁTTEKINTÉS

Az elektronikus adatkezelésre vonatkozó szabályozás az alkalmazott technológiának megfelelően a rejtjelzés, az ügyvitel, a híradás (benne a vezetékes és vezeték nélküli híradás), és az informatika területein azonosíthatók[2] a következők szerint összefoglalva.

Rejtjelzésre vonatkozó megfogalmazások

Kormányzati szintű, rejtjelzésre vonatkozó központi követelmény 1994-ben határozta meg a szervezetek szaktevékenységére vonatkozó szabályozási kötelezettséget, de a keretjellegű szabályozók sajátossága szerint nem határozott meg minden területen pontos követelményeket (a szervezetek közötti együttműködés az eszközök, eljárások szintjén és támogató szervezési lépéseken keresztül valósulhatott meg).

A szabályozási kötelezettség a következő területekre vonatkozott:

- a rejtjelfelügyelet hatásköre, szervezeti és működési rendje, feladatai;
- a vezetői beosztásokat ellátó személyek azonosítása, akik betekintési engedély nélkül is megismerhetnek rejtjeltevékenységgel kapcsolatos információkat;
- a rejtjeltevékenység védelmét előíró különleges biztonsági követelmények;
- a nyilvántartás és ügyvitel részletes szabályai;
- a rejtjeltevékenység ellenőrzésére jogosultakat.

A jogszabály meghatározta, hogy a rejtjelszabályzat kiadásához előzetes hatósági engedély szükséges (Országos Rejtjelfelügyelet). [1.] E követelmények alapján miniszteri utasításban történt a Magyar Honvédség rejtjelfelügyeleti rendjének szabályozása 1995-ben, majd 1996-ban megjelent a „Magyar Honvédség Rejtjelszabályzata”. A rejtjelző szakiratkezelést e mellett önálló utasítás szabályozta, illetve kiegészítéseként a rejtjelző eszközök üzemeltetési utasításai, az egyedi szolgálati utasítások és munkaköri leírások szolgálták a szabályozási feladatokat.

[2] Az áttekintésnek nem célja minden egyes szabályozó azonosítása és értékelése, célként csak a fontosabb tendenciák feltárása tűzhető ki. Az áttekintésnek tartalmaznia kell a kormányzati követelmények azonosítását is, mert e nélkül nem lehetséges a reális megítéléshez szükséges összehasonlítási lehetőség.

Az 1995-ös miniszteri utasítás kijelölte a felelősségi köröket és a tevékenységet (a rendszeresített eszközök üzemeltetése és az ehhez szükséges rejtjeltevékenység; illetve a gazdálkodó szervezeteknél csak eszközfejlesztés, gyártás, javítás és értékesítés történhet). Meghatározta az MH Központi Rejtjelfelügyelet (MH KRF), középszintű vezető szerveknél pedig rejtjelfelügyelet működését. A rejtjeltevékenységet végző rejtjelző szolgálatok a saját katonai szervezet alárendeltségében, de az illetékes rejtjelfelügyelet szakirányításával végzik feladatukat. Az MH KRF és az önálló rejtjelfelügyeletek az Országos Rejtjelfelügyelet szakirányításával végzik feladatukat. [2.]

1997-ben az MH Parancsnoka, Vezérkari Főnöke adminisztratív követelményeket határozott meg az Internet használatáról, benne a rejtjelző eszközök internetes csatlakoztatásának tilalmáról. [3.]

Ügyviteli szakterületű, elektronikus információvédelmet érintő megfogalmazások

Az MH esetében az ügyviteli feladatoknál a nyomtatott formájú adatok kezelése, illetve az elektronikus adathordozók nyilvántartása, felügyelete jelölhető meg szakterületi feladatként, mint: „A számítástechnikai eljárás (nyomtatás) során keletkezett minősített adatot, rontott listát a legrövidebb időn belül az ügyviteli szervnek (aláírás ellenében) le kell adni megsemmisítésre." Adminisztratív szabály, hogy „minősített adatok feldolgozásakor a helyiségben csak betekintésre jogosultak tartózkodhatnak.", illetve „A képernyőn megjelenített adaton a minősítést fel kell tüntetni." Az elektronikus adat is nyilvántartási körbe tartozik: „A minősített adat felírása előtt az adathordozót nyilvántartásba kell venni, kísérőlappal kell ellátni.", az adathordozók is nyilvántartottak kell, hogy legyenek: „a minősített adatot tartalmazó beépített, vagy telepített adattárolót az ügyviteli nyilvántartáson kívül típus és gyári szám szerint a számítástechnikai titokvédelmi felelősnek is nyilván kell tartania.". Az átmeneti másolatok kérdése is szabályozott: „az átmeneti másolatok készítésekor nincs szükség a minősítésre jogosult személy engedélyére, de a másolatot a legrövidebb időn belül nem visszaállítható módon törölni kell.".

Az ügyviteli feladatok mellett a szabályzat a jogszabályban megfogalmazott követelmény szerint meghatározza a minősített adatok elektronikus továbbítására vonatkozó rejtjelzési kötelezettséget. Rögzíti, hogy rejtjelzésre csak jóváhagyott eszközt lehet alkalmazni, illetve ezzel kapcsolatos rendszabály, hogy a vezetési vagy fedőnév és fedőszám táblázatok nem tartoznak a rejtjelzés hatókörébe, az erre vonatkozó megoldások a minősített adatok védelmének körébe tartoznak. Kifejezetten rejtjelzésre vonatkozó követelmény, hogy adattovábbítás csak a rejtjelző eszköz minősítési szintje szerinti, vagy alacsonyabb minősítésű adat esetében történhet, mely rendszabály betartásáért az alkalmazó személy vagy a távbeszélő szolgáltatást igénybevevő személy a felelős. A rejtjelző eszköz engedélyezett szintjét az alkalmazó személyeknek ismerniük kell. [4.][3]

A nem minősített adatok kezelésére vonatkozó iratkezelési szabályzat az iratkezelő szoftver biztonsági kérdéseivel és az elektronikus szervezeti levelező postafiók kérdéseivel foglalkozik, az elektronikus iratokra visszakereshető archiválási követelményt határoz meg, szabályozza az elektronikus irattal kapcsolatos ügyviteli kérdéseket, lehetővé teszi az elektronikus érkező irat átvételének megtagadását kockázat esetén. [5.]

[3] A 2010-ben kormányrendeletben megfogalmazott követelmények alapján az MH-nál is elkészült 2012-ben a minősített adatkezelésre vonatkozó központi Biztonsági Szabályzat (tervezet), mely a bemutatott szabályzat kiváltását célozza. A tervezet az elektronikus információbiztonsági szabályozásra már csak hivatkozik, és kifejezetten csak ügyviteli kérdésekre irányul.

Híradó és informatikai szabályozásban megjelenő megfogalmazások

A szabályozási helyzet objektív megítéléséhez célszerű megvilágítani, hogy nemzeti kormányzati szinten nem minősített elektronikus adatkezelésre vonatkozó általános követelmények jelenleg nem azonosítók. Sspecifikus követelmények jelentek meg pénzügyi, egészségügyi adatok és személyes adatok védelme területén; 1996-ban majd 2008-ban szabványra alapozott – de annak teljesen nem megfelelő –, kormányzati ajánlások kiadása is megtörtént, de ezek kötelező jellegű alkalmazását nem rendelte el jogszabály.[6.] [7.]

Szakmai érdekesség, hogy az állami ellenőrzési feladatokkal megbízott szervezetek informatikai (benne jelentős részben elektronikus információbiztonsági) ellenőrzéseket tartanak, szabályozási hiányosságokat azonosítanak napjainkban is, *de a hiányosságok összehasonlítási alapja nemzetközi szabvány, vagy ajánlás, és nem jogszabályban megfogalmazott követelmény*. Az Állami Számvevőszék elnökének utasítása szerint az informatikai rendszerek ellenőrzése során az ellenőrök vizsgálják, hogy a közigazgatási szervezetnél van-e informatikai stratégia, információ biztonsági politika és informatikai biztonsági szabályzat, és azok figyelembe veszik-e az 1996-os ITB 8-as és 12-es ajánlást, alkalmaznak-e biztonsági osztályokat és kriptográfiai eszközöket.[8.]

Minősített elektronikus adatkezelés esetén az általános követelmények jogszabályban történő egységes megfogalmazása 2010-ben megtörtént, de a keretjellegű megfogalmazáson túlmenően végrehajtást támogató, konkrét követelmények nem azonosíthatók. A minősített adatkezelés területén *megszűnt a NATO, EU és nemzeti adatok védelmére vonatkozó eltérő eljárásrend*. Megjelentek az első kompromittáló kisugárzás elleni védelemre vonatkozó követelmények és megváltozott a rejtjelzésre vonatkozó követelmény és felügyeleti rendszer.

Ezt megelőzően 1999-2010 között a kormányzati szabályozás „kétfokozatú" volt, mert a nemzeti szabályozás mellett megjelent a NATO minősített adatkezelésre vonatkozó követelményrendszer, benne a bonyolultnak tekinthető elektronikus információbiztonsági szemlélet és szabályozás.

Az 1995-ben megjelent minősített adatok kezelését szabályozó kormányrendelet lényegében papír alapú szabályozási szempontokat tartalmazott. Az elektronikus adatkezelés kapcsán csak a hozzáférés korlátozására, az adathordozók nyilvántartásba vételére illetve a rejtjelzési kötelezettségre deklarált szabályokat, az adatkezelésre vonatkozó részletes és végrehajtható követelményeket nem határozott meg, hatósági auditálási vagy akkreditálási feladatokat nem azonosított. [9.][4]

Az eddigiekben vázolt kormányzati követelmények alatti szinten központi szabályozóként azonosítható az 1993-ban kiadott MH Informatikai Szabályzat. A szabályzat szerint a katonai szervezeteknél titkos ügykezelésben is jártas és megfelelő számítástechnikai ismeretekkel rendelkező[5] számítástechnikai felelőst (felelősöket) kell kijelölni. A felelősnek ki kell dolgoznia a Számítástechnikai Védelmi Szabályzatot (SZVSZ), naprakészen kell tartani a számítástechnikai eljárásokba betekintésre jogosultakat, ellenőriznie kell a védelmi előírások betartását, figyelemmel kell kísérni a veszélyforrásokat, és már a tervezési fázisban érvényesíteni kell a titokvédelmi szempontokat.

A szabályzatot a feldolgozott adatok minősítési fokozatának és a katonai szervezet sajátosságainak megfelelően kell készíteni és a parancsnoknak kell kiadnia. A szabályzatban meg kell határozni a felelős és az ügyviteli szerv együttműködésének rendjét. Meg kell határozni a minősített adatok készítésének, feldolgozásának, hozzáférhetőségének,

[4] E „hőskorszak" jellegzetessége, hogy a NATO követelmények honosítására szolgáló első jogszabály *az elektronikus információbiztonsági kérdéseket nem kezelte*, ilyen tartalmú fejezet a kormányrendelet nem tartalmazott. [10.] A helyzet a szakterületet újraszabályozó kormányrendelet megjelenésével 2003-ban változott.

[5] Ez a követelmény a gyakorlatban rengeteg problémát okozott, mivel a „jártasság"-ot a vezetők automatikusan az informatikai állományhoz kötötték. Így az informatikai üzemeltetés biztonsági ellenőrzésének (felügyeletének) felelőssége ugyanarra a végrehajtásban érintett informatikai állományra hárult.

tárolásának, másolásának, felülírásának, megsemmisítésének szabályait. Meg kell határozni továbbá az átmeneti és biztonsági másolatok készítésére, használata, megsemmisítése, valamint a számítógépes vírusok elhárítására vonatkozó előírásokat. [11.]

A vezetékes vagy rádióhíradásra vonatkozó követelmények komplexen tartalmazták a védelmi rendszabályokat, például legkevesebb átkötés, legrövidebb útvonal, vezetékes járőr, jelszavak és jelszámok rendje, hírközpontok őrzése és a beléptetés szabályozása vagy minimális kisugárzott teljesítmény, irányított antenna alkalmazása, minimális adásidő, egyéni billentyűzési jellemzők tiltása, vezetési táblázatok alkalmazása. Részletes, nagy hagyományokkal rendelkező adminisztratív szabályozásnak tekinthető a rádiófogalmi szakutasítás, mely az eljárások között azonosítja a szükséges védelmi rendszabályokat. Kifejezett „híradó biztonsági" területű, önálló központi szabályzat ezek mellett nincs kialakítva.

Az MH-nál az 1999-es NATO csatlakozás okozta azt a változást, ami alapján a biztonsági kérdések elkülönültek az informatikai és híradó szakterületi kérdésektől, másrészt a NATO követelmények szerint megjelent az eddigi szervezeti típusú gondolkodás mellett a szervezeti határokat átlépő hálózati gondolkodás. A minősített elektronikus adatkezelésre ösztönző erővel jelentkezett a NATO követelményrendszer [12.], mert a NATO adatok védelmét a felhasználó és az üzemeltető állománynak közvetlenül a szövetségi követelmények szerint kell, hogy végezze (a jogszabályokban foglalt követelményektől függetlenül). A NATO követelmények gyakorlati adoptálásának negatívumként értékelhető a kezdeti rengeteg félreértelmezés, illetve mesterséges (és gyakran felesleges) nemzeti - NATO elkülönítés, melynek káros hatásait még napjainkban sem sikerült felszámolni.[6]

A NATO követelményeknek való megfelelésnél szakmai érdekesség a NATO/NYEU Központi nyilvántartó és a NATO/NYEU Központi Rejtjelelosztó esete. E központi funkciókkal kapcsolatban egy tárca szintű szabályozási szándék történt 2000-ben.[7] Ezt követően 2009-ben és 2010-ben az ügyviteli és az elektronikus információbiztonsági kérdések kormányrendeletben történő szabályozásakor már említés történik a két funkcióra, megtörténik a tárcavezető miniszter felelősségének kijelölése, de a minősített adatkezelés általános szabályain kívül *részletes működési vagy szolgáltatási követelmények nem azonosíthatók.*

Az MH-nál elektronikus információvédelemre vonatkozó egységes szabályozási szándék 2002-ben kezdődött miniszteri utasítás formájában. Az utasítás az elektronikus információbiztonság szakterületeit a rejtjelbiztonsági, kompromittáló kisugárzás elleni védelmi, átvitelbiztonsági és informatikai biztonsági területekre bontotta. Kijelölte a minisztérium szakfeladatokért felelős szervét, és meghatározta, hogy minden szervezetnél ki kell jelölni az elektronikus információvédelmi szakfeladatokért felelős személyt, vagy szervezeti elemet. A központi szerv feladata az eszközök, eljárások és alkalmazások engedélyezése, a szakfeladatokat végzők számára a képzés és vizsgáztatás irányelveinek kidolgozása, illetve általánosságban szakfelügyelet ellátása, együttműködésben a nemzeti hatósági feladatokat ellátó szervezetekkel.

Az utasítás részletes biztonsági követelményeket, feladatokat nem határozott meg, de ez tekinthető az első olyan szabályozási kísérletnek, amelynek célja egységes, korszerű mederbe

[6] Kivételként kezelendő Király Imre, aki 2002-ben a dokumentumbiztonság helyi szabályozása kapcsán az addigi gyakorlattól eltérően azt írta, hogy „a katonai szervezetek szintjén nem célszerű külön-külön szabályzatban rögzíteni a nemzeti és a NATO adathordozók kezelésével kapcsolatos helyi eljárási szabályokat". [13.]

[7] 4/2000. (II. 29.) HM rendelet és a 13/2000. (HK 6.) HM utasítás a NATO/NYEU Központi Nyilvántartó és a nyilvántartási rendszerről (hatályon kívül).

terelni az elektronikus információbiztonság kérdését és *a korábbi rejtjelzésre koncentráló védelmi szemlélet helyett szélesebb értelmezést kijelölni*.[8] [14.]

Kifejezetten a NATO követelmények adoptálása történt, amikor Váncsa Julianna a NATO Üzemeltetési Biztonsági Szabályzat kialakítására vonatkozó központi segédletet készített 2003-ban.[9] Ugyanígy az ő nevéhez köthető a központi szabályozási kísérlet 2004-ban, amikor a már említett az MH Informatikai Szabályzatba ágyazott elektronikus információvédelmi szabályozás felváltását célozta meg NATO mintát alapul véve, a számítógépes hálózatok és önálló telepítésű eszközök biztonságát komplex módon kezelve (fizikai-, személyi-, dokumentum és elektronikus információbiztonsági szakterületű gondolkodás).[10]

A híradó és informatikai rendszerek biztonságának témakörét is érintette az ellenőrzésekre vonatkozó egységesítési szándék, amelynek megfelelően 2005-ben elkészült a katonai szervezetek központi ellenőrzésére vonatkozó ideiglenes ellenőrzési kézikönyv. A kézikönyvben a szakterületekért felelős szerveknek meg kellett határozni az ellenőrzési szempontokat, illetve az értékelési mutatókat. A mai fogalmakkal elektronikus információvédelem szakterületére vonatkozóan az informatikai, a titokvédelmi és az úgynevezett információvédelmi szakterületen[11] olvashatók ellenőrzési követelmények.

A meghatározottak szerint *informatikai szakterületen* ellenőrizni kell az SZVSZ tartalmát és naprakészségét, az események naplózását és nyilvántartását, az archiválást és az adatmentést.

Titokvédelmi szakterületen ellenőrizni kell az SZVSZ-t és annak felhasználói szintű ismeretét, a számítástechnikai berendezések, eljárások titok és adatvédelmével kapcsolatos előírások betartását, a felelős kijelölését és okmányrendszerét, valamint a felhasználói jogosultságokra vonatkozó követelmények teljesülését. Ellenőrizni kell az SZMSZ-ben a rejtjeltevékenységgel kapcsolatos felelősség, jog- és hatáskör, szabályozottságát. A (helyi) Titokvédelmi Szabályzatnak tartalmaznia kell a rejtjeltevékenységre vonatkozó előírásokat.[12]

Információvédelmi szakterületen ellenőrizni kell az alárendelt szervezetek irányítására, a rejtjeltevékenységre vonatkozó előírások megfelelőségét. Ellenőrizni kell továbbá a béke és tábori vezetési pontokon az információvédelmi eszközök megbízható működését, az elkülönített ügyvitel megvalósulását, a szaküggyviteli szabályok érvényesülését.

A szabályozás területén a következő fejlődési lépcső 2009-ben a honvédelmi tárca információ biztonságpolitika megjelenése,[13] illetve erre építve később alacsonyabb szintű szabályozók kiadása.

A fentiek szerint megfogalmazott rendszabályok és eljárások mellett azonosíthatók még a kiadási formát tekintve azonos elrendelési szintű szabályozók. Erre a teljesség igénye nélkül példaként említhető miniszteri utasítások a NATO Irodaautomatizálási Rendszer (NIAR) biztonsági kérdéseiről,[14] a HM Költségvetési és Gazdálkodási Rendszer (KGIR) üzemeltetésének és biztonságának szabályozása, az Egységes Digitális Rendszer üzemeltetési és biztonsági kérdései, vagy a mobil kommunikációs eszközök biztonsági kérdéseinek szabályozása. Ezekhez hasonlítható szabályozó az MH állandó jellegű távközlő hálózatának békeidejű üzemeltetési és felügyeleti rendjéről szóló vezérkar főnöki intézkedés 2003-ban.

---

[8] Az utasítás a korábban említett 23/1995 (HK 13.) HM utasítást hatályon kívül helyezte.

[9] NATO Irodaautomatizálási Rendszer Üzemeltetés Biztonsági Szabályzat kitöltési útmutató, 2003.

[10] A Honvédelmi Minisztérium és a Magyar Honvédség ideiglenes elektronikus információvédelmi szabályzata (tervezet), 2004. Az ideiglenes szabályozat kidolgozása az első szakmai köröztetés után megállt, a komplex, új szemléletet mutató szabályozási szándék szakterületi támogatások hiányában megszakadt.

[11] Az „információvédelem" kifejezés ebben a szabályozóban egyértelműen „rejtjelzés"-ként értendő, de az akkori szervezeti megnevezések, szokás alapján a „rejtjelzés" kifejezés alkalmazása nem volt gyakorlat.

[12] Ez a követelmény nyilvánvaló átfedés a rejtjelzésre vonatkozó szabályozási követelménnyel.

[13] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról.

[14] A 2002-es szabályozást HM utasítás, Vezérkar Főnöki intézkedés és ezek alapján helyi parancs, valamint a NATO követelmények szerinti rendszer-specifikus biztonsági dokumentumok lépezték.

A híradó és informatikai szakterületen régóta megoldatlan kérdés a szakkifejezések szabályozása, melynek kapcsolódó következménye az információvédelem – szűkebben fogalmazva az elektronikus információvédelem – területén is tapasztalható terminológiai összehangolatlanság. A helyzet rendezésére informatikai szakterületen egy kísérlet történt 2002-ben Munk Sándor vezetésében az akkori ZMNE informatikai tanszék szervezésében, de a megrendezett konferencia és a konferencia kiadvány megjelenéséből adódó hasznon kívül további eredmény nem született.

A jogszabályok értelmező rendelkezésein kívül a szakkifejezések pontos meghatározására a Hadtudományi Lexikon (1995), az önkéntes alapon kialakított Katonai Lexikon 4000, az MH Összhaderőnemi Doktrína (3) által meghatározott rövid fogalomtár, a NATO kifejezések kapcsán pedig a 2012-ben honosított NATO AAP-6[15] állnak rendelkezésre.

A TÉMÁHOZ KAPCSOLÓDÓ HADTUDOMÁNYI FORRÁSOK ÁTTEKINTÉSE

A fontosabb szabályozási lépések bemutatása mellett az eddigi eredmények hasznosítása érdekében célszerű a hadtudományi források lényegi áttekintése is, kifejezetten a 2010-2011. előtti időszakra koncentrálva.[16]

Szabó László 2004-ben az információvédelem tanulmányozása kapcsán a HM szintű fontosabb szabályozók azonosításával rávilágított, hogy a „*szabályozók évszámából is kitűnik egyfajta rendszertelenség*", a szabályozók jelentős része NATO csatlakozás előtti, így nyilvánvalóan nem lehetnek összehangolva a NATO, EU követelményekkel. A nemzeti követelmények területén *a nemzeti elektronikus minősített adatok védelmi kérdése nem szabályozott*, a *rejtjelzésre vonatkozó kormányrendelet túl általános*. A tárcán belüli egységes szabályozási rendszer kialakításának nagy akadálya „*a szervezeti elkülönültségből fakadóan a szakkifejezések nem egységes értelmezése*". A hatékony működés feltételei között fogalmazta meg a szerző az „adat (információ) biztonság *teljes szabályozó rendszerének felülvizsgálata, egységes filozófián alapuló új, átfogó* részletes szabályozók kiadása." követelményt és a továbbképzési rendszer áttekintését, továbbfejlesztését. [16.]

Beinschróth József 2007-ben informatikai területen működésfolytonosság szempontjából vizsgálta az alkalmazható bevált gyakorlat körébe tartozó dokumentumokat és megállapította, hogy *a kérdést taglaló szakirodalom „elsősorban az informatikai biztonságra vonatkozó ajánlásokra támaszkodik"*. Az ITIL,[17] az ITIL-re épülő gyártófüggő megoldások és a COBIT[18] módszertan rövid bemutatása mellett *felhívta a figyelmet az ITIL és a COBIT összehasonlíthatóságára* (megmutatja mely ITIL témakörök fedik a másik ajánlás tartalmi elemeit), illetve utalt arra, hogy NATO szervezeteknél, illetve a brit hadseregnél felismerhető az ITIL alkalmazással kapcsolatos szabályozási szándék. [17.]

Haig Zsolt 2007-es előadásában a nemzetközi szabványokat[19] ismertette, és megállapította, hogy azok „szinte kizárólag az informatika területére koncentrálnak", az ISO/IEC 27000 szabványcsalád tekinthető az első átfogó jellegű szabályozónak. A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság (ITB) ajánlásait tekintve megállapította, hogy azok a kormányzati és a közigazgatási információs rendszerek

[15] NATO Glossary of Terms and Definitions AAP-6 (V). A 2012-ben magyarul megjelenő – egyébként hiánypótlásként értékelhető – NATO szabályozó a szakmai terminológiai helyzet megoldására nem alkalmas.
[16] Az áttekintésben nem szerepelnek a szerző korábbi cikkei.
[17] ITIL: Information Technology Infrastructure Library.
[18] COBIT: Control Objectives for Information and Related Technology.
[19] Ismertetett szabványok: Common Criteria v.2 (ISO/IEC 15408) - Common Criteria for Information Technology Security Evaluation; ITIL v.3 (BS 15000:2000); COBIT4 4.1; és ISO/IEC 27000 szabványcsalád.

biztonságos működtetésének szabályozására születtek, de nem kerültek bevezetésre,[20] majd összegzi, hogy „a szabványok és ajánlások terén látható a törekvés az egységesítésre”, de *a kidolgozók az informatikai biztonságot tekintik szabályozandónak az információbiztonság átfogó szabályzása helyett*. Ennek megfelelően javasolta *egy komplex, infokommunikációs rendszer szemléletű biztonsági szabályozás kialakítását* a kormányzati és a közszféra területén. [18.]

Munk Sándor 2007-ben írt munkájában látható az információbiztonsággal kapcsolatos fogalmak lépésről-lépésre történő megközelítése, alapmodell megjelenítése. A szerző utalt arra, hogy az „információvédelem” kifejezés a múltban más tartalommal bírt (rejtjelzés). A „biztonsági esemény” kifejezés kapcsán kettős jelentés tapasztalható (fenyegetés bekövetkezése az adott objektum sérülése nélkül, vagy bekövetkezett a védendő objektum biztonságának sérülése). Jelentős megállapítás, hogy a biztonság értelmezésénél korábban a védendő objektum az információ volt, míg napjainkban e helyett szélesen értelmezve az információ – információs szolgáltatás – és az azokat biztosító informatikai rendszer értelemben kellene gondolkozni. [19.]

Kerti András 2008-ban megfogalmazta, hogy a szárazföldi csapatok híradásának szervezési elveire vonatkozó szabályzat hatályon kívül helyezése szabályozatlan helyzetet teremtett és cikkében az vizsgálta, hogy helyette egy „infokommunikációs szabályzat”-ot kell kiadni, illetve e mellett szabályozó struktúrát kell kialakítani. A struktúrát az „infokommunikációs irányelv” – a (híradó, információvédelmi és informatikai) doktrínák – és a (híradó, információvédelmi és informatikai szakterületű) szabályzatok rendje képezi. [20.]

Muha Lajos cikkében (2008) vizsgálta a szakkifejezéseket (információbiztonság/védelem, informatikai biztonság, elektronikus információbiztonság/védelem), összefüggéseiket, eredetüket és Munk Sándor 2007-es munkáját hivatkozva jelzi, hogy terminológia területén a tartalmi kérdéseknek elsőbbsége kell, hogy legyen a megnevezésekkel szemben, amit a fordítási problémák bemutatásával is alátámaszt. A szerző „informatikai biztonság” megnevezéssel az MSZ/ISO 27001 szabvány struktúrájához hasonlítható rendszertant mutat be. [21.]

Munk Sándor 2009-es cikkében az új Informatikai Szabályzat kidolgozása kapcsán az informatikai fejlesztés és üzemeltetés területén rámutatott *az új terminológia, szabványok és ajánlások megjelenésére*. Megfogalmazta, hogy *a szabályozás kialakításánál szükség van alapelvek, illetve azokhoz illeszkedő szabályok rögzítésére*. Az alapelveket ellentmondásmentesen kell összeállítani, szükség esetén prioritásokat kell közöttük felállítani, illetve fontos szerepe van az időtállóságnak, beleértve az esetleges pontosítás lehetőségét is. [22.]

Pristyák János 2009-es felsővezetői tanfolyam dolgozatában a kiszolgálás oldaláról közelítve azonosította az MH központi informatikai alapszolgáltatásait és megállapította, hogy „A jelenlegi központi szabályozók elavultak és hiányosak.”[21] A dolgozat átfogóan bemutatja az ITIL és a MOF[22] módszertanokat. Következtetése, hogy *mindkét esetben precíz leírásokra van szükség, a folyamatokhoz mérési elveket és mérőszámokat kell kialakítani*, illetve az, hogy ez a típusú szabályozás átlépi („nem tiszteli”) a szervezeti határokat A szerző javasolja *az üzemeltetés szervezésekor, korszerűsítésekor az ITIL és a MOF módszertani*

[20] A szerző jelzi, hogy a cikk írásakor az ajánlások átdolgozása folyamatban van.

[21] A szerző korábban megállapítja, hogy az informatikai terület működését az 1993-ban kiadott MH Informatikai Szabályzat tartalmazza (röviden ismerteti a benne lévő általános biztonsági követelményeket). Megállapítja továbbá, hogy a NATO, EU minősített elektronikus adatkezelő rendszereket un. rendszer-specifikus dokumentumok szabályozzák, az Üzemeltetési Biztonsági Szabályzat említésénél szerepel, hogy „… a szabályzatra vonatkozó tartalmi és formai követelmény központilag szabályozott.”. További megállapítás, hogy „a honvédelmi miniszter utasításban rögzítette az elektronikus információvédelem általános felelősségi rendjét” (p. 8-9.).

[22] Microsoft Operations Framework (az ITIL nagyvállalati specifikációja).

ajánlások figyelembe vételét, mert az ajánlásokat a szervezetek igény szerint alkalmazhatják, illetve a javasolt a folyamatszemlélet alkalmazása. [23.]

Muha Lajos 2009-es cikkében megállapította, hogy „az infokommunikációs biztonságra vonatkozó ajánlásokat tíz éve nem frissítették, azok elavultak." *A közigazgatásban nincsenek érvényes informatikai biztonsági, infokommunikációs biztonsági követelmények.* [24.]

Talabos Tibor felsővezetői tanfolyam dolgozatával 2010-ben megkezdte a rejtjelzésre vonatkozó 2010-es jogszabály követelménye szerinti szabályozás előkészítését „A HM és MH rejtjeltevékenységének szabályai" címmel, ami a későbbi szabályozási lépések egyértelmű megalapozásaként azonosítható.

Haig Zsolt 2011-es cikkében az információs műveletek sajátosságait, összetevőit tanulmányozta. Az USA Információs Műveletek Doktrína[23] említése mellett azonosítja a NATO hasonló témájú doktrínájában[24] az információs műveletek összetevőit ahol látható, hogy *a korábbiakhoz képest az információbiztonság*[25] *a műveleti biztonság területéből kiválva már önállóan jelenik meg, illetve összetevőként megjelenik a számítógép hálózati műveletek terület is* (Computer Network Operations; CNO). A szerző jelzi, hogy a képességek, eszközök és eljárások azonosítása a doktrínában nem elég pontos, átfedések is azonosíthatók.[26] A magyar Összhaderőnemi Doktrína (2. kiadás) ismertetésekor olvasható, hogy magyar információs műveletek megközelítés összhangban van a NATO szemlélettel. Az új doktrína kidolgozása kapcsán a szerző jelzi a támadó képesség fejlesztésének kérdését, amely területen nem elsősorban a költségigényes megoldásokon van a hangsúly. [25.]

Kovács László – Illés Zsolt 2011-es cikkükben azonosították a cybertér összetettségét, jelezve, hogy a vezeték nélküli tartomány és a vezetékes hálózatok annak egyaránt részei. Megállapítják, hogy *a hatékony felderítést és elemzést nehezíti a szakértők szűkös eszközrendszere, a hatékony kommunikáció hiánya, a szakértők technikai tudásának esetlegessége, illetve a felderítési, nyomozati módszertanok kidolgozatlansága*. Összefoglalásként jelzik, hogy szükség van annak eldöntésére, hogy hazánknak kell-e támadó képességeket fenntartani, illetve ez milyen szervezet feladata kell, hogy legyen. [26.]

ÖSSZEGZÉS ÉS KÖVETKEZTETÉSEK

A fentiek alapján megállapítható, hogy az MH szervezeteinél az elektronikus adatkezelés biztonsági kérdéseinek szabályozására informatikai területen 1993-tól szervezeti szabályozási követelmény szolgál. *Biztonsági célú rendszabályok azonosíthatók híradó és ügyviteli szabályzatokban*. A rejtjelzés szabályozása 1996-tól központi követelmények meghatározását tartalmazó szabályozóban történt.

Közigazgatási szinten kötelező jellegű részletes követelmények, irányelvek, vagy ellenőrzési szempontok nem azonosíthatók, de a megjelent ajánlásokban már megjelent a szabványok alkalmazási igénye.

Az előbbiek alapján megállapítható, hogy az MH elektronikus adatkezelésének szabályozása a jogszabályok követelményeinek megfelelő, de a jogszabályban meghatározottakkal összhangban – főleg a vizsgálati időszakban – nem tekinthető teljes körűnek és részletesnek.

---

[23] JP 3-13; 2006.

[24] AJP-3.10; 2009.

[25] Az információbiztonság a szerző megfogalmazásában a legszélesebb körű kategória (information security), melynek eleme az elektronikus információbiztonság.

[26] A szerző példái mellett szükség van az elektronikus információbiztonság és a számítógép hálózati műveleteken belül azonosított számítógép hálózati védelem (CND) tartalmi tisztázására is, mert „az információs műveleti képességeinek meghatározásakor az egyértelműségre kell törekedni". A cikk összegzésében a szerző kiemeli, hogy „a számítógép hálózatok védelme alapvető fontosságú a hatékony vezetés és irányítás megvalósításához".

A NATO tagság elektronikus információbiztonsági szempontból hajtóerőként értékelhető, mert a jogszabályok alkalmazhatóságától függetlenül[27] megkezdődött az MH-nál a NATO információbiztonsági követelmények alkalmazása. Ezek a változások szervezeti feladatokban történő változásokat is okoztak, mert a volt „számítástechnikai" védelmi kérdések felügyelete ekkor került át az informatikától az akkor „információvédelem"-nek nevezett rejtjelző szakterülethez. Elektronikus információbiztonság területén *a számítógépes hálózatok biztonsága, a kompromittáló kisugárzás elleni védelmi (TEMPEST) kérdések megjelenése egyértelműen támogatták a nemzeti rendszabályok fejlődését*, amely jelenség lassabban, de a rejtjelzés területén is érzékelhető.

Az ismertetett MH szabályozók nemzetközi vagy nemzeti szabványt nem követnek. A *szabályzatok a szabályozási cél szerinti területek mellett jól láthatóan más szakterületekre is kiterjednek*. Ez a szakterületek eltérő feladatrendje miatt jelentősen megnehezíti a rendszabályok pontosításának lehetőségét, ami elavult szabályozást eredményezhet.

Az ellenőrzés egységesítésének szándéka (így az objektivitásra való törekvés) a kiadott ideiglenes szabályzat formájában felismerhető, azonban nyilvánvaló, hogy *az elektronikus információvédelmi kérdések ellenőrzése három szakterület között nem rendezett* (a végrehajtás során nem kevés bonyodalmat okozva).

A jogszabályok a minősített adatkezelést 2009-től egységesítették, de *a nem minősített elektronikus adatkezelés biztonságára vonatkozó követelmények nem azonosíthatók*, illetve *a minősített és nem minősített adatok biztonságának egységes szabályozására vonatkozó közigazgatási szándék sem azonosítható*.

A szakkifejezések kapcsán megállapítható, hogy korszerűségük, illetve más-más szemléletük miatt az említett források az elektronikus információbiztonság, vagy azon belül szűkebb területeken (rejtjelzés, kompromittáló kisugárzás elleni védelem) *nem alkalmasak szakterületi alkalmazásra*.

A szabályozásra vonatkozó *hadtudományi publikációkban megjelent a nemzetközi szabványok, ajánlások megismerésének igénye*, azonosítható az útkeresés, megkezdődött az alkalmazhatósággal kapcsolatos gondolkozás, javaslattétel. *Felismerhető a szabályozási rendben (hierarchiában) történő gondolkozás* az egy-egy szabályzat kiadásának szemlélete mellett. *Megjelent az alapelvek megfogalmazásának igénye is*.

A szabályozási kérdések vizsgálata megalapozza annak kijelentését is, hogy az elektronikus információbiztonság – de tágabban tekintve az információbiztonság és a híradó és informatikai szakterületek – *szabályozási kérdéseinek vizsgálata szegényesen publikáltnak tekinthető*.

Következtetésként levonható, hogy az adatkezelés bonyolultabbá válásával párhuzamosan *megjelent az elektronikus információvédelem szabályozására vonatkozó szakterületi igény is*. A hagyományos értelembe vett katonai „szabályzat"-ban (mint kiadványban) való gondolkodás *a szabályozást rugalmatlanná tette*. A jogszabályok ügyviteli („papír alapú") szemlélete szintén nem támogatta az elektronikus információvédelmi kérdések önálló megjelenését, mely területen a NATO csatlakozással kapcsolatos feladatok jelentettek változást.

A NATO Irodaautomatizálási Rendszerre vonatkozó utasítások kapcsán meghatározható az az igény, hogy a szakterületi kérdések általános szabályozásának támogatnia kell az egyes rendszerek üzemeltetésének és biztonsági kérdéseinek szabályozását. Lehetővé kell tenni, hogy egy központi rendszer specifikus követelmény (érintett szervezetek, hatáskörök és

[27] A NATO (és az erre hasonlító EU) minősített elektronikus adatkezelés szabályozása politika (policy) - direktíva (directive) - irányelv (guideline) logikai vonalon történik. Elektronikus információbiztonság vonatkozásában ez a szabályozási hierarchia tízes nagyságrendű, egymással összehangolt szabályozók halmazát jelenti, melynek magyar alkalmazása napjainkban egy kormányrendelet közvetítésével történik.

feladatok) alapján minden érintett szervezetnél elvégezhetők legyenek a szükséges kijelölések, felhatalmazások.

Ellenőrzési területen az egységes szemlélet támogatása, a rögtönzések elkerülése és az összehasonlíthatóság biztosítása érdekében soron következő feladatnak kell tekinteni a *minél részletesebb ellenőrzési kérdőívek kidolgozását a híradó és informatikai rendszerek védelmi képességeinek azonosítása érdekében*, mely feladat vonatkozik a rejtjelző szakterületre is.

A hadtudományt művelők sok részterületen azonosítottak problémákat. Ennek összefoglalásaként egyértelműen azonosítható a szabványok alkalmazásának igénye, mely területen jelen áttekintés során *nem lehetett olyan megfogalmazást azonosítani, mely az MSZ/ISO 27000-es szabvány alkalmazása ellen érvelt volna*.

A nemzeti követelmények területén a nem minősített és a minősített elektronikus adatkezelés más jogszabályokon alapul és eltérő szabályozási követelményeket határoz meg, ami *fennakadásokat okozhat például különleges jogi helyzetben, ami a Magyar Honvédség szervezetei számára létfontosságú rugalmasságot és gyorsaságot negatívan befolyásolhatja*. Ezen a területen nyilvánvaló *szakterületi feladat az adminisztrációs terheket csökkentő megoldás kialakítása*.

Felhasznált irodalom

[1.] 43/1994. (III. 29.) Korm. r. a rejtjeltevékenységről (hatályon kívül), 7. § (1-2), 8. §, 8. § 7. § (1) (2), 12. §. (5), 16. §. (3), 17. §. (2) és 19. § (1)

[2.] 23/1995. (HK 13.) HM utasítás a rejtjelzés felügyeleti rendjéről (hatályon kívül), 1-3. §.

[3.] 81/1997. (HK 20.) MH PK VKF intézkedés az Internet igénybevételével kapcsolatos titokvédelmi és adatbiztonsági rendszabályok betartásáról

[4.] HM-MH Titokvédelmi és Ügyviteli Szabályzat, Ált/3, 1996, 148, 146, 152, 147, 149, és 111-114. p.

[5.] A Magyar Honvédség egységes iratkezelési szabályzata (Ált/40); 2007; 22. 30. és 54. p.

[6.] Informatikai Tárcaközi Bizottság (ITB) 12. ajánlás, Informatikai rendszerek biztonsági követelményei, 1996.

[7.] Közigazgatási Informatikai Bizottság 25. számú Ajánlása, Magyar Informatikai Biztonsági Ajánlások (MIBA) 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK) 25/1-2. kötet Informatikai Biztonság Irányítási Követelmények (IBIK) 1.0 verzió; 2008. június)

[8.] 6/2011. (X. 7.) ÁSZ utasítása a számvevőszéki ellenőrzésre vonatkozó eljárási szabályok és módszerek alkalmazásáról, valamint azok nyilvánosságra hozataláról, és a végrehajtását szolgáló „Módszertan az informatikai rendszerek kontrolljainak ellenőrzéséhez”, 2004, p. 55, 72. és 91; http://www.asz.hu/modszertan/modszertan-az-informacios-rendszerek-kontrolljainak-ellenorzesehez/it-ell-modsz-2004-02.pdf)

[9.] 79/1995. (VI. 30.) Korm. rendelet a minősített adat kezelésének rendjéről (hatályon kívül), 27. és 31. §

[10.] 56/1999. (IV. 2.) Korm. rendelet a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített, valamint a korlátozottan megismerhető adat védelmének eljárási szabályairól (hatályon kívül)

[11.] A Magyar Honvédség Informatikai Szabályzata, Ált/210, 1993, p. 197. 199 és 200. p.

[12.] 2000. évi IV. törvény az információ biztonságról szóló, Brüsszelben 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről

[13.] Király Imre: A helyi Titokvédelmi Szabályzat rendeltetése, elkészítésének tartalmi követelményei; Új Honvédségi Szemle 2002/9, p. 85.

[14.] 33/2002. (HK 13.) HM utasítás az elektronikus információvédelemről (hatályon kívül), 1-2, 4. p.

[15.] Ideiglenes szakutasítás a katonai szervezetek rendeltetésével összefüggő ellenőrzések követelményeire és értékelési rendjére (Ált/13), 2004; 7.3.1.6, 7.3.2.4, 7.3.5.4, 7.4.1, 7.4.4, 7.6.1, 7.6.2, 7.6.5, és 7.6.6. p.

[16.] Szabó László: az információvédelem továbbfejlesztésnek lehetőségei, 2004, ZMNE, VKT-14 tanfolyamdolgozat, p. 8-9, 37.

[17.] Beinschróth József: a működésfolytonosság kérdése az informatikai rendszerek üzemeltetésére vonatkozó ajánlásokban, Nemzetvédelmi Egyetemi közlemények p. 191, 197-198.
http://portal.zmne.hu/download/konyvtar/digitgy/nek/2005_2/10_beinschroth.pdf

[18.] Haig Zsolt: Az információbiztonság szabályozói és szervezeti keretei; 2007. p. 5, 11.

[19.] Munk Sándor: Információbiztonság vs. informatikai biztonság (A "Robothadviselés 7" konferencián 2007. november 27-én elhangzott előadás kibővített, szerkesztett változata), p. 5, 6, 9 és 19.

[20.] Kerti András: Katonai infokommunikációs rendszerszervezés, Hadmérnök, 2008. június, p. 96-97, 103.

[21.] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, 2008. Robothadviselés Konferencia, p. 139, 147-15
www.portal.zmne.hu/download/bjkmk/bsz/.../4/10_Muha_Lajos.pdf

[22.] Munk Sándor: A katonai informatika alapelvei a Magyar Honvédségben I. (alapok), Hadtudomány, 2009. szeptember, p. 334, 336, és 337.

[23.] Pristyák János: A Magyar Honvédség informatikai rendszere üzemeltetésének megszervezése, ZMNE Kossuth Lajos Hadtudományi Kar, Budapest, felsővezetői tanfolyam szakdolgozat, p. 10, 26, és 34-35.

[24.] Muha Lajos: Infokommunikációs Biztonsági Stratégia, Hadmérnök 2009. március, p. 220.

[25.] Haig Zsolt: Az információs hadviselés kialakulása, katonai értelmezése, Hadtudomány, 2011/1-2. szám, p. 12-28. 24, 25 és 27.

[26.] Kovács László – Illés Zsolt: Cyberhadviselés, Hadtudomány, 2011/1-2. szám, p. 30, 40, és 41.

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Róbert Kovács
kovacs.robert@nbsz.gov.hu

DIVERSITY RECEPTION IN RADIOCOMMUNICATION LINKS

Abstract

The increased throughput capacity needs in wireless audio video and data transmission networks demanded by the information society of the 21st century are satisfied by commonly used, enhanced, digital high bitrate radio transmission technologies. Versatility in conditions of the surrounding enviroment (e.g. physical nature of atmosphere and ionosphere, mobile communications, urban environment, digital transmissions) implies continuous wide range fluctuation in radio channel parameters. To eliminate these negative effects there are some advanced technologies supporting our radio devices in the background. The purpose of this article is to present the fundamentals of one of these technologies namely the not generally known, but everyday used diversity reception technique and to provide a systematic overview of the variety of its application branches.

A 21. század információs társadalmának megnövekedett vezeték nélküli hang-kép- és adatátviteli igényeit általánosan használt, fejlett, digitális, nagysebességű rádiós technológiák biztosítják. A környezeti feltételek (pl. atmoszféra, ionoszféra fizikai tulajdonságai, mozgás közbeni kommunikáció, nagyvárosi környezet, digitális jelátvitel) a rádiócsatorna paramétereinek folyamatos, extrém értékek közötti változását eredményezi. A negatív hatások kiküszöbölésére rádiós eszközeinket fejlett technológiák támogatják a háttérben. A cikk ezek egyikének, a köztudatban kevésbé ismert, ám mindennap használatos diverziti vételtechnika alapjainak bemutatását, szerteágazó fajtáinak egységes rendszerbe foglalását célozza meg.

Keywords: *radio propagation, fading, diversity reception, multipath, signal combining, rádió hullámterjedés ~ fading, diverziti vétel, többutas, jelösszegzés*

1. INTRODUCTION

Nowadays, different types of wireless communications play a very important or an almost essential role in a life of human being of 21st century. In an every day life we are promted to use several kinds of sophisticated communication technologies even when we are not aware at all of doing that. It is really unobserved how we stepped into the age of new high data rate and high quality video broadcasting services like terrestrial digital video broadcasting (DVB-T) or using digital data transmissions embedded in conventional analogue radiobroadcast transmissions. The number of mobile applications is continously growing, e.g. global system for mobile communications (GSM), short message service (SMS), Bluetooth, wireless-Internet connections in our homes are basic services for our digital communication needs. The WIFI, WIMAX, LTE, HSPA are also technologies which are wellknown and available at relatively affordable costs for masses of people.

But, a question may be raised, e.g. what factors made it possible to develop and deploy these new techniques? Of course, the answer is not simple because these new enhancements could not have been acheived without a sort of developments in communication technologies. As a frequency spectrum is limited, it is not easy to provide higher data transmission rates at a given bandwidth which is inevitable for the new requirements. Improvements in spectral efficiency, using digital modulation, coding algorithms, electronic circuitry technology led to the necessity to cope with the challenges mentioned. Besides these segments a new approaches were also necessary the give answers for challenges of theory originated from the nature of wave propagation. One of these features is the diversity reception technique, which has been used in almost all segments of wireless communication applications to combat unlovely behavior of radio propagation.

2. WHY DIVERSITY ? – RADIO PROPAGATION BACKGROUND

The technical literature concerning radio propagation is quite extensive therefore hereby the most important related propagation issues are only mentioned, mostly based on [1].

RF signal transmission between two antennas commonly suffers from different factors that affects performance significantly.

The power loss in space as a power loss between transmitter and receiver is a result of three different phenomena. These are the distance-dependent decrease of the power density called *path loss* or *free space attenuation*, the *absorption* caused by the molecules in the atmosphere of the earth and *signal fading* caused by terrain and weather conditions in the propagation path. Path loss is a theoretical attenuation which occurs under free line of sight conditions and which increases with the distance between the transmitter and receiver. The frequency dependent atmospheric absorption is due to the electrons, uncondensed water vapour and molecules of various gases. In frequency domain it has two quite high peaks at 60GHz and 21GHz for oxygen and water vapor respectively.[1]

Fading is an attenuation that varies between a maximum and minimum value in an irregular way. It has two forms which are of different origin.

The *shadow fading* is an effect that is of main importance in mobile communication links. As mobile terminals move through different surrounding areas (urban, rural, mountains, buildings) occasionally, these obstacles will shadow or completely cut off the signal. The consequences of such shadowing effects will depend on the size of an obstacle and on the distance to it, the received signal strength will inevitably vary. It is possible to decrease the effect of shadow fading with some awareness in network planning. By placing the transmitter

and receiver stations as high as possible or close to each other it is possible to avoid some obstacles in transmission.

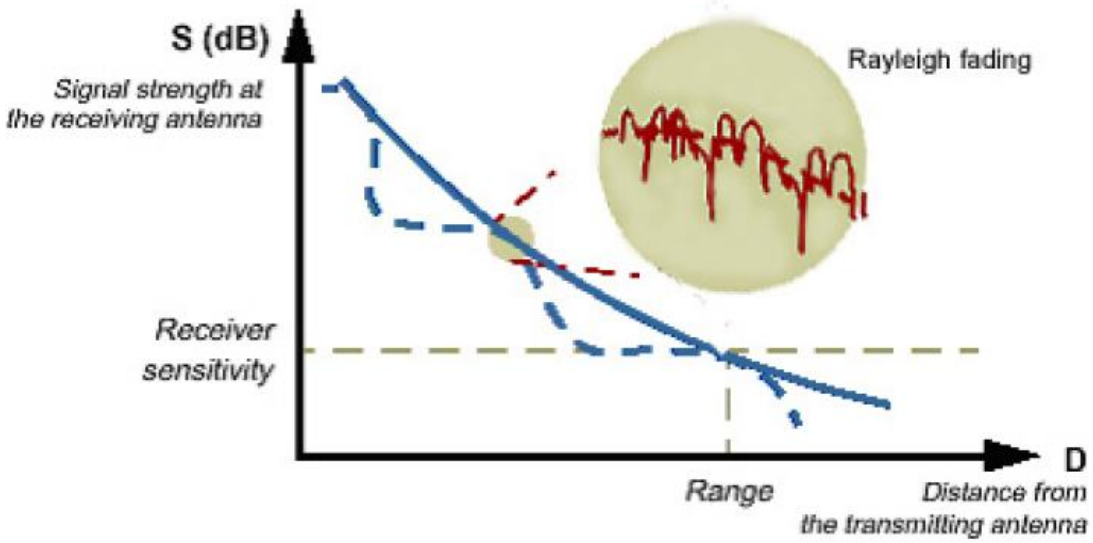


Figure 2.1. Shadow and Rayleigh fading

Source: http://www.es.lth.se/teorel/Publications/TEAT-5000-series/TEAT-5064.pdf (26/01/13)

The much more unpredictable power loss in communication links is a *Rayleigh fading, multi-path fading* or *short term fading*.

It is a result of a reception of a signal at the receiver reflected from many different objects and directions in the area which is illustrated by Figure 2.1. As different paths the waves are coming at different angles, the incoming signals of same origin will usually not be in phase at the receiver, therefore they will reinforcing or even extinguishing each other.

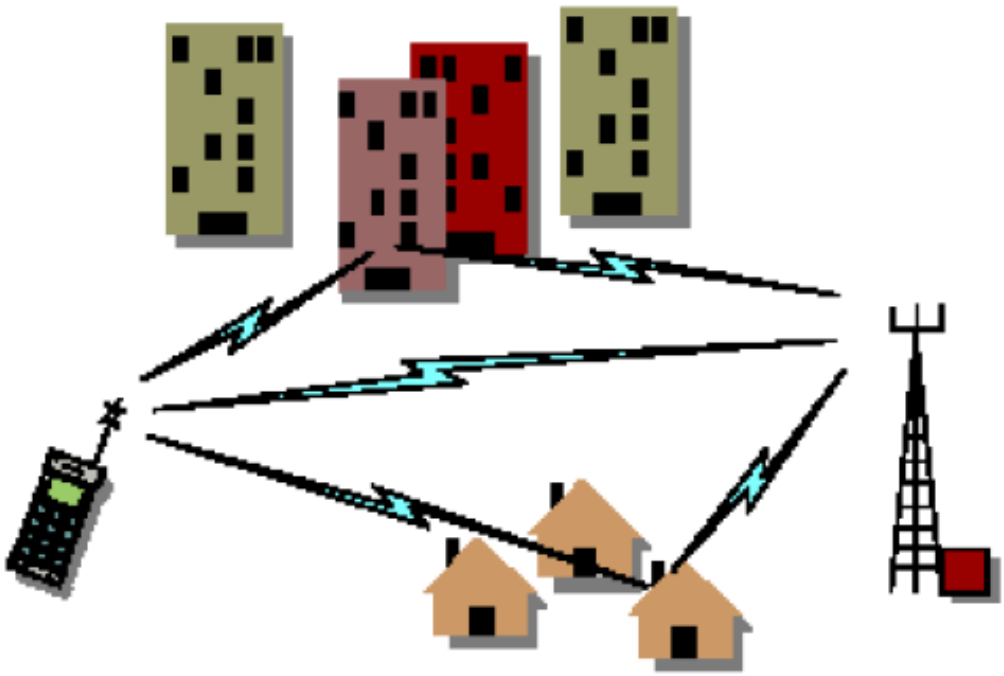


Figure 2.2. Multi-path propagation

Source: http://www.es.lth.se/teorel/Publications/TEAT-5000-series/TEAT-5064.pdf (26/01/13)

The movement of the mobile terminals causes continuous and unpredictable variations of the signal phases over time, making the overall attenuation in the link very variable with extremely high values (fading dips). Rayleigh fading is most perceptible in urban areas involving irregular signal strength variations. Dips will occur more frequently at higher frequencies and more rapid mobile movement.

To overcome this phenomenon is also important in high frequency band communications links where the reflection from the different layer heights of the ionosphere also results in a severe multi-path propagation circumstences.

3. DIVERSITY RECEPTION AT GLANCE

As explained above the quality of the communication radio link can be poor, particularly in urban environments. In such environments this propagation phenomenon affects the signal-to-noise ratio (SNR) and introduces signal distortion. This altogether results in a poor audio signal for analogue systems and a high bit-error rate for digital communications systems. In order to diminish the vulnerability of mobile systems against the destructive interference of multipath radiowaves, special reception techniques can be applied to merge the „original" and the reflected signals decreasing or eliminatig the data losses coming from the amplitude and phase differences of the signals. [2]

According to [1] the performance degradation shown in the difference between the mean signal-to noise ratio and non-fading signal can be solved by increasing the transmitting power and resizing the antenna, however the economical aspect of these solutions, especially for the small terminals, is not that attractive.

To overcome all these problems in order to enhance the signal quality special reception and transmission techniques are used, amongst them the multiple receiver combining techniques known as *diversity*.

4. TYPES OF DIVERSITY RECEPTION TECHNIQUES

The definitions and classifications of diversity reception can be found in several papers (e.g.: [1], [2], [3], [4], [5], [6], [7], [8], [9], [10]).

Basicly, the main purpose of using diversity is to improve the reliability of the analogue or digital message content in radio connections. To acheive this there are several methods to distinguish between the multi-path signals. Common base of the concepts is to separate the multi-path signals as individual channels experience different levels of fading and interference. [3] For this several approaches are known. The channel separation as an essence of the diversity can be carried out in different domains (e.g. space, frequency, phase (time), polarisation, angle of arriving or even modulation and code distance for digital signals).

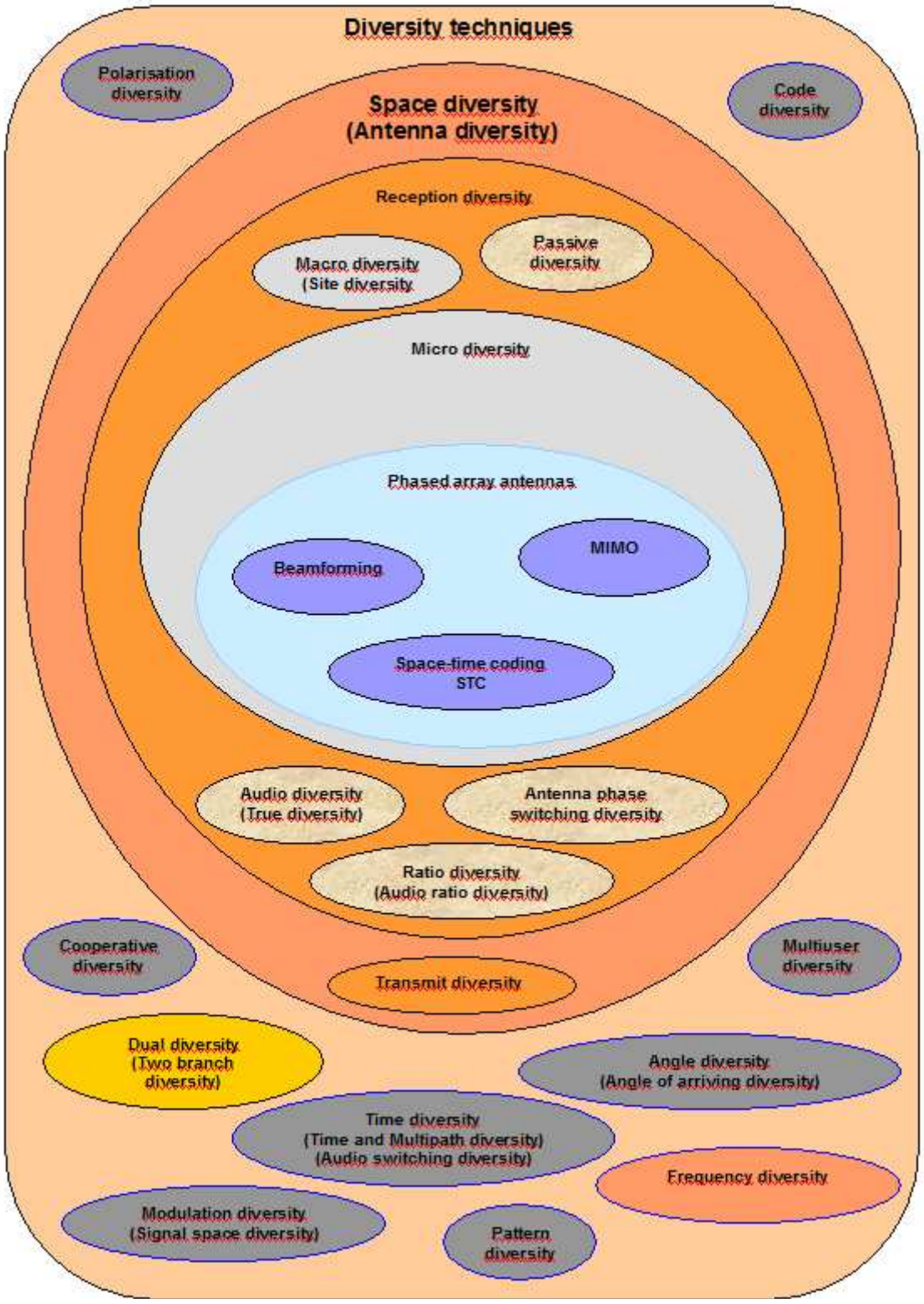


Figure 4.1. Scheme of diversity reception techniques

There are several possibilities to approach the classification of diversity techniques (Figure 4.1.) The basic case is the consideration of the mechanism how the independent fading signals are being produced in domains. Another possibility is to examine the method of linear combining of the signals received. The scheme above represents the first because it is more

detailed and more informative therefore in the explanation below this method will also be followed. The latter one is discussed in Chapter 4.4.

4.1. Space diversity

As the most common and probably the simplest mechanism for achieving diversity branches *space, spatial* or *antenna diversity* as a traditional way of diversity uses multiple antennas separated by a distance from each other. As it is mentioned in [7] as a definition for space diversity, ***"r****adio reception involving the use of two or more antennas located several wavelengths apart, feeding individual receivers whose outputs are combined; the system gives an essentially constant output signal despite fading due to variable propagation characteristics, because fading affects the spaced-out antennas at different instants of time*".

This statement summarizes the nature of antenna diversity though sometimes there might be some overlapping among diversity classes.

Considering semibranches of space diversity, depending on the side the antenna multiplication is used (transmitter or receiver) we can differentiate *transmit* diversity and *reception* diversity respectively. [3]

Using two antennas (called *dual* or *two-branch* diversity [5]) at the receiver with a distance between them the phase delay makes multi-path signals arriving at the antennas differ in fading. The minimum spacing required for sufficient low correlation between fading signals is usually some 0.5 wavelengths. When spacing is smaller than 0.5 wavelengths other diversity mechanisms will have strong influence. [1] According to [4], by placing two receivers (with 2 separate antennas) at a sufficient distance from one another, multipath will become uncorrelated between both receivers. Thus, statistically, the chance for destructive fading at both ends decreases significantly.

Based on the antenna separation if the distance between the antennas is in order of one wavelength, this is called *microdiversity*. If the antennas are well separated (at several wavelength distance) the terms of *macrodiversity* or *site diversity* are used. [3]

There is a special case of antenna arrays considered as a set of antennas close to each other and used for *MIMO* (Multiple Input Multiple Output) channels, *space time coding (STC)* and *beamforming* techniques can be considered as a part of microdiversity. [3]

Of course, beamforming with a standalone antennas far apart (specially at higher frequency band) can be considered as a macrodiversity application as well. (This option is not indicated in the scheme.) It is necessary to mention that MIMO technology can also be considered as both transmit and reception diversity type and there are also some applications where even in HF band researches are executed to study the effectiveness of diversity in *array processing*. [11]

4.2. Frequency diversity

Frequency diversity is based on a supposition that the same signal transmitted on different frequencies simultaneously will not suffer the same fading on each frequency carriers. Depending on the number of frequencies this mechanism need multiplicativ number of transmitters and receivers and frequency bandwidth as spectrum usage as well. This method became wellspread in OFDM modulation systems and spread spectrum technologies (e.g. WIFI and WIMAX).

4.3. Other branches of diversity reception

As it is shown in Figure 4.1 there are several other terminologies used in wireless communications. These would be the followings:

In the case of *polarization diversity* the signal is transmitted over antennas of different polarization. On the receiver side two receivers and a combinig technique are needed to obtain the signal.

The fundamental of *angle* or *angular diversity* is that signals coming from different directions will suffer different and independent level of fading. Using receiver antennas capable to form a direction sensitive pattern, it is possible to acheive diversity gain in the system.

Time and multi-path diversities are related mechanisms mostly applicable in digital transmission. *Time diversity* is achieved by transmitting the same bit of information repetitively at short time intervals. Fading variations for these different repetitions of a signal will be independent. *Multi-path* diversity is using time diversity in multi-path environments getting the information from repetitive signals traveling different paths. [12]

Pattern diversity can be achieved when patterns of two diversity antennas are compared. When using two different antennas, the radiation patterns are different so the signals arriving at the antennas will be from different directions and uncorrelated. Pattern diversity is never applied alone, it usually appears in addition to space diversity. [13]

As a definition of *multiuser diversity* in [14] we can find the followings:

"Multiuser diversity is a diversity technique using user scheduling in multiuser wireless channels where user scheduling allows the base station to select high quality channel users so as to transmit information through a relatively high quality channel in time, frequency and space domains based on the channel quality information fed back from all candidates UEs."

It means that the users in the system communicate simultanously and each of them have different and variable time-slots in the communication channel. The multiuser diversity gain can be obtained by letting the user with the best instantaneous channel quality to communicate. A fundamental property of multiuser diversity is that the more users that are available, the higher expected channel quality of the best user. [15] Further descriptions are available in [16], [17] and [18] respectively.

Through *cooperative diversity*, sets of wireless terminals benefit by relaying messages for each other to propagate redundant signals over multiple paths in the network. This redundancy allows the ultimate receivers to essentially average channel variations resulting from fading, shadowing, and other forms of interference. [19]

A very challenging method of increasing the diversity order is the *signal space* or *modulation diversity*. Using a multidimensional rotating of constellations of digital modulations as QAM is investigated in enhancing the throughput capability of transmission channels with high spectral efficiency.

There are some classifying approaches studied in [6] for *passive diversity*, *antenna phase switching diversity, audio switching diversity* and *ratio diversity*. As their definition of deployment models are explained in details there, thus this article does not discuss them. For reasons of simplification it can be assumed that these diversity types belong to a branch of reception diversity methods. The main difference between those systems is the nature and place of combining decision made in the structure of receiving process.

4.4. Combining techniques

Using diversity reception there are several signal combining techiques to use in order to counteract small scale fading. The method of istantaneously selecting between the multipath signals to acheive improvement in the output signal of the receiver is called *diversity combining*.

Assuming that signal fading behaviours at each particular antenna tend to be independent and the output signals are uncorrelated linear combining techniques are used to derive an output signal with better parameters than any of particular multipath signals.

The most common combining techniques are selection combining (SC), maximum ratio combining (MRC), equal gain combining and switch and stay or switch combining (SSC).

In *selection combining* instantaneously the stronger (i.e. the signal with the greatest signal to noise ratio) is selected. *Switch combining* uses switching when SNR of one signal falls below a certain signal threshold. (Figure 4.2.)

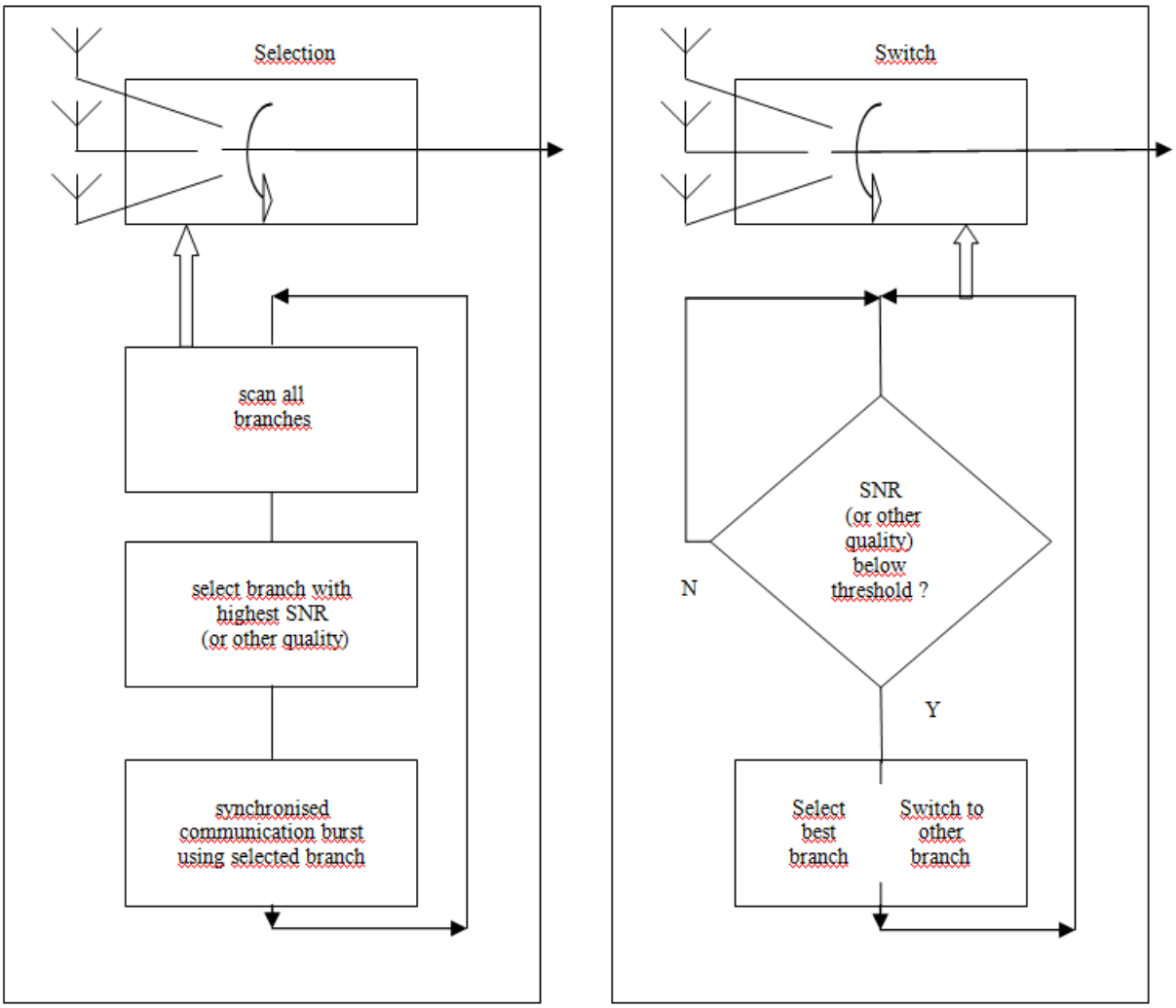


Figure 4.2. Selection and switched combining [1]

While *equal gain combining* adds the signals when they are in phase, *maximum ratio combining* obtains the weights of the SNRs. MRC is therefore the most sofisticated method but produces the best result in terms of output SNR.

There are also some other combining methods used in diversity reception (e.g. *feedback* or *scanning* diversity), where the signals are scanned in a fixed sequence and the selected signal above given threshold performs the output until it falls below the threshold.

The processes mentioned above are sometimes used in combination, but mostly out of the scope of terrestrial communication links. [1], [8], [10]

5. SUMMARY

The purpose of this article was to present the fundamentals of diversity reception techniques. By representing the main factors like path loss, and fading that affect the performance of the radio propagation channel, a focus was put on the definition of diversity reception. Studying the technical literature related to diversity reception techniques, diversity branches were overviewed in details to describe their specifity.

It has been concluded that several approaches are available to distinguish between different types of diversity. It has been pointed out that the channel separation as an essence of the diversity can be carried out in different domains e.g. space, frequency, phase (time), polarisation, angle of arriving or even modulation and code distance for digital signals. As most spread technical solutions, space and frequency diversities has been described.

Finally, the basic types of signal combining techniques like the most common selection combining (SC), maximum ratio combining (MRC), equal gain combining and switch and stay or switch combining (SSC) have also been introduced.

As a main achievement of this paper diversity branches were summarized in a visual scheme to illustrate the versatility of the technology and the variety of its branches.

References

[1] Vanja Plicanic: Antenna Diversity Studies and Evaluation. Master of Science Thesis, Department of electroscience, Lund University, Sweden http://www.es.lth.se/teorel/Publications/TEAT-5000-series/TEAT-5064.pdf – (2013.01.26.)

[2] [P. Mattheijssen, Matti H. A. J. Herben, G. Dolmans, L. Leyten: Antenna-Pattern Diversity Versus Space Diversity for Use at Handhelds. IEEE Transactions on Vehicular Technology, 4 Vol. 53 (2004) 1035-1042 http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1541759&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1541759 http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.60.8790 – (2013.01.26.)

[3] Wikipedia Diversity scheme http://en.wikipedia.org/wiki/Diversity_scheme – (2013.01.26.)

[4] Space and Frequency Diversity Ceragon Newsletter, December 2008. http://www.ceragon.com/newsletter_page.asp?id=32 – (2013.01.26.)

[5] Adam Farson: Note on dual-diversity reception with the IC-7800 http://www.ab4oj.com/icom/ic7800/7800div.html – (2013.01.26.)

[6] Wireless Microphone Systems: Diversity Reception http://www.download.n7tgb.net/Misc/wg_diversity.pdf – (2013.01.26.)

[7] The Free Dictionary: Space diversity reception http://encyclopedia2.thefreedictionary.com/space+diversity+reception – (2013.01.26.)

[8] L. C. Godara, Handbook of Antennas for Wireless Communications. CRC Press, 2002. Receive Diversity http://www.comm.utoronto.ca/~rsadve/Notes/DiversityReceive.pdf – (2013.01.26.)

[9] Joseph Boutros, Emmanuele Viterbo: Signal Space Diversity: A Power- and Bandwidth-Efficient Diversity Technique for the Rayleigh Fading Channel. IEEE Trans. Inform Theory, Vol. 44. No. 4, july (1998) 1453-1466 http://www.ecse.monash.edu.au/staff/eviterbo/papers/itjul98s.pdf5 – (2013.01.26.)

[10] M. K. Simon, M.-S. Alouini: Digital Communication over Fading Channels, 2nd ed. New York: Wiley, 2005

[11] http://www.antenna-theory.com/arrays/diversity.php – (2013.01.26.)

[12] Schwartz M., Bennet W.R., Stein, S., Communication Systems and Techniques, Vol.4, McGraw-Hill Book Company, US 1966

[13] Sulonen K., *Evaluation of Handset Antenna Configurations*, Dept. of Electrical and Communications Engineering, Helsinki University of Technology, March 1999

[14] http://humancommunications.wikia.com/wiki/Multiuser_diversity – (2013.01.26.)

[15] http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5165300&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F7693%2F5165281%2F05165300.pdf%3Farnumber%3D5165300 – (2013.01.26.)

[16] http://www.eecs.berkeley.edu/~dtse/ima810.pdf – (2013.01.26.)

[17] www.web.njit.edu/~simeone/p776seven.ppt – (2013.01.26.)

[18] www.kth.diva-portal.org/smash/get/diva2.../FULLTEXT01 – (2013.01.26.)

[19] http://www3.nd.edu/~jnl/pubs/thesis.pdf – (2013.01.26.)

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Róbert Kovács
kovacs.robert@nbsz.gov.hu

THE HISTORY OF FIRST HIGH FREQUENCY DIVERSITY RECEPTION TECHNIQUES

Abstract

In the early 1900s, as improvement of radiocommunications technology had provided solutions for longwave and later, shortwave communications links, it was inevitable to discover and investigate the propagation anomalies experienced in high frequency bands. The recognition of fading behaviour and its independent characteristics in space, time and polarization straightly led to a development of special receiving techniques using more than one receiver inputs simultaneously and combining them to achieve improvements in signal quality, called diversity. The pioneer's way from the unique technical solutions to receiver prototypes ready for mass production is introduced in this article.

Ahogyan az 1900-as évek elején a rádiókommunikációs technológia fejlődése megoldásokat kezdett kínálni a hosszúhullámú, majd később rövidhullámú összeköttetések számára, elkerülhetetlenné vált a terjedési anomáliák felfedezése és tanulmányozása a rövidhullámú sávokban. A fading jelenségének, valamint tér-, idő- és polarizációfüggetlen viselkedésének felismerése, a vett jel minőségének javítása érdekében egyenes utat képezett az egyidejűleg több vételi ágat és azok közösítését alkalmazó, diverzitinek nevezett vételtechnikai módszer kifejlődéséhez. A cikk az egyedi műszaki megoldásoktól a sorozatgyártásra alkalmas prototípusokig vezető utat mutatja be.

Keywords: *space diversity, multi-path propagation, fading, XG1E receiver, DD-1 Skyrider receiver ~ térdiverziti, többutas terjedés, féding, XG1E vevő, DD-1 Skyrider vevő*

1. INTRODUCTION

Different layer heights of the ionosphere have always resulted in a severe multi-path radio propagation circumstances. Especially in high frequency band different types of fading occur. The transmitted skywave signals follow different paths through the ionosphere differing in direction and length. Sometimes these deep fades may last for half a minute or more, causing the signal received to drop below noise level, thus a long stream of information flow may be lost until the signal level increases above noise level again. Besides that, another type of fading also occurs as a result of several waves from the same transmitter are refracted through the ionosphere, causing distortion on signals. The refraction of signals leads to additional phenomena, as the radio waves suffer rotation through ionosphere producing changes in their polarization.

The first theorethical and practical studies of the phenomena above are almost as old as commercial and amateur HF radiocommunications and were firstly executed on an experimental basis as early as the first quarter of the twentieth century. This work is intented to give a historical overview of results acheived at that early age in recognising and identifying the phenomena and finding the initial technical solutions to mitigate them with a receiver techniques called diversity reception.

2. THE PIONEER AGE OF DIVERSITY RECEPTION

The story of diversity reception started in the early 1920s, when two engineers working for the Radio Corporation of America (RCA), Harold. Henry Beverage and his associate, H. O. Peterson, known for their pioneering research in early radio, began investigating the circumstances of fading. Their interest focused on the actual happenings of the signal received through fading channel. The two engineers were monitoring and comparing the same transmitter signal as received from two different locations simultaneously. They set up experiments with receiving antennas spaced initially some fifteen kilometers apart. By stages, they decreased the separation to only 800 meters away. [1] By monitoring from Peterson's home and from the RCA station site connecting them via telephone line, Beverage and Peterson noted that each station received the same transmitted signal with different fading characteristics. Based on further tests the minimum distance of the receiving antennas was found to be as little as 100 meters. This was the base to invent the space diversity in 1926. [2], [3], [4]

Beverage and Peterson first connected strip-chart recorders to a combination of three antennas and three receivers. The charts showed that the transmitted signal was received at different amplitudes and different phase at the antennas. Searching for the reason of the phenomenon the two engineers speculated that radio waves were being refracted in the ionosphere at different angles and therefore some wave-angles would miss the antenna. They multiplied the number of receiving antennas in order to capture more wave angles, but actually they found the opposite happened. The use of larger antenna arrays caused degradation in fading effect. The two men then theorized that over the horizon radio waves could be simultaneously refracted from different heights in the ionosphere, thus travelling different paths and therefore arriving at the single receiving antenna at slightly different times. They realized that the effect of multiple phases would result in strong fluctuating in the received signal strenght. They also established that since the ionosphere was nearly always in a changing state, fading was always going to be present. To eliminate the negative effect of fading they used receivers with at least a full wavelength of antenna separation and equipped them with separate antennas to provide the necessary isolation. This structure suplemented with the use of second detector made possible to eliminate the effect of phase differences after

converting the signal to audio level. Perfecting the system they were also the firsts to use an operational AVC (Automatic Volume Control) and Tone Keyer, which supported the diversity receiving of CW signals. [2]

Beverage and Peterson, while working at Riverhead, NY, installed the first space diversity stations for reliable, long-distance communication. As a result of these observations, the RCA Diversity Receiving System was developed. [5]. (Figure 2.1)

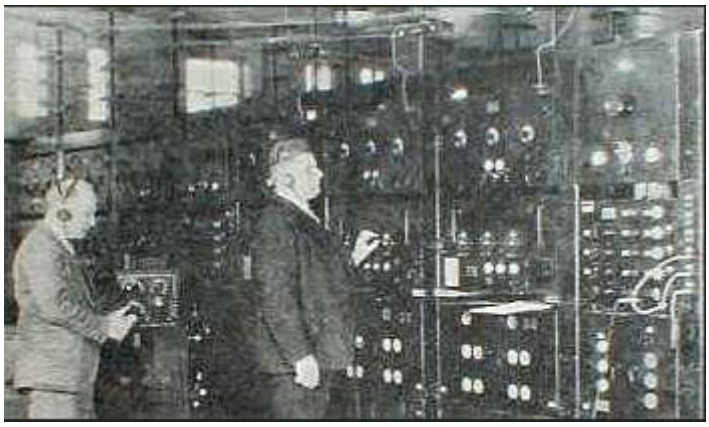


Figure 2.1. H.O. Peterson and H. H. Beverage and their triple diversity HF receiver (1933)
Source: http://www.radioblvd.com/DiversityDD1.html (23/02/13)

By the late twenties, RCA had 41 triple-diversity receivers with associated antenna farm, with 300 meters of separation between antennas installed at Riverhead in communications with 26 different countries. These inventions related to diversity made up the bases of several of Beverage's adopted patents. [6]

By the 1940s, the diversity stations became more sophisticated. RCA had introduced its AR-88 receiver which was adapted to the new triple-diversity receiver, the DR-89 (Navy designation RDM.) These two meter tall racks contained three AR-88 receivers.

Even more complex was the military RCP and RBP-1, also built by RCA for the Navy during World War II. The RCP used double conversion receivers with multiple tuners installed in four racks. The RBP-1 was a dual-triple diversity receiver (six double conversion receivers) that was essentially two RCPs side-by-side. The entire setup weighed not less than about 1500 kgs. The RBP-1s were still in use as late as the 1970s. (Figure 2.2)

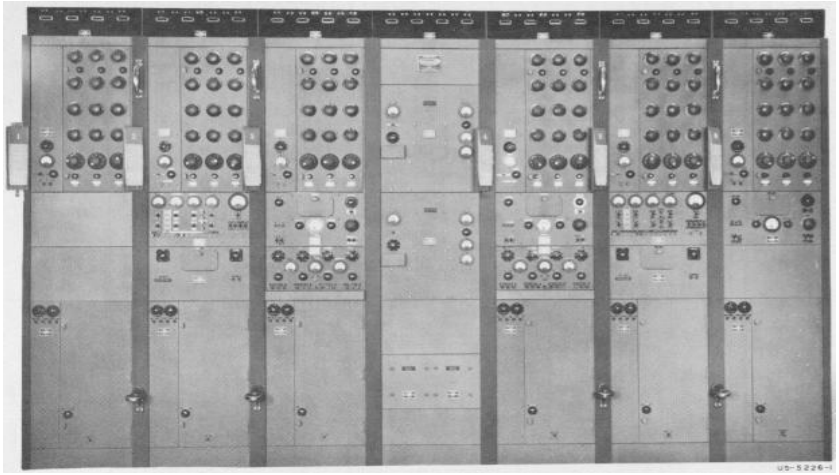


Figure 2.2. The RBP-1 dual-triple diversity HF receiver (1945)
Source: http://www.navy-radio.com/manuals/rbp/rbp-fig1.jpg (23/02/13)

From the beginning of the fifties, besides space diversity the first attempts of frequency diversity were also presented in teletype installations. Presuming that two different frequencies would rarely fade together, in this applications one frequency and receiver was used for „mark" and another set for „space". The Collins Radio Company manufactured about 20.000 receivers of this type for the US Armed Forces under the name R-388 and R-390. [2] , [7] (Figures 2.3 and 2.4.)

Figure 2.3. Collins R-388 HF diversity receiver (1951)
Source: http://www.virhistory.com/navy/rcvrs/r388.htm (23/02/13)

Figure 2.3. Collins R-390 HF diversity receiver (1950)
Source: http://www.radioing.com/collins/rx08.html (23/02/13)

From the early 1940s, if a full wavelength of antenna separation wasn't practical to apply, an initial form of polar diversity also appeared. There are some printed sources available featuring a solution which used both horizontally and vertically oriented antennas for receiving with only one receiver. Using a 400 Hz switching between the antennas the switching gave an additional modulation to the signals that made the use of BFO-s (Bit Frequency Oscillator) redundant.

3. EARLY RADIOAMATEUR APPLICATIONS OF DIVERSITY RECEIVING

Amateur interests in diversity reception waned as World War II loomed in the near future. The expense, the complexity, the space required for antennas all made the results not worth the effort. On CW, there was no obvious benefit to diversity and, in the pre World War II days, most hams were on CW. Amateurs became familiar with the principals of diversity reception by reading various books and magazine articles throughout the twenties and thirties. QST magazine published an article „Short Wave Radio Transmissions and Its Practical Uses Part II". by Chester W. Rice in the August 1927 issue about shortwave uses that mentioned diversity theory and reception. For the avid phone operator, having the equipment to eliminate fading signals and the associated distortion, it must have seemed like a virtual necessity. To the CW operation mode diversity seemed not be worth the effort. After all, CW copy was not that seriously affected by fading. [2]

As John. J Nagle reffered in [9] there was an attempt of Carll Roland, using two antennas and shortwave broadcast receivers for diversity receiving purposes spacing them at around 180 meters apart. He summarized his experiences in the March issue of Radio News Magazine in 1936. as "If the broadcast listeners had not wanted their receivers back, we would have kept on using diversity reception."

However, James Lamb, Technical Editor for QST, and engineer James McLaughlin decided that diversity was worth a try and began their research into some kind of practical amateur receiver that would incorporate diversity. [2]

3.1. The XE1G receiver

James Lamb and James McLaughlin had been separately experimenting with diversity reception as early as 1931. In the spring of 1935 they decided to have an informal meeting to discuss each others' thoughts on what technical advances might be used to create a practical amateur diversity receiver. A third person, a well-known amateur operator Dr. James M. B. Hard, XE1G from Cuernavaca, Morelos, Mexico, was ready to finance the construction of a dual-diversity receiver of Lamb's and McLaughlin's design. Both Lamb and McLaughlin thought that the tuning of commercial diversity receivers was too cumbersome because in an amateur station, the ability to tune through each amateur band easily and switch from band to band quickly was an obvious necessity. The XE1G receiver used a single Local Oscillator between the two receiver front ends to provide "single dial" tuning. Other circuits incorporated in the XE1G receiver were chain-driven with a tuning coverage from 1.7-30 MHz in four tuning ranges. [2] The completed receiver was delivered to Dr. Hard in 1936. [8] (Figure 3.1.)

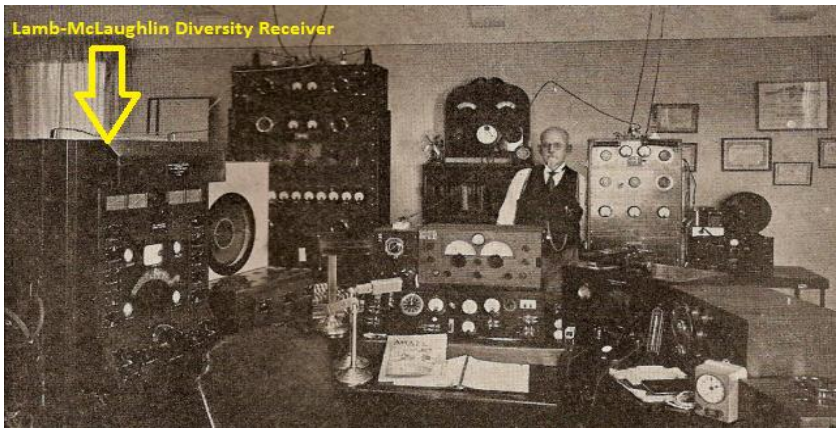


Figure 3.1. Dr. Hard and his Lamb-McLaughlin diversity receiver (1937)
Source: http://www.radioblvd.com/DiversityDD1.html (23/02/13)

Dr. Hard mainly operated on 20 meters with two antennas spaced at 15 meters, just sufficient to provide usable diversity action. With some mechanical improvements and technical development in IF amplifier the frequency range of the new prototype was extended to 540kHz - 36MHz and Dr. Hard's XE1G receiver had logged in 5000 hours of reliable operation.

It is also necessary to mention that there were some other attempts to use not so specially made receivers or even identical receivers for diversity. In the September 1939 issue of QST, S. Gordon Taylor described a diversity receiving system using Hallicrafters SX-17 and a Skyrider 5-10 receivers associated with a horizontal 10 meter dipol and one half of a vertical 5 meter beam. [9]

A slightly different approach to diversity reception was suggested by Forrest A. Bartlett in the same issue of QST. He feeded two separate preamplifers with two antenna signals paralelly connected their outputs to a single receiver. Switching the input of the conventional receiver between the signals, he produced a receiver output proporcional to the strongest signal present in either antenna at any instant of time. As a side effect, the structure implied a modulation content in the output with its frequency equal to switching frequency or its double, depending on the ratio of the receiver inputs. [9]

3.2. DD-1 prototype

Shortly after the QST article about the XE1G receiver was published, Hallicrafters became interested in building a dual diversity receiver for the amateur market. Working directly with James McLaughlin, Karl W. Miles, Hallicrafters' chief engineer was to build a dual diversity receiver. The first prototype of DD-1 underwent several technical modifications and was finally set in much smaller cabinet. (Figure 3.2.)

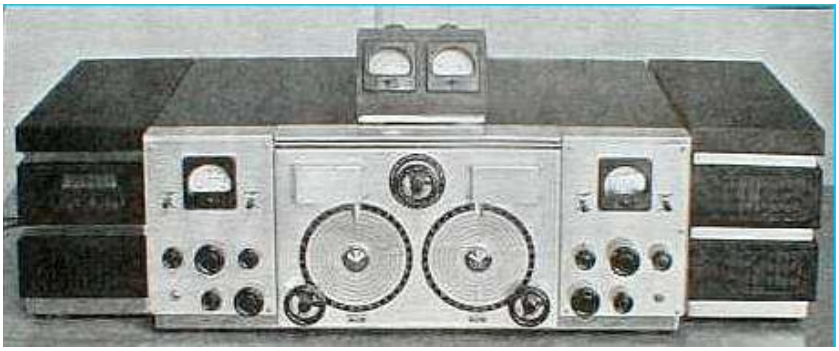


Figure 3.2. DD-1 diversity receiver prototype (1937)
Source: http://www.radioblvd.com/DiversityDD1.html (23/02/13)

As further improvements were implemented the later prototype and the production DD-1 are very different from the original Dr. Hard's one. Frequency coverage was also changed from the early prototype with the new range being 540kHz-36MHz in six bands. Besides few exterior changes in an arrangement of a front panel, as a main difference the production DD-1 used two IF amplifiers instead of three. [10]

3.3. The production "Skyrider Diversity" DD-1 receiver

Following Hallicrafters' tradition of naming receivers, the DD-1 was designated as the "Skyrider Diversity". Though radio broadcasting sector had a very wide segment in printed materials, the DD-1 production prototype was given the largest advertising campaign up to that time. [2], [11] Hallicrafters began advertising the Dual Diversity DD-1 in June 1938. and the DD-1 was only advertised till January 1939. [12] During these 6 months advertisements could be found everywhere. Despite a huge campaign it was widely supposed that the Skyrider Diversity was not going to be a major seller. The base price for the receiver was 300

USD, with the additional extras it could reach the amount of 500 USD which was almost a price of a new Chevrolet Coupe in 1938. As the price was rather high, Hallicrafters probably estimated that somewhere around 200 receivers would fill all of the orders besides all of the publicity donations that might be needed. But based on the results of quests carried out recently by serial number collector enthusiasts, only the production of about 100 to 125 DD-1 receivers in two production runs (approximately 100 units and later approximately 25 units) can be proven. It is also verifiable that the most majority of the receivers has been restored and renewed and are still available possessed by receiver collectors. (Figure 3.3.)

Figure 3.3. ”Skyrider Diversity” DD-1 production receiver prototype (1939)
Source: http://www.radiomuseum.org/r/hallicraft_skyrider_diversity_dd_1_d_1.html (23/02/13)

The major benefit to Hallicrafters was to their reputation as they had proven that they were capable of successfully engineering and building a complex, dual-diversity receiver for the market.

After World War II, there is hardly any mention of diversity in any ham magazines. The commercial stations and the military had always been and were to remain the primary users of diversity reception. As technology progressed into satellite communications by the late 1970s and other more reliable forms of communication came into use, the need for large, expensive diversity receiving installations all but vanished. Most of the equipment has been scraped or sold into surplus. [2]

During the second half of 20th century, radiocommunications technology underwent a lots of new improvements which finally manifestated in a dual or stereo receiving techniques.

5. SUMMARY

The first radiocommunications engineers being first to be faced with the fact of multi-path propagation and fading phenomena started their experimental analisys and understanding the behaviour experienced as early of 1920s. Based on Harold. Henry Beverage’s and his associate, H. O. Peterson’s first steps, the basics diversity reception techniques were deployed. In this article the early receiver prototypes have been introduced along with the first series producted DD-1 Skyrider receiver. Due to space limitation only the early milestones of history of diversity reception were presented in this paper. The diversity achievements of modern era and the way to the stereo reception technology being used recently, should be a subject of futher work.

References

[1] Pioneering in Electronics. The David Sarnoff Library http://www.davidsarnoff.org/kil-chapter01.html – (2013.02.23.)

[2] H. Rogers: Restoration of the Skyrider Diversity DD-1 Concole Receiver. Western Historic Radio Museum. http://www.radioblvd.com/DiversityDD1.html – (2013.02.23.)

[3] Oral-History: Harold H. Beverage and H. O. Peterson. http://www.ieeeghn.org/wiki/index.php/Oral-History:Harold_H._Beverage_and_H._O._PetersonD1.html – (2013.02.23.)

[4] Oral-History:Harold H. Beverage and H. O. Peterson. http://www.ieeeghn.org/wiki/index.php/Oral-History:Harold_H._Beverage_and_H._O._Peterson#Space_and_Polarization_Diversity_System – (2013.02.23.)

[5] Harol Henry Beverage, Explorer of the Wavelengths. Radio's 100 Men of Science,1944 ISBN 0-8369-1916-5 http://www.oldradio.com/archives/people/Harold_Beverage – (2013.02.23.)

[6] http://ok1ike.c-a-v.com/soubory/beverage.htm – (2013.02.23.)

[7] Pentti Stenman: The Muscle Radio: R-390A/URR. http://www.penan.net/dx/r-390a.htm (2013.02.23.)

[8] Diversity Reception and the Hallicrafters DD-1 – Part III. Carson Currents,,April/May 2003.12-13 http://www.cvrc.net/members/newsletters/AprMay03.pdf – (2013.02.23.)

[9] John J. Nagle K4KJ: Diversity Reception: An Answer to High Frequency Signal Fading. Ham Radio Magazine, September (1979), 48-55 http://www.epanorama.net/sff/Radio/Receivers/Diversity%20Reception.pdf – (2013.02.23.)

[10] Radiomuseum online. http://www.radiomuseum.org/m/hallicraft_usa_en_1.html – (2013.02.23.)

[11] Broadcasting History. http://www.americanradiohistory.com/Broadcasting_Individual_Issues_Guide.htm (2013.02.23.)

[12] Classic Pre-WWII Ham Gear 1928–1941. Radio Boulevard: Western Historic Radio Museum. http://www.radioblvd.com/Pre-WWII%20Ham%20Gear.htm – (2013.02.23.)

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Kovács Zoltán
zkovacs@nbsz.gov.hu

FELHŐ ALAPÚ RENDSZEREK TÖRVÉNYES ELLENŐRZÉSI PROBLÉMÁI

Absztrakt

A kommunikáció formái, lehetőségei az Internet és az azt kihasználó alkalmazások fejlődésével ugrásszerűen változnak, bővülnek. Ebben nagy szerepük van a nyilvános számítási felhő (Public cloud) telepítési modell szerint működő, elsősorban szoftver, mint szolgáltatás (Cloud Software as a Service (SaaS)) szolgáltatási modell típusú rendszereknek. Ezek azok a mindenki számára elérhető, akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen igénybe vehető rendszerek, szolgáltatások, amelyek ma már szerves részét képezik mindennapi életünknek A felhő alapú rendszerek törvényes ellenőrzésének igénye a felhasználás ütemével arányosan nő, ugyanakkor a törvényes ellenőrzést végző szervek több – jogi és technikai – problémával is szembesülnek. A cikk megvizsgálja a hírközlés és a kommunikáció viszonyát, a jelenleg is zajló strukturális változásokat, valamint az ezek kapcsán a törvényes ellenőrzés végrehajtásában jelentkező problémákat.

The forms and the possibilities of communication have been changing dramatically by the spread of internet and the development of applications using it. Mostly the public cloud (deployment model) and Cloud Software as a Service (SaaS) (service model) systems have a great role in it. These systems and services, which have become the part of your everyday life, are available for everyone and can be used with slight IT knowledge at a low price or free. The requirement of lawful monitoring of cloud computing systems has been growing proportionally to the growth of using, although the organizations doing lawful monitoring have been facing more and more legal and technical problems. This article is analysing the relation between communication and electronic communication, the changing of structure of them taking place nowadays, and the problems appearing in lawful monitoring.

Kulcsszavak: *felhő alapú rendszerek, hírközlés, kommunikáció, törvényes ellenőrzés ~ cloud computing, electronic communication, communication, lawful monitoring*

BEVEZETÉS

A kommunikáció formái, lehetőségei az Internet és az azt kihasználó alkalmazások fejlődésével ugrásszerűen változnak, bővülnek. Ez közhelyszerű megállapítás, de teljes mértékben igaz. A változások ütemét tovább növeli a felhő alapú rendszerek egyre nagyobb mértékű felhasználása, azon belül is a nyilvános számítási felhő (Public cloud) telepítési modell szerint működő, elsősorban szoftver, mint szolgáltatás (Cloud Software as a Service (SaaS)) szolgáltatási modell típusú rendszereké. Egyszerűbben fogalmazva ezek azok a mindenki számára – a meglévő személyi használatú eszközök (pl. notebook, okostelefon stb.) felhasználásával, akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen – igénybe vehető rendszerek, szolgáltatások (mint pl. Facebook, gmail, Dropbox, Twitter, Skype stb.) amelyek ma már szerves részét képezik mindennapi életünknek, kommunikációnknak.

A felhő alapú rendszerek törvényes ellenőrzésének igénye a felhasználás ütemével arányosan nő. Természetesen ezek közül is a fent már említett kategória (nyilvános számítási felhő telepítési modell szerint működő, szoftver, mint szolgáltatás szolgáltatási modell típusú) emelhető ki a törvényes ellenőrzést végzők szempontjából, hiszen a potenciális célszemélyi kör is ezt használja leginkább. A cikk elsősorban ennek a – továbbiakban PC/SaaS felhő alapú rendszerek megnevezéssel szerepelő – kategóriának a törvényes ellenőrzése kapcsán felmerülő problémákra fókuszál.

A törvényes ellenőrzés feladatrendszerébe – a mai megközelítés szerint – alapvetően az alábbi három tevékenységet értjük:

- adatszolgáltatás,
- kommunikáció ellenőrzés,
- forensic tevékenység.

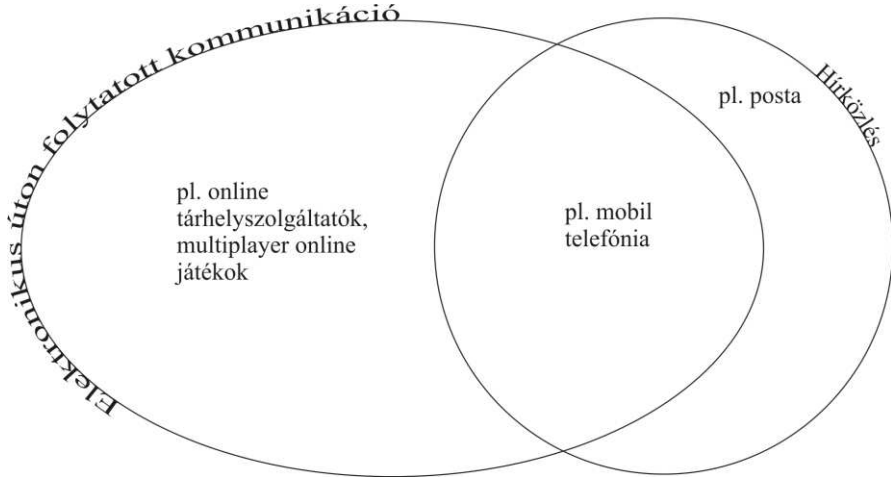
Ez azonban a korábbi ellenőrző tevékenységekhez képest vegyes képet mutat. Míg az adatszolgáltatásról és a kommunikáció ellenőrzésről elsősorban a klasszikus hírközlési hálózatoknál beszéltünk, addig a forensic tevékenység eddig kifejezetten számítástechnikai rendszerek vizsgálatára volt jellemző. Ma már a fejlett infokommunikációs rendszerek jellege, valamint az azokból kinyerhető, a nemzetbiztonsági és a bűnüldözési feladatokat segítő információk köre miatt mindháromra egyaránt szükség van. Ebből levonható tehát az a következtetés, hogy nem csak a technológiák konvergenciája figyelhető meg napjainkban, hanem ennek kapcsán a törvényes ellenőrzési metódusok konvergenciája is.

A technikai fejlődés, a kommunikációs szokások változása, az informatikai és hírközlő rendszerek összeolvadása és az ebből következő törvényes ellenőrzési metódusok konvergenciája komplex problémákat vetnek fel a törvényes ellenőrzésre feljogosított szervezetek számára. Érdemes megvizsgálni a változások okait, tendenciáit, majd az azokból következő problémákat és lehetőségeket. Erre azért van szükség, mert a korábbi, jól működő, a törvényes ellenőrzésre feljogosított szervek számára tevékenységük ellátásához jelenleg rendelkezésre álló technikai és jogi eszközök ma már sok esetben nem teszik lehetővé a teljes körű, hatékony feladat végrehajtást.

ELEKTRONIKUS ÚTON FOLYTATOTT KOMMUNIKÁCIÓ VS. HÍRKÖZLÉS

Az elektronikus úton folytatott kommunikáció megnevezés teljesen tudatos szóhasználat. Napjainkban ugyanis az említett fogalom alatt nem csak a hírközlő rendszereken folytatott kommunikációt értjük, hanem minden olyan kommunikációs lehetőséget, formát, amely lehetővé teszi két – vagy adott esetben több – fél között információk, adatok áramlását, cseréjét. Ez pedig messze túlmutat nemcsak a hírközlés, de a kifejezetten kommunikáció céljából kifejlesztett Internet alapú rendszereken is.

Húsz évvel ezelőtt a hírközlés teljes egészében lefedte az elektronikus úton folytatott kommunikációt (ez utóbbi a hírközlés mintegy részhalmazát képezte). Mára ez a kép megváltozott. Ha ábrázolnánk, akkor talán az 1. ábra megfelelően szemléltetné a kettő kapcsolatát. (A területek nagysága az egymáshoz képesti jelentőséget is szemlélteti.)



1. ábra. Az elektronikus úton folytatott kommunikáció és a hírközlés viszonya

Ma az elektronikus úton folytatott kommunikáció lehetőségei messze meghaladják a hagyományos hírközlését. A végeredmény szempontjából ugyanis nincs különbség a között, hogy megírok és elküldök egy elektronikus levelet, vagy megírás után a piszkozatok közé teszem, de a másik félnek megadom a postafiók eléréséhez szükséges felhasználó nevet és jelszót. Hiszen ez utóbbi esetben is hozzáfér, olvashatja ugyanazt az üzenetet. De itt még legalább a „levélszerűség" megvan, a „hagyományos" hírközlési forma fellelhető. Ha a továbbítani szánt információkat azonban egy felhő alapú tárhely szolgáltatónál kialakított fiókba helyezem el fájlként, majd ennek adom meg a belépéshez szükséges adatait a másik félnek, akkor a végeredmény ugyanaz: „A" felhasználótól „B" felhasználóhoz eljutott az információ. Ez a forma azonban már „nyomokban sem tartalmaz" hagyományos hírközlést. Ugyanilyen jellegű példa a multiplayer online játékok esete. Ezeket nem azért fejlesztették ki, hogy a felhasználók kommunikálni tudjanak egymással, az csak egy kiegészítője, hozadéka a játékoknak. Ugyanakkor tényszerűen vizsgálva, a végeredményt tekintve itt sincs különbség a játék során folytatott beszélgetések, chatelések és egy kifejezetten erre szakosodott hírközlő rendszeren folytatott beszélgetés vagy üzenetküldés között.

A törvényes ellenőrzést végző szervezeteknek alapvetőn az a feladata, célja, hogy a kijelölt célszemélyek kommunikációját lehetőség szerint teljes mértékben ellenőrizzék, függetlenül annak formájától, a felhasznált technológiától. Az egyik legnagyobb feladat tehát, hogy pontosan meghatározzuk azt, hogy mi kívánunk ellenőrizni, majd ehhez ki kell alakítani a megfelelő technikai és jogszabályi környezetet.

AZ ELEKTRONIKUS ÚTON FOLYTATOTT KOMMUNIKÁCIÓ VÁLTOZÁSA

A cikknek nem célja az elektronikus úton folytatott kommunikációs technológiák változásának okait, tendenciáit teljes vertikumukban bemutassa, csupán érzékeltetni kívánja, hogy miért kell foglalkozni vele, miért és milyen hatása van a törvényes ellenőrzésre.

A kommunikációs technológiák és szokások nem választhatók szét egymástól, egyfajta összefonódó spirált képezve, egymást is erősítve, gerjesztve hozták létre a mai népszerű kommunikációs formákat, lehetőségeket. A szélessávú és mobil Internet elérések elterjedése, a hordozható eszközök (pl. ultrabookok, tabletek, okostelefonok stb.) hihetetlen mértékű fejlődése, a közösségi oldalak népszerűségének ugrásszerű növekedése, a különböző

kommunikációs lehetőségeket biztosító PC/SaaS felhő alapú rendszerek, valamint az ezek használatát biztosító alkalmazások megjelenése minden nagyobb platformra (Windows, iOS, Andoid), mind mind növelték a felhasználás mértékét, egyre több emberben erősítették az igényt a csatlakozásra, használatra.

A technológia fejlődésének, a kommunikációs formák és lehetőségek rohamos bővülésének köszönhetően a felhasználói szokások nagymértékben megváltoztak az elmúlt években. Az un. Y (1980-1994 között születtek) és Z (1995-2009 között születtek) generáció [1] tagjai abszolút meghatározó szerepet játszanak ebben. Ők azok, akik vagy már gyermekkorban találkoztak az Internettel, (Y generáció), vagy már beleszülettek az Internet „uralta" világba (Z generáció), így élen járnak az új kommunikációs lehetőségek használatában. [2] A korábbi generációk hagyományos elektronikus kapcsolatteremtési formái (pl. telefónia, SMS) helyett számukra sokkal fontosabbak az Internet alapú kommunikációs lehetőségek, azok használatát játszi könnyedséggel sajátítják el, kibővített funkciókat természetesen és teljes körűen használják. Okostelefonjaikkal, vagy más mobil eszközeikkel évről évre növekvő mennyiségű adatforgalmat generálva bárhonnan, bármikor az Internetet használatával kommunikálnak másokkal, kapcsolódnak a közösségi oldalakhoz, osztják meg életük pillanatait, töltik fel magukról a fényképeket, videókat. Emiatt a hagyományos kommunikációs lehetőségek túlságosan drágák és/vagy nem képesek biztosítani ugyanazokat a szolgáltatásokat számukra, így azokra egyre inkább csak „kisegítő", „tartalék" rendszerként tekintenek. Jellemző, hogy a McCrindle Research kutatása szerint a Z generáció számára a MacBook, az iPad a Google, a Facebook, a Twitter, a Wii, a PS3 és az Android jelentik az ikonikus technológiákat, szemben például az X (1965-1979 között születtek) generáció tagjaival, akiknek ugyanezt a kazettás videomagnó, a walkman és az IBM PC testesítették meg. [1]

Az új technológiák megjelenése önmagukban is arra késztetik a kommunikáció törvényes ellenőrzésével foglalkozó szervezeteket, hogy figyeljék a trendeket, kövessék a sokak által használt technológiák fejlődését, és biztosítsák azok törvényes ellenőrzését. Legalább ugyan ilyen mértékű kényszerítő erőt jelent, hogy a fenti bekezdésekben vázolt felhasználói változások okán a hagyományosnak mondható kommunikációs formák és rendszerek (pl. telefónia) jelentősége a felhasználók – ezáltal a potenciális célszemélyi kör, így a törvényes ellenőrzést végző szolgálatok – számára csökken.

A HÍRKÖZLÉS VÁLTOZÁSA

A megfizethető havidíjú, korlátlan adatforgalmat biztosító szélessávú Internet elterjedése, a sokszor ingyenesen elérhető és használható, elektronikus kommunikációt lehetővé tevő alkalmazások, valamint a mobil eszközök fejlődése alapjaiban változtatja meg a hírközlési piacot. Egy jól megfigyelhető folyamat zajlik le, amikor is a korábbi, klasszikus hírközlési szolgáltatók helyét specializált szolgáltatók veszik át.

Klasszikus hírközlési szolgáltatónak tekinthetők azok a szolgáltatók, akik elektronikus hírközlő hálózatot üzemeltetnek és ezen hírközlő szolgáltatást nyújtanak. Ilyenek pl. a hagyományos (vezetékes és mobil) telefonszolgáltatást biztosító cégek. A hangsúly a klasszikus szolgáltatók esetében az „és"-en van, azaz a két tevékenységet együtt végzik.

Az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) [3], így annak a törvényes ellenőrzéshez kapcsolódó részei is elsősorban a klasszikus hírközlési szolgáltatásokon és szolgáltatókon alapulnak. A törvény a 188. § (értelmező rendelkezések) alatt definiálja az elektronikus hírközlési szolgáltató és az elektronikus hírközlési szolgáltatás fogalmát. Ezek a következőek:

„13. Elektronikus hírközlési szolgáltatás: olyan, más részére általában ellenszolgáltatásért végzett szolgáltatás, amely teljesen vagy nagyrészt jeleknek elektronikus hírközlő hálózatokon történő átviteléből, és ahol ez értelmezhető, irányításából áll, de nem foglalja magában az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások felhasználásával továbbított tartalmat szolgáltató vagy ilyen tartalom felett szerkesztői ellenőrzést gyakorló szolgáltatásokat, valamint nem foglalja magában az információs társadalommal összefüggő, más jogszabályokban meghatározott szolgáltatásokat, amelyek nem elsősorban az elektronikus hírközlő hálózatokon történő jeltovábbításból állnak."

„14. Elektronikus hírközlési szolgáltató: elektronikus hírközlő hálózat üzemeltetője, valamint elektronikus hírközlési szolgáltatást nyújtó természetes, illetőleg jogi személy vagy jogi személyiséggel nem rendelkező gazdasági társaság."

A törvény 2003-as megalkotásakor számos, napjainkban már széleskörűen használt technológia még nem létezett. A probléma érzékeltetésére lássunk két példát. A rendkívül népszerű Skype első béta verziója 2003. augusztusában jelent meg (tehát a törvény megalkotásakor még nem volt elérhető!), míg 2011-re átlagban 20 millió felhasználó használta egyidejűleg. [4] Másik példa a Facebook, amely 2004. február 4-én debütált, tehát a törvény hatályban lépésekor (2004. január 1-én) [3] még el sem indult! 2012. október 4-én az alapító saját Facebook oldalán tette közzé, hogy havi szinten több, mint 1 milliárd ember használja aktívan a közösségi oldal nyújtotta szolgáltatásokat. [5] [6]

A Skype mellett számtalan jelenleg kisebb vagy nagyobb jelentőséggel bíró Internet alapú kommunikációs alternatíva létezik, amelyek megfelelnek az elektronikus hírközlési szolgáltatás definíciójának, de a Skype-hoz hasonlóan üzemeltetőjük (vagy Magyarországon, vagy egyáltalán) nem rendelkezik saját elektronikus hírközlési hálózattal.

A klasszikus hírközlési szolgáltatói modellt egyre inkább felváltja egy specializált infrastruktúra-, alkalmazás-, és tartalomszolgáltatói (ez utóbbival jelen cikk nem foglalkozik) modell, és ez a tendencia a jövőben várhatóan tovább erősödik. Az új modell legjelentősebb hatása a hírközlésre, hogy az infrastruktúraszolgáltató a hírközlési hálózatot – vagy célszerűbb megfogalmazással Internet elérést – biztosítja, míg az alkalmazásszolgáltató gondoskodik a tényleges kommunikációs szolgáltatásról.

Az alkalmazásszolgáltató elnevezést nem csak azért célszerű használni a hírközlési szolgáltató helyett, hogy megkülönböztessük a korábban együtt nyújtott két funkció (infrastruktúra-, és alkalmazásszolgáltatás) szétválasztását, hanem azért is, mert az alkalmazásszolgáltató kifejezés egy bővebb, tágabb értelmezésű fogalom, és nem csak a hírközlési szolgáltatást nyújtó alkalmazásokat érjük, érthetjük alatta. (Ennek a törvényes ellenőrzés jogi eszközeinek átalakítása során is nagy jelentősége lesz.)

A hírközlési szolgáltatók specializált szolgáltatókra történő szétválása nem csak a törvényes ellenőrzés tekintetében jelent problémát. Amint az már a cikk elején is bemutatásra került, a szélessávú, mobilan bárhonnan elérhető Internet arra ösztönzi a felhasználókat, hogy az erre alapuló, a korábbiaknál olcsóbb, több szolgáltatást biztosító kommunikációs formákat válasszák. Az Internet – és ez ma már a mobil Internetről is elmondható – megfizethető, nem túlságosan magas fix havi díjért, korlátlan, vagy az átlag felhasználói szokások okán annak tekinthető adatforgalommal nagyon sok ember számára elérhető. Ha kifejezetten a mobil kommunikációt nézzük, minden költséget összeadva olcsóbban lehet főleg külföldi viszonylatban kommunikálni a Skype vagy a Viber segítségével, mint hagyományos telefonszolgáltatás segítségével. Ugyanakkor az említett, vagy a hasonló jellegű Internet alapú kommunikációs szolgáltatásoknak csupán egy része ingyenes, más részük igénybevételéért (pl. vezetékes vagy mobil telefon hívása esetén) viszont fizethetnünk kell. Ám ez a profit nem az Internet szolgáltatónál (aki ez esetben infrastruktúraszolgáltatóvá avanzsált), hanem az alkalmazásszolgáltatónál képződik. Ugyanez elmondható más – és nem csak kommunikációs – alkalmazások esetén is.

Az Internet szolgáltatók az éles piaci verseny, a sávszélesség és a szolgáltatások minőségének növelése okán óriási összegeket költenek technológiai fejlesztésekre, miközben időről időre csökkentik a havi díjak összegét. Ez a mobil Internetet nyújtó, infrastruktúrát is üzemeltető (valódi, nem virtuális) szolgáltatókra fokozottan igaz. Természetesen ez is termel profitot, de az igazán nagy nyereség nem náluk keletkezik, hanem az általuk üzemeltetett infrastruktúrán nyújtott, Internetet felhasználó alkalmazások szolgáltatóinál. Ezt pedig ez utóbbiak a jóval kisebb mértékű és értékű beruházási igényeknek, az alacsonyabb működési költségeknek, valamint a felhasználóktól és nem utolsó sorban a hirdetőktől befolyó jóval magasabb összegeknek köszönhetik.

Ezt a jelenségeket az egyre inkább infrastruktúraszolgáltatóvá váló hírközlési cégek is kezdik felismerni, és próbálnak valamit tenni a helyzet megváltoztatása érdekében. Erre az egyik legjobb példa az Orange cég esete, akinek sikerült elérnie, hogy a nagy költséggel járó infrastrukturális fejlesztéseihez a hálózatát – természetesen a felhasználói kérések által – leginkább használó Google pénzügyileg hozzájáruljon. [7][8] Erre korábban is voltak már – sikertelen – kezdeményezések [9], a francia szolgáltató sikeres akciója azonban precedenst teremtett. Lépésével várhatóan egy folyamat indul el, átalakul az Internet korábbi, sérthetetlennek tűnő üzleti modellje. [7]

A PC/SAAS FELHŐ ALAPÚ RENDSZEREK TÖRVÉNYES ELLENŐRZÉS PROBLÉMÁI

Amint az a bevezetőben is olvasható, a törvényes ellenőrzést végző szervezetek technikai és jogi eszközökkel rendelkeznek tevékenységük ellátásához. A napjainkban rendelkezésre álló eszközök alkalmazása, alkalmazhatósága és azok hatékonysága azonban több problémát is felvet.

A PC/SaaS felhő alapú rendszerek ellenőrzése esetén a jogi kapcsolat a szolgáltató és a törvényes ellenőrzést végző között áll fenn, – ideális esetben – törvényi kötelezettség alapján. Problémaként jelentkezik azonban, hogy amíg a hírközlési hálózatoknál egy kialakult, minden szereplő által elfogadott és a demokratikus államokban hasonló jellegű törvényekre alapozott törvényes ellenőrzésről beszélhetünk, addig a felhő alapú rendszerek esetében nem mondható el ugyanez. Itt ugyanis sokkal inkább különálló infrastruktúra-, alkalmazás-, és tartalomszolgáltatókkal találkozunk, nagyon ritka az az eset, amikor a felhasznált infrastruktúrát és alkalmazást egyazon szolgáltató biztosítja. Márpedig a hatályos magyar jogszabályok alapján csak ez utóbbi esetében lenne vitán felül állóan hírközlési szolgáltatónak tekinthető, és így a törvényes ellenőrzés kapcsán együttműködésre kötelezhető. Ugyanakkor a jelenleg érvényben lévő jogszabályainkban az infrastruktúra-, alkalmazás-, és tartalomszolgáltatók nem, vagy nem megfelelő módon vannak definiálva, törvényes ellenőrzés kapcsán felmerülő kötelezettségeik pedig szintén nem, vagy jó esetben is csak részlegesen olvashatók ki ezekből.

Az ellenőrzéshez használt technikai eszközök kapcsán ugyancsak problémákkal szembesülnek a felhatalmazott szolgálatok. Egyrészt az új technológia új ellenőrző eszközöket kíván, kívánhat, ez pedig beruházást igényel. Ráadásul eltérően felépített szolgáltatói infrastruktúrák esetén ez akár szolgáltatónként eltérő megoldás lehet, ami igen költséges. Másrészt a hírközlés ellenőrzésnél kialakult és elfogadott rend, miszerint az infrastruktúrával és szolgáltatással az adott országban egyaránt jelen lévő szolgáltató együttműködik a nemzetbiztonsági és bűnüldöző szervekkel, ebben az esetben nem, vagy nem teljes mértékben működik. A hírközlési szolgáltatók számára többek között kötelező a szolgáltatást bejelenteni, és *„biztosítani az elektronikus hírközlő hálózatban továbbított küldemények, közlések, továbbá a szolgáltató által kezelt adatok titkos információgyűjtéssel, illetve titkos adatszerzéssel történő megismeréséhez szükséges eszközök és módszerek*

alkalmazási feltételeit". [3] Ilyen fajta kötelezettsége jelenleg nincs az alkalmazás szolgáltatóknak Magyarországon, de ennek előírása Európai Unió országainak, sőt a világ többi államának is komoly problémákat okoz.

Jelenleg nincs olyan szabályozás, amely európai szinten irányadó lenne a kérdésben, és amely rövid időn belül, nagyobb szolgáltatói ellenállás nélkül, átemelhető lenne a magyar törvényekbe. Ez két gondot okoz. Az első, hogy az alkalmazás szolgáltatók hajlandóságán múlik, hogy engedi-e ellenőrző eszköz telepítését, esetleg saját eszközeivel, egyfajta törvényes ellenőrzés, mint szolgáltatás (Lawful Monitoring as a Service) [10] nyújt a szolgálatok számára, vagy teljesen elutasítja az együttműködést. Ez utóbbira – sajnos negatív – példa a Google esete, aki nem, hogy nem működik együtt, de átláthatósági jelentéseiben még közzé is teszi, hogy melyik országból hány adatszolgáltatási kérést kapott és abból mennyit, milyen minőségben teljesített. A cég Magyarországnak, annak ellenére sem szolgáltatott információkat, hogy az azokra vonatkozó kérések teljes mértékben kielégítették a hazánkban jelenleg hatályos törvényi feltételeket. [11] A másik gond, hogy míg a hagyományos hírközlés ellenőrzésénél a jól ismert törvényi és technikai háttér okán teljes értékű technikai megoldásokat kínálnak az erre szakosodott gyártók, addig a PC/SaaS felhő alapú rendszerek ellenőrzésére elsősorban egyedi problémákat megoldó eszközöket tudnak csak szállítani. Ez pedig drágává, bonyolulttá és esetivé teszi az ellenőrzéseket.

A megoldás első lépését a törvényi háttér kialakítása jelentheti. Ebben az egyik legfontosabb feladat, hogy pontosan definiáljuk az infrastruktúra-, alkalmazás-, és tartalomszolgáltatók fogalmát, meghatározzuk, mit kell ellenőrizni és annak megfelelően kell kialakítani a megfelelő jogszabályi környezetet. Amint az előző fejezet végén az Orange cég példáján keresztül bemutatásra került, elindulhat egy folyamat, amely során átalakul az Internet korábbi, sérthetetlennek tűnő üzleti modellje. Várhatóan hasonló változások következnek be a törvényes ellenőrzés területén is. Ahhoz ugyanis, hogy a nemzetbiztonsági és bűnüldözési munkát hatékonyan támogató ellenőrzést lehessen kialakítani, olyan, jelenleg sérthetetlennek tűnő dolgokhoz kell hozzányúlni (szabályozni és adott esetben szankcionálni!), mint a hazai infrastruktúrával nem rendelkező, Internetes alkalmazást nyújtó cégek működési jogai, kötelezettségei Magyarországon.

A hírközlési szolgáltatók kontra alkalmazásszolgáltatók kapcsán korábban említett kettős helyzet rendezése a nemzetbiztonsági, bűnüldöző szerveken kívül a klasszikus hírközlési szolgáltatóknak is érdeke. Ugyanis amíg az infrastruktúrával is rendelkező, azokat üzemeltető hírközlési cégek kötelezettségeit (bejelentés, együttműködés a törvényes ellenőrzés kapcsán, adófizetés, frekvenciadíj, stb.) a hatályos jogszabályok pontosan előírják, az erre feljogosított hatóság pedig szankcionálhatja, addig az infrastruktúrával nem rendelkező alkalmazás szolgáltatók esetében ez nem mondható el. Ez utóbbi szolgáltatók egy része csak bizonyos jogértelmezéssel lenne az Eht. hatálya alá tartozónak tekinthető, más részük pedig még úgy sem. (Az NMHH által közzétett, „Elektronikus hírközlési szolgáltatások hatósági osztályozása" alatt megtalálható „Szolgáltatás típusok" [12] és „Szolgáltatás leírása" [13] dokumentumok sem segítenek a probléma feloldásában, hiszen azok is kifejezettem a klasszikus hírközlési szolgáltatásokra koncentrálnak. Ezt bizonyítja az is, hogy az „Egyéb előfizetői adatátviteli szolgáltatás" címke alatti leírásnál – ahová talán beleérthetőek lennének az alkalmazásszolgáltatók – a következő példa szerepel: *„Ide tartozik például az önálló elektronikus hírközlési szolgáltatásként nyújtott MMS szolgáltatás."*) Az viszont egységesen elmondható, hogy az alkalmazásszolgáltatók szankcionálására egyrészt eddig nem volt példa, másrészt az egyébként is rendkívül nehezen kivitelezhető.

Így fordulhat elő, hogy a korábban már említett eset szerint a Google bár Magyarországon szolgáltat, ki tud bújni a hatályos jogszabályok alól, és az érvényes törvényeknek megfelelő adatszolgáltatási kérést vissza tudja utasítani. [11] Ez a hagyományos postai és klasszikus elektronikus hírközlési szolgáltatók esetében elképzelhetetlen lenne. Ráadásul a Google-nak

(és a többi hasonló alkalmazásszolgáltatónak) még azok a törvényes ellenőrzéshez kapcsolódó költségeket sem kell viselnie, amit a hírközlési szolgáltatók a magyarországi piacra lépésükkel vállalnak.

A felhő alapú – így a PC/SaaS – rendszerek törvényes ellenőrzésének szabványosításán többek között az ITU és az ETSI is dolgozik. Ám amíg ezek elkészülnek, és megjelennek az akár ezekből levezetett európai szintű jogszabályok, addig még várhatóan hosszú évek telnek el. További időt vesz igénybe az európai szabályzó átültetése a hazai jogi környezetbe, majd annak elfogadtatása és hatályba léptetése. Ezt viszont nem célszerű megvárni. A megoldás tehát egy új – akár átmenetinek is tekinthető – hazai jogi szabályozás kialakítása.

ÖSSZEFOGLALÁS ÉS KÖVETKEZTETÉSEK

A cikk bemutatta az Internet és az azt kihasználó alkalmazások fejlődésével ugrásszerűen változó, bővülő kommunikációs formák, lehetőségek hatásait, áttekintette az elektronikus úton folytatott kommunikáció és a hírközlés viszonyát, e kettő változásait, valamint a PC/SaaS felhő alapú rendszerek törvényes ellenőrzése kapcsán felmerült problémákat.

A cikkből a következő következtetések vonhatók le:

1. Az információs és kommunikációs technológiák konvergenciája mellett a törvényes ellenőrzési metódusok konvergenciája is megfigyelhető.
2. Az elektronikus úton folytatott kommunikáció fogalma sokkal szélesebben értelmezhető, mint a hírközlés, és ez kihatással van a törvényes ellenőrzésre is.
3. A klasszikus hírközlési szolgáltatók helyét egyre inkább specializált infrastruktúra-, alkalmazás- és tartalomszolgáltatók veszik át, és ez a tendencia a jövőben várhatóan tovább erősödik.
4. Az elektronikus úton folytatott kommunikáció változásában nagy szerepük van a PC/SaaS felhő alapú rendszereknek, ám ezek törvényes ellenőrzése jogi és technikai problémákba ütközik.
5. A törvényes ellenőrzés hatékonyságának növelése érdekében az új hazai jogi szabályozás kialakítását – akár átmeneti jelleggel is – mi hamarabb meg kell tenni, azzal nem célszerű megvárni a feltehetően még évekig húzódó szabványosítási és Európai Uniós irányelvek kialakítását. Ennek során olyan, jelenleg sérthetetlennek tűnő dolgokhoz kell hozzányúlni (szabályozni és adott esetben szankcionálni!), mint a hazai infrastruktúrával nem rendelkező, Internetes alkalmazást nyújtó cégek működési jogai, kötelezettségei Magyarországon.

A cikk a belőle levonható következtetésekkel együtt is alapvetően problémafelvető és nem problémamegoldó. Ahhoz, hogy a felvetett problémákat – a helyükön – kezelni lehessen további feladatok, vizsgálatokat kell végrehajtani. Elsősorban a jogi szabályozás kialakítása előtt pontosan definiálni kell az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmát. Másodszor célszerű áttekinteni, összehasonlítása *a törvényes ellenőrzésre jelenleg* rendelkezésre álló technikai eszközöket és módszereket, azok előnyeivel, hátrányaival együtt. Harmadszor meg kell határozni, hogy mit kell ellenőrzés alá vonni ahhoz, hogy a nemzetbiztonsági és a bűnüldözői munkát hatékonyan lehessen a továbbiakban is támogatni.

Felhasznált irodalom

[1] Generations Defined. McCrindle Research 2012
http://mccrindle.com.au/resources/Generations-Defined-Sociologically.pdf
(letöltve: 2013. 02. 09.)

[2] X, Y, Z: GENERÁCIÓK A VILÁGHÁLÓ VONZÁSÁBAN (2011. december 18.)
http://www.intergeneracio.hu/2011/12/18/x-y-z-generaciok-a-vilaghalo-vonzasaban/
(letöltve: 2013. 02. 07.)

[3] [3] 2003. évi C. törvény az elektronikus hírközlésről
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300100.TV – (letöltve: 2013. 02. 09.)

[4] [4] Molnár Gábor, Zalatnay Zsolt: Szolgáltatások és architektúrák Skype előadás
www.tmit.bme.hu/dl239 – (letöltve: 2013. 02. 13.)

[5] [5] http://newsroom.fb.com/Timeline – (letöltve: 2013. 02. 15.)

[6] [6] https://www.facebook.com/zuck/posts/10100518568346671
(letöltve: 2013. 02. 15.)

[7] Dajkó Pál: A Google fizet Franciaországban: megtört a netsemlegesség? (2013.01.22.)
http://itcafe.hu/hir/google_orange_netsemlegesseg.html – (letöltve: 2013. 02. 09.)

[8] Gálffy Csaba: A Google már fizet a francia internetszolgáltatónak (2013. január 21.)
http://www.hwsw.hu/hirek/49670/google-france-telecom-orange-afrika-okostelefon-youtube-android.html – (letöltve: 2013. 02. 09.)

[9] Koi Tamás: Skype: az internet nem a mobilszolgáltatóké! (2010. április 26.)
http://www.hwsw.hu/hirek/44435/voip-skype-mobil-internet-halozat-mobiltelefon.html
(letöltve: 2013. 02. 09.)

[10] Kovács Zoltán: Cloud security in terms of the law enforcement agencies – Hadmérnök VII. Évfolyam 1. szám - 2012. március

[11] Dajkó Pál: A Google továbbra sem ad ki adatokat a magyar kormánynak
(2013. január 24.)
http://itcafe.hu/hir/google_atlathatosag_transparency.html – (letöltve: 2013. 02. 09.)

[12] Elektronikus hírközlési szolgáltatások új hatósági osztályozása – lista 2012.02.13. 16:14 Forrás: Szolgáltatásbejelentési osztály, Nyilvántartási és tájékoztatási főosztály
http://nmhh.hu/dokumentum/448/szolgaltatas_hierarchia_20081009.pdf
(letöltve: 2013. 02. 19.)

[13] Szolgáltatások osztályozása - fogalmak 2012.02.13. 16:13 Forrás: Szolgáltatásbejelentési osztály, Nyilvántartási és tájékoztatási főosztály
http://nmhh.hu/dokumentum/447/szolgaltatas_leirasa.pdf – (letöltve: 2013. 02. 19.)

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Munk Sándor
munk.sandor@uni-nke.hu

AZ INFORMÁCIÓKERESÉS ALAPJAI

Absztrakt

Az elérhető információk mennyiségének ugrásszerű bővülésével az információkeresés feladatai is megnehezedtek, megváltoztak. Az információhoz jutás egyik lehetősége a már meglévő információk közötti keresés. Napjainkban az információk már túlnyomórészt informatikai rendszerekben kerülnek tárolásra és egyre bővülő mértékben azokban is keletkeznek. Az információkeresés számos más alkalmazási terület mellett a védelmi szférában is jelentős lehetőségeket kínál. Az eredményes kutatás és alkalmazás e téren is szükségessé teszi a különböző értelmezések, megközelítések áttekintését, elemzését. Ennek érdekében jelen publikáció az információkeresés alapvető kérdéseinek rendszerezését, egységes keretbe foglalását tűzte ki céljául. Ezen belül: bemutatja a keresés általános értelmezését; meghatározza az informatikai eszközökkel támogatott információkeresés alapfogalmait, főbb típusait és javaslatot tesz az információkeresés általános fogalmára.

With the dramatic expansion of the amount of available information, the tasks of information search, retrieval have changed, became more difficult. One of the possibilities to acquire necessary information is searching between existing information. Today information is mainly stored in IT systems and in growing extent is also created in these systems. Besides a number of other application areas, information search/retrieval provides significant opportunities for the defense sector too. Effective research and application in this field also requires the review and analysis of the variety of different interpretations, approaches. For this reason this publication aims to systematize, and organize into a unified framework the fundamental issues of information search/retrieval. In particular: presents the general interpretation of searching; defines the basic concepts of computer aided information search/retrieval, sets out the its main types, and proposes a comprehensive definition of information search.

***Kulcsszavak**: keresés, információkeresés, szemantikus keresés, informatikai szolgáltatások ~ search, information retrieval, semantic search, IT services*

BEVEZETÉS

Az információk szerepe, jelentősége a történelem során soha sem volt kérdéses. Ami egyes korokban ugrásszerűen megváltozott és ezzel megváltoztatta az információs tevékenységek lehetőségeit, az az írás megjelenésétől a számítógépek és hálózataik megjelenéséig tartó technikai fejlődés. A folyamatosan fejlődő információs technológiák jelentős mértékben, napjainkban már a feldolgozhatóság határain is túl bővítették az elérhető információk körét. Az információrobbanás, a korábban alig ismert és használt előtét tagokkal leírt peta-, exa- és zetta-bájtokkal jellemezhető világméretű információtömeg a mindent elöntő információáradat új megoldásokat követel, különben – mint ahogy azt John Naisbitt jövőkutató már 1982-ben megfogalmazta – "belefulladunk az információkba, miközben éhezünk a tudásra".

A szervezeti, vagy egyéni célok, feladatok megvalósításához szükséges információk megszerzésének egyik lehetősége a már meglévő és valamilyen rögzített formában rendelkezésre álló információk közötti keresés. Ez természetesen elvileg végrehajtható az összes információ átnézésével és a megfelelő információk kiválasztásával, azonban ez már a sumér agyagtábla 'könyvtárakban' sem volt hatékony, megvalósítható megoldás. Ebből következően vált aktuális kutatási és szakterületté az információkeresés és maradt is mindmáig az.

A rendelkezésre álló információk napjainkban már túlnyomórészt informatikai rendszerekben kerülnek tárolásra, sőt egyre növekvő mértékben azokban is keletkeznek. Lassan oda jutunk – egyetértünk-e ezzel, vagy sem; 'jó'-e ez, vagy sem – hogy, ami nem érhető el informatikai eszközökkel, az nincs is.[1] Ebből következően és az információtechnológia lehetőségeinek bővülésére támaszkodva az információkeresés módszerei, megoldásai között is mindenekelőtt az informatikai támogatásra épülőek játszanak jelentős szerepet.

Az informatikai eszközökkel támogatott hagyományos keresés az adatbázis-kereséstől, a szöveges információtárolás és visszakeresésen át, a világháló keresőrendszereiig a 2000-es évek elején eljutott a jelentés és a szövegösszefüggés kérdéseit is figyelembe vevő szemantikus keresésig. Az információkeresés és a szemantikus keresés a védelmi szférában is jelentős szerepet játszik. Csak példaként felsorolva, ide tartozik a nyílt forrású hírszerzés katonai, nemzetbiztonsági, rendőri célú felhasználás; vagy a szervezeti tudás széleskörű elérhetőségének, megosztásának, hasznosításának megoldásai. Mint minden szakterület esetében, a szakirodalomban itt is számos különböző kifejezéssel, értelmezéssel, megközelítéssel találkozhatunk, amely nehezíti az e téren folytatott kutatások eredményeinek hasznosítását, egymásra épülését.

Mindezek alapján jelen publikáció célja az információkeresés alapvető kérdéseinek összegezése, rendszerezése és egységes keretbe foglalása. Ennek érdekében:

- bemutatja a keresés általános fogalmát, értelmezését, meghatározza folyamatát, alapvető összetevőit, valamint az információkeresés meghatározó sajátosságait;
- meghatározza az informatikai eszközökkel segített információkeresés fogalmait, főbb típusait, azok sajátosságait;
- valamint javaslatot tesz az információkeresés általános fogalmára.

[1] Jelen publikációban az 'informatikai' jelzőt tág értelemben, 'információs tevékenységeket támogató, megvalósító technikai [megoldás]' tartalmú értelmezésben használjuk.

A KERESÉS ALAPJAI

A keresés széles körben létező, megfigyelhető tevékenység (jelenség), amely nem korlátozódik az emberekre. A helyváltoztatásra képes élőlények fiziológiai szükségleteik kielégítésére általában többféle dolog keresésére kényszerülnek: pld. táplálék, menedék, pihenőhely, fajtársak, stb. Ennek részét képezi a bejárás, az érzékelés, a minősítés, a felismerés és a választás. A továbbiakban a keresés fogalmát témánk szempontjából az emberi tevékenységre szűkítve vizsgáljuk és bemutatjuk a fogalom köznapi értelmezését, röviden, mélyebb elemzés nélkül számba vesszük legfontosabb összetevőit, végül megfogalmazzuk az információkeresés alapvető sajátosságaira vonatkozó megállapításainkat.

A keresés fogalma, értelmezése általában

A *keresés köznapi fogalma* azt a tevékenységet takarja, amikor valakit, vagy valamit – akit, amit nem tudunk, hogy hol van, esetleg azt sem tudjuk, hogy létezik-e – meg akarunk találni. Az értelmező szótár szerint a keres kifejezés témánk szempontjából érdekes jelentése: "I. (Meg)találni igyekszik. 1. <Meghatározott személyt, dolgot, aki, amely elveszett, ill. akiről, amelyről nem tudja (pontosan), hogy hol van> megtalálni igyekszik. … 3. Találni igyekszik <ismeretlen személyt, dolgot, akiről, amiről még azt sem tudja, hogy létezik-e olyan minőségben, amilyenre szüksége van, amilyen neki megfelel>." [1, 858. o.] Ugyanilyen értelmezést hordoz az angol 'search' kifejezés is: "megpróbálni megtalálni valamit gondosan, alaposan végignézve, vagy más módon keresve"[2] [2], illetve "gondosan bejárni, vagy átnézni (helyet, területet, stb.) azért, hogy meg lehessen találni valami hiányzót, elveszettet"[3] [3, 1287. o.]

A keresés már a köznapi értelmezés szerint is két átfogó típusba sorolható aszerint, hogy egy már ismert dolgot, vagyis tulajdonképpen annak aktuális helyét, hollétét keressük, vagy adott tulajdonságoknak megfelelő dolgot/dolgokat keresünk, amilyen/amilyenek nem is biztos, hogy létezik/léteznek. Az elsőre példát nyújtanak a 'keresem a lányomat[a buliban]', 'keresem a mobil telefonomat[a lakásban]', vagy 'keresem a sógorom telefonszámát[, amit valahová felírtam]'. A második csoportba tartoznak a 'keresek egy angolul tudó hallgatót[a tancsoportban', 'keresek aknát [a menetvonalon]', 'keresek legfeljebb 56x45x25 cm méretű kis bőröndöt', vagy 'keresek szinonimákat a krumpli szóra'.

A keresés modellje, összetevői

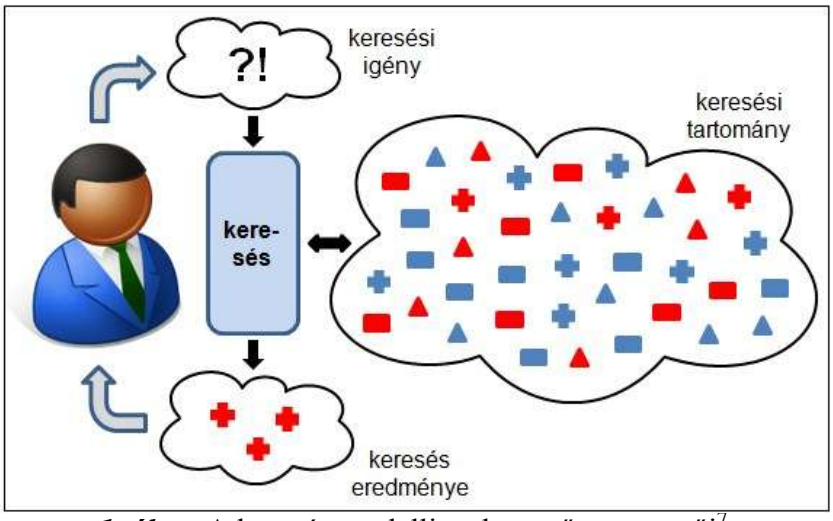
A *keresés fogalmának alapvető összetevői* közé a keresés alanya, a keresés tárgya, valamint a keresési tartomány tartozik, vagyis hogy ki keres, mit keres és hol keresi. Ezen túl a keresésnek mindig van, kell legyen célja, igénye, amelyben a kereső fél meghatározza, hogy mit kíván (meg)találni. Ennek a célnak, igénynek megfelelően indul a keresés, mint tevékenység, amelynek eredménye a keresett – a keresési célnak megfelelő – dolog (dolgok). A keresés részfeladatokra osztható, különböző szereplőkkel megosztható. A kereső fél a keresés során igénybe vehet különböző, a keresést támogató rendszereket, eszközöket, szolgáltatásokat. Végül a konkrét keresések előtt már végrehajthatóak egyes keresési részfeladatok, vagy a kereséseket megkönnyítő előkészítő feladatok.

A *keresés tárgya* lehet egy konkrét személy, tárgy, dolog (amiből egy van), vagy egy adott keresési célnak, feltétel-halmaznak megfelelő dolgok összessége. Az első esetben a keresés akkor ér véget, amikor az adott dolgot megtaláltuk,[4] a második esetben pedig akkor, ha egy adott körből kiválasztottuk a feltételeknek megfelelő dolgokat, vagy találtunk közülük meghatározott számút. A keresés tárgya egyben a *keresés eredménye* is. A keresés

[2] Try to find something by looking or otherwise seeking carefully and thoroughly.
[3] To go or look through (a place, area, etc.) carefully in order to find something missing or lost.
[4] Lehetséges egy időben több konkrét dolog keresése is, ami akkor eredményes, ha valamennyit megtaláltuk.

eredményessége igen/nem skálán leírható azzal, hogy megtaláltuk-e a keresett dolgot, illetve találtunk-e a keresési célnak megfelelő dolgo(ka)t. A második esetben a keresés eredményességének, illetve hatékonyságának fontos jellemzője a pontosság és a teljesség.[5] A pontosság azt mutatja meg, hogy a kiválasztott dolgok közül hány felel meg ténylegesen a keresési igényeknek, a teljesség pedig azt, hogy a feltételeknek megfelelő dolgokból mennyi került ténylegesen kiválasztásra. Ezekkel az információkereséshez kapcsolódóan a későbbiekben részletesebben is foglalkozunk.

A *keresési tartomány*, a keresés helye szintén alapvető összetevő, hiszen teljesen más feladat valamit/valakit megkeresni a szobában, a lakásban, az épületben, vagy a városban; a gyerekek, a felnőtt férfiak, vagy nők között; illetve a feljegyzéseim között, a szervezet iratai között, egy könyvtárban, vagy az Interneten. A keresési tartomány azon dolgok körét határozza meg, amelyek közül ki akarjuk választani a keresettet, vagy a feltételeknek megfelelőket. Ez – halmazok definiálásához hasonlóan – megtehető az átvizsgálandó tárgyak felsorolásával, vagy jellemzőik segítségével történő meghatározással. Anyagi objektumok esetében ilyen jellemző lehet pld. a térbeli (megadott területen történő) elhelyezkedés. Információk keresése esetében a keresési tartomány hagyományos, vagy elektronikus információhordozók meghatározott köre, vagy azok meghatározott részei. Egy adott tartományban történő keresés megvalósítható résztartományokon végrehajtott keresések segítségével, illetve különböző tartományok keresései egyesíthetőek összevont kereséssé[6].



1. ábra. A keresés modellje, alapvető összetevői[7]

A keresés legegyszerűbb formája (anyagi objektumok esetében) a keresési tartomány, egy adott terület személyes bejárása és a keresett dolgok személyes felkutatása, megvizsgálása. Már anyagi objektumok keresése esetében is szükség lehet *segédeszközök* igénybevételére a keresett dolgok felismeréséhez és a keresési feltételeknek történő megfelelés ellenőrzéséhez (pld. aknakeresés, lemerült akkumulátorok keresése, stb.). Számos esetben – pld. nem anyagi dolgok, vagy különösen elektronikus formában tárolt információk keresése esetében – a keresés már nem személyesen, hanem egy *kereső rendszer, keresési szolgáltatás* segítségével kerül végrehajtásra. A kereső rendszer, szolgáltatás számára meghatározott formában rendelkezésre kell bocsátani a keresési igényt, ennek alapján a rendszer, szolgáltatás 'bejárja' a keresési tartományt, hozzáfér az átnézendő dolgokhoz, összeveti azokat a keresési feltétellel, majd az ennek alapján kiválasztott dolgokat, illetve a rájuk vonatkozó információkat (helyüket, elérhetőségüket, stb.) rendelkezésre bocsátja.

[5] Precision, recall.
[6] Federated search.
[7] Saját szerkesztés.

Az információkeresés sajátosságai

Az információkeresés alapvető sajátossága, hogy tárgya – amelyet a keresés alanya megtalálni, megszerezni kíván – *információ*. Az információkeresés kiinduló pontja, motivációja mindig egy információigény. Értelmezésünk szerint az információ emberhez kötődő fogalom, szorosan kapcsolódik az ismeret(ek) és a tudás fogalmához. A *tudás* – viszonylag egységesen elfogadott értelmezés szerint – a közvetlen megismerés és kommunikáció útján megszerzett, valamint a gondolkodás eredményeként létrehozott ismeretek, illetve a gyakorlás útján kialakított speciális képességek (műveletek) összessége, az *ismeretek* pedig a megismerő tevékenység eredményei, a valós vagy elképzelt világ visszatükröződései az emberi tudatban. Ezekre építve az információ a világ egy megragadott aspektusának visszatükröződése, mentális reprezentációja az emberi tudatban. [4, 134-135. o.]

Mivel az információt az emberi tudatban létező dolognak tekintjük, azokat az emberi tudaton kívül kezelni, feldolgozni, velük különböző műveleteket végezni (tárolni, továbbítani, stb.) – így köztük keresni is – csak különböző *információreprezentációk* segítségével lehet.[8] Az információk feldolgozás, vagy későbbi felhasználás (megismerés, átvétel, stb.) céljából anyagi hordozón, egyezményes formában rögzíthetőek. A rögzített információk két nagy csoportba sorolhatóak. Az első csoportot a *szemléletes információreprezentációk* alkotják, amelyek az ember által érzékelhető környezeti hatásokat viszonylag valósághű formában reprodukálják, míg a második csoportba az *absztrakt információreprezentációk* tartoznak, amelyek az előbbiekkel szemben nem hordoznak a valósághoz hasonló jellemzőket, kapcsolatuk az általuk reprezentált dolgokkal önkényes (megállapodáson alapul). [5, 10-11. o.]

Az *adatok* értelmezésünk szerint az absztrakt külső információreprezentációk szinonimáját jelentik, szemben a korábbi és részben még ma is élő értelmezéssel, amely szerint csak a numerikus és logikai adatok, mennyiségi és igaz-hamis jellegű tulajdonságok absztrakciói sorolhatók ide. Napjainkban valójában már nem kérdés a szöveges, vagy multimédiás (rajz-, képi, hang, stb.) adatok létezése, illetve besorolása. Vagyis nincs olyan rögzített információreprezentáció, ami ne lenne adat.

Az adatok (információreprezentációk) strukturáltságuk alapján három nagy csoportba, a strukturált, a félig-strukturált és a nem strukturált adatok körébe sorolhatóak. A *strukturált adatok* közé a relációs adatbázisokban tárolt, tágabb értelemben a táblázatos adatokat sorolják. Ezek olyan adatok (adategyüttesek), amelyek típusokba (egyedtípusokba, osztályokba) sorolt gondolati egységek (egyedek) jellemzőit reprezentálják. Egy típusba tartozó egyedek ugyanazon jellemzőkkel kerülnek leírásra, az egyedeket leíró jellemzők típusa, formátuma és sorrendje meghatározott. Az adatok struktúráját leíró séma és a tényleges adatok egymástól elválnak, utóbbiak a séma nélkül kezelhetetlenek, értelmezhetetlenek.

A *nem strukturált adatok* közé olyan adatok tartoznak, amelyek tetszőleges típusúak lehetnek, nem követnek kötelezően egyetlen formai, sorrendi előírást, vagy szabályt. Ide tartoznak a szöveges adatok, illetve a szemléletes reprezentációk (álló- és mozgóképek, hangfelvételek). A *félig strukturált adatok* struktúrája a strukturált (táblázatos) adatokhoz képest jóval szabadabb, kötetlenebb. Ezek is típusokba sorolt egyedek jellemzőit reprezentálják, azonban az egyes egyedeket leíró jellemzők nem feltétlenül azonosak, a jellemzők típusa, formátuma, sorrendje eltérhet, létezésük nem feltétlenül kötelező. Ide tartoznak mindenekelőtt az XML formátumú dokumentumok és a különböző formalizált üzenetek.

Az információkeresés eredményeként kapott információreprezentációk rendeltetése, hogy értelmezésük segítségével a keresés alanya információhoz jusson, bővítse, módosítsa

[8] Az emberi emlékezetben történő "kereséssel" jelen publikációban nem foglalkozunk.

ismereteit. Ez viszont igaz minden információszerzésre, információfeldolgozásra is, így az információkeresést – bár nem mindig könnyű – el kell határolni az információ előállítástól, amely egy információigényt a keresés eredményeinek további feldolgozásával elégít ki. Ezzel azonban részletesebben majd a következő pontban foglalkozunk.

AZ INFORMATIKAI ESZKÖZÖKKEL SEGÍTETT INFORMÁCIÓKERESÉS ALAPJAI

Az információkeresés kérdései a tudományos vizsgálat tárgyaként intenzívebben a nagytömegű információkban történő kereséshez kapcsolódóan, a XX. század közepén jelentek meg. Természetesen a probléma ennél sokkal régebbi, a könyvtártudomány és előzményei már az ókortól foglalkoztak az írott információforrások gyűjtésének, rendszerezésének és rendelkezésre bocsátásának feladataival. Az igényelt információkat tartalmazó 'könyvtári dokumentumok' előkeresését már akkor különböző megoldások (katalógusok, osztályozási rendszerek, stb.) segítették. [6]

A számítógépek megjelenése más funkciók mellett megteremtette a lehetőségét az információk (pontosabban az azokat hordozó adatok) tárolásának és a tárolt adatok igény szerinti rendelkezésre bocsátásának is. Az információtechnológia fejlődése, a hálózatok megjelenése a hagyományos megoldásokhoz képest elképzelhetetlen mennyiségű információ technikai elérhetőségét teremtette meg. Azonban az információk ebben a tömegben a keresés megfelelő támogatása, megoldásai nélkül egyre kevésbé hasznosultak, egyre kevésbé jutottak el a lehetséges felhasználókig. Ennek megoldására jelentek meg az 1950-es évektől az információkereséshez kapcsolódó szakterületek.

A továbbiakban vizsgálatainkat az informatikai eszközök segítségével történő információkeresésre szűkítjük. Ennek keretében bemutatjuk az információtárolás és visszakeresés alapjait, főbb típusait; összegezzük, elemezzük az információkeresésnek az adatok strukturáltságáról függő sajátosságait; végül megfogalmazzuk az információkeresés általános fogalmát.

Információtárolás és visszakeresés

Az informatikai szakterület, az informatikai megoldások esetében az információkeresés fogalma, feladatai kezdettől szorosan összekapcsolódtak az információtárolás feladataival. Ennek alapját az képezte, hogy a keresési tartományt vagy maguk az informatikai rendszerekben tárolt információk, vagy a hagyományos információhordozók informatikai rendszerekben tárolt leírásai alkották. Az információkeresés így a tárolás és visszakeresés[9] részeként jelent meg.

Az információtárolás és visszakeresés kérdései a hozzáférhető információk körének ugrásszerű bővülésével és ezek pontos és gyors elérése egyre nehezebbé válásával az 1940-es évek második felében jelentek meg és az 1960-as évek első felében kerültek az érdeklődés homlokterébe. Egyre gyakoribbá vált, hogy egy adott információigényt kielégítő, releváns információ nem került felhasználásra, mert feltáratlan maradt, ami sok esetben újbóli előállításukhoz is vezetett. Az információkeresés, mint szélesebb körben elérhető lehetőség, az 1960-as években megjelent adatbázis-kezelő, illetve információ-visszakereső rendszerekhez kapcsolódott.

Az *adatbázisokban történő keresés* az információkeresés egy speciális típusa. *Adatbázis* alatt legáltalánosabb értelemben logikailag összefüggő, meghatározott szerkezetben tárolt adatok gyűjteményét értjük, amelyek a valóság meghatározott aspektusait reprezentálják és rendeltetésük ilyen adatok tárolása és rendelkezésre bocsátása különböző alkalmazások

[9] Storage and retrieval.

számára, ezeken keresztül pedig különböző felhasználói igények kielégítésére. Az *adatbázis-kezelő rendszerek* olyan szoftver rendszerek, amelyek lehetővé teszik adatoknak adatbázisokban történő tárolását, módosítását és elérését.

Az adatbázisok, illetve az azokat kezelő adatbázis-kezelő rendszerek osztályozhatóak a bennük tárolt adatok típusai és az adatbázis struktúrája szerint. Kezdetben a lehetséges adattípusok közé csak a numerikus, a logikai, a dátum-időpont és a korlátozott méretű karaktersorozat típusú adatok tartoztak, amelyek tárolására az 1970-es évek óta szolgál a relációs adatmodell. A lehetséges adattípusok köre később folyamatosan bővült a hosszabb szövegekkel, rajzokkal, multimédia adatokkal (álló- és mozgókép, hang), illetve számos új adatformátummal (pld. XML, vagy RDF dokumentumok).

Az adatbázisok kezelése során végrehajtható műveletek különböző csoportokba sorolhatóak, amelyek különböző utasítások segítségével valósíthatóak meg. Ezek közé tartoznak mindenekelőtt az adatstruktúrák létrehozását, módosítását biztosító adatleíró utasítások; az adatokkal végzett műveleteket (létrehozás, tárolás, módosítás, mozgatás, törlés, stb.) biztosító adatkezelő utasítások; az adatok visszakeresését biztosító lekérdező utasítások; valamint az adatbázis-műveletek végrehajtását irányító tranzakció-vezérlő utasítások. Napjainkban az adatbázisok kezelésének alapvető eszköze a fenti utasításokat magában foglaló SQL nyelv.[10]

Az adatbázis-kezelés egyik fő feladata a meghatározott feltételeknek megfelelő adatok megkeresése és rendelkezésre bocsátása. A keresés alapját a lekérdező nyelven megfogalmazott *adatbázis lekérdezés*[11] ('kérdés') – egy információ igény formális megfogalmazása – alkotja, amelyre az adatbázis-kezelő rendszer 'válaszként' a keresett, a lekérdezésben megfogalmazott körből a megadott feltételeknek megfelelő adatokat válogatja ki, bocsátja rendelkezésre.[12] Az adatbázis lekérdezések (köztük a relációs adatbázisok SQL lekérdezései) túlnyomórészt az információ visszakeresés ún. Boole modelljére épülnek: a feltételek adatelemekre vonatkozó elemi feltételekből felépülő logikai kifejezések. Relációs adatbázisok és az SQL lekérdezés esetében a keresés összekapcsolódhat az új információk (pld. összegző, tömörítő értékek) előállításával.

Az *információ visszakeresés*[13] fogalma az adatbázisokban történő kereséssel ('adat visszakereséssel') szembeállítva, lényegében dokumentumok visszakereséseként került megfogalmazásra. Eszerint az információ visszakeresés az információkeresés egy speciális típusa, "egy információigénynek megfelelő nem strukturált (általában szöveges) anyagok (általában dokumentumok) megtalálása nagy (általában számítógépeken tárolt) gyűjteményekben". [7, 1. o.]

A bibliográfiai adatbázisokban történő keresésből megszülető fogalom eredeti értelmezése szerint az információ visszakeresés célja, rendeltetése nem az információigényben meghatározott információk, hanem az ezen információkat tartalmazó *dokumentumok, információhordozók létezésére, hollétére vonatkozó információk rendelkezésre bocsátása*. "Egy információ visszakereső rendszer nem nyújt információt (nem változtatja meg a felhasználó ismereteit) a kérdés tárgyáról. Egyszerűen csak tájékoztatja a kéréséhez kapcsolódó dokumentumok létezéséről (vagy nem létezéséről) és hollétéről." [8, 1. o.] Ez így van a napjainkban már az informatikai rendszerekben tárolt dokumentumok között kereső rendszerek esetében is.

Az információ visszakeresés folyamata fő vonalaiban hasonló az adatbázis keresés folyamatával: az információ visszakereső rendszer egy lekérdezés formájában megfogalmazott információigényt összevet az elérhető dokumentumokról rendelkezésére álló

[10] Structured Query Language.
[11] Database query.
[12] A lekérdező nyelvek megjelenéséig a lekérdezések megvalósítására egyenként programot, eljárást kellett írni.
[13] Information retrieval.

információkkal és válaszként az igénynek megfelelő dokumentumok listáját (elérhetőségét) bocsátja rendelkezésre. A keresés részleteiben és eredményében azonban jelentős különbségek vannak.

Talán a legfontosabb a megfelelés kritériuma, ami az adatbázis-keresés pontos egyezésével szemben az információ visszakeresés esetében a *relevancia* (fontosság, tárgyhoz tartozás). A relevancia a kategorikus igen/nem helyett sorrendbe rendezett értékekkel jellemezhető, meghatározása jóval nehezebb feladat (amelyre különböző megoldások születtek és jelennek meg napjainkban is). Szorosan kapcsolódik ehhez a második különbség, a relevancia szerinti *rangsorolás*, ami az adatbázis-keresésből hiányzik. A keresés így részleges megfelelőség esetén is szolgáltat eredményt és azok közül kiemeli a 'legjobbakat'. Az információ visszakeresés történhet a dokumentumokat leíró adatok (pld. szerző, cím, kulcsszó, tárgyszó) segítségével, vagy a dokumentumok teljes tartalmának feldolgozásával.

Az eredményes és hatékony információ visszakeresés alapvető feltétele a keresési tartományt képező *dokumentumok előzetes feldolgozása*, amely lehet manuális és automatizált. Az feldolgozás eredményeként létrehozott leíró információk rendeltetése a (későbbi) keresés teljesítményének, gyorsaságának optimalizálása.[14] Ezen információk nélkül a keresés során végig kellene vizsgálni a keresési tartományt, az összes dokumentumot, ami nem hatékony, számos esetben nem is megvalósítható. Az előzetes feldolgozás feladatai az információ visszakereséshez kapcsolódóan számos különböző megnevezés alatt, részben sajátos tartalommal jelennek meg, pld. katalogizálás, indexelés, leíró adatok (metaadatok) előállítása.

Az információkeresés sajátosságai az adatok strukturáltsága szerint

Az informatikai rendszerekben tárolt információk keresése (visszakeresése) az alkalmazott információreprezentációk jellegétől függően különböző sajátosságokkal rendelkező megoldásokra épült, jelentőségük és lehetőségeik az idők során folyamatos változásokon ment keresztül. Ehhez kapcsolódóan az információreprezentációk (adatok) alapvető típusait strukturáltság szempontjából az előző pontban már ismertetett strukturált, strukturálatlan és félig-strukturált adatok, illetve ezek kombinációi alkotják.

A rendelkezésre álló háttértár-kapacitás és az információtárolás lehetőségeinek folyamatos bővülésével egyre több adat keletkezik strukturálatlan és félig strukturált formában. Egyes megállapítások szerint a szervezeti információk 80-85%-a tartozik ebbe a körbe, bár ezt valós felmérések pontosan még nem támasztották alá. Mindesetre a strukturálatlan és félig-strukturált adatok – melyek az adat-univerzum 'sötét anyagát' képezik – elérése, feldolgozása és így a bennük történő információkeresés jelentősége is folyamatosan nő.

A *strukturált adatokban történő keresés* alapját a már említett adatbázis-kezelés, illetve a táblázatkezelés lehetőségei képezik. Hagyományos megoldásai, lehetőségei régóta léteznek, hosszú évek tapasztalatai alapján alakultak ki és biztosítják a relációs adatbázisokban, (számoló)táblázatokban tárolt adatok közötti keresést. Az információ visszakeresés szakirodalma a keresés ezen típusát *adat visszakeresésnek* nevezi és lényegének az objektumok (egyedek) jellemzőire és kapcsolataira vonatkozó tényeket, elképzeléseket hordozó ún. propozicionális (állítás-alapú) információreprezentációk kinyerését tekinti. Az adatok strukturáltságából következően a keresés információigénye könnyebben, bár nem minden esetben könnyen alakítható formalizált lekérdezéssé. Ehhez azonban ismerni kell a keresési tartományt képező adatbázis, táblázat struktúráját (sémáját) és az egyes adatelemek formátumát, értékkészletét.

A strukturált adatokban történő keresés sajátossága, hogy az információigény megfogalmazása során felhasznált elemi keresési szempontok (feltételek) a táblázatos formában tárolt

[14] Az ún. indexelés az adatbázis-kezelésben is létező megoldás a keresések gyorsítására.

adatok egyes mezőinek vizsgálatával közvetlenül, minden előkészítő tevékenység nélkül ellenőrizhetőek. Ezen kívül ezen adatok tartalma és formátuma (talán csak a karaktersorozat mezőktől eltekintve) viszonylag jól meghatározott.

A *strukturálatlan adatokban történő keresés* elsőként a szöveges dokumentumok[15] visszakeresése formájában jelent meg. A vonatkozó szakirodalom információ (vissza)keresés alatt tulajdonképpen mindmáig – a kifejezés köznapi értelmezésétől eltérően – nagyobbrészt dokumentum (vissza)keresést és ezen belül *szöveges dokumentum (vissza)keresést* ért. [6, 7, 8, 9] A következő lépést az 1980-as évek közepén a szintén a strukturálatlan adatok közé sorolt képek, majd később a további multimédia formátumú információreprezentációk (hangfelvételek, videók) keresése képezte. A *kép/hangfelvétel/video keresés (multimédia információk keresése)*[16] adott információigénynek megfelelő képek/hangfelvételek/videók kiválasztása informatikai rendszerekben tárolt képek/hangfelvételek/videók (multimédia dokumentumok) gyűjteményéből.

A strukturálatlan adatok (szöveges és multimédia dokumentumok) keresésének legegyszerűbb módszere az előzőekben már említett, az egyes dokumentumokhoz kapcsolódó *leíró adatokban történő keresésre* épül. A dokumentumok 'természetes' leíró adatai (szöveges dokumentum szerzője, címe, hossza, keletkezés időpontja, stb.; kép készítője, címe, helyszíne, mérete, készítés időpontja, stb.; hangfelvétel, videofelvétel címe, szereplői, hossza, felvétel időpontja, stb.) a dokumentum tárolásával együtt kerülnek rögzítésre. Ezen adatok segítségével lényegében alkalmazhatóak a strukturált adatokban történő keresés módszerei.

A dokumentumok keresése történhet *kategorizáló adatok* (kulcsszavak, tárgyszavak, tartalmi kategóriák, stb.) segítségével, amelyeket megadhat a dokumentum szerzője, készítője, meghatározhatnak a dokumentum gyűjteményt kezelő szakemberek és meghatározhatóak a dokumentumok tartalmának automatizált elemzésével, feldolgozásával. A kategorizáló adatok meghatározhatóak szabadon, vagy előre rögzített kategória-listák felhasználásával. Az egyes kategóriák jelentéstartalmuk, kapcsolataik alapján fogalom-rendszerekbe (taxonómiák, tezauruszok, ontológiák) rendezhetőek, amelyek a keresés során is felhasználhatóak.

A keresés szöveges dokumentumok esetében lehetséges a dokumentumban előforduló valamennyi szó figyelembe vételével. A *teljes szöveges keresés* jellemzően az előforduló szavakra, kifejezésekre, esetleg azoknak a dokumentum adott részeiben (pld. cím, főszöveg, stb.) történő előfordulására, vagy egymáshoz viszonyított elhelyezkedésére vonatkozó feltételek alapján történik.[17] Kisebb dokumentum gyűjtemények esetében a feltétel ellenőrzése történhet a dokumentumok keresés során történő feldolgozásával, nagyobb számú dokumentum esetében azonban már teljes szöveges kereső indexek felhasználása szükséges.

A *strukturálatlan dokumentumok tartalom-alapú keresése* során hatékonyan használhatók fel az információkinyerés egyes korszerű módszerei. Ezek a lehetséges információigényekhez, keresési szempontokhoz igazodó módon határoznak meg, emelnek ki tartalmi elemeket, jellemzőket. Ide tartozik például szöveges dokumentumok esetében a névelem-felismerés[18], a képi és video dokumentumok esetében az arc/személy, illetve tárgy/helyszín felismerés, vagy a hangfelvételek esetében a hang/beszédfelismerés, beszélő/előadó felismerés, illetve zene felismerés.

A *félig strukturált adatokban történő keresés* jelentősége az Interneten elérhető ilyen típusú adatok (dokumentumok) mennyiségének ugrásszerű bővülésével nőtt meg. Ezen adatok a strukturált adatokhoz hasonlóan – mint azt korábban már megjegyeztük – egyedek (entitások) jellemzőit és kapcsolatait reprezentálják, azonban a táblázatos formátumhoz képest jóval rugalmasabb formában, jellemzően fa-struktúrába rendezetten. Az információkat a fa

[15] Pontosabban olyan dokumentumok, amelyek információkat alapvetően szöveges formában tartalmaznak.
[16] Image retrieval, audio retrieval, video retrieval, multimedia information retrieval.
[17] További teljes szöveges keresési eszközök: helyettesítő karakterek, reguláris kifejezések használata.
[18] Named entity recognition, named entity extraction.

egyes csomópontjai (az azokban tárolt adatok) és a csomópontok közötti kapcsolatok hordozzák. A keresés ilyen esetben az információigénynek megfelelő, releváns összefüggő dokumentum-részek megtalálására és rendelkezésre bocsátására irányul.

A félig strukturált adatokban történő keresés módszerei még kevésbé kimunkáltak, mint a két másik csoport esetében, azonban léteznek megoldások, lekérdező nyelvek XML dokumentumokban csomópontok kiválasztására (XPath) és adatok lekérdezésére (XQuery); relációs adatbázisokban XML adatokra is kiterjedő lekérdezésekre (SQL/XML); vagy RDF dokumentumokban tárolt adatok lekérdezésére (SPARQL[19]).

A szakirodalomban találkozhatunk a *részben strukturált adatok* fogalmával is, amelyek olyan adatok, amelyek nagyobb része strukturált, de vannak strukturálatlan összetevőik is. [10] Ez a típus a strukturált és a félig strukturált adatok között helyezkedik el. Ide sorolható számos olyan formalizált dokumentum, amelyben az alapvetően strukturált adatokat kiegészítik szabad szöveges, vagy multimédiás részek (pld. jelentések, jegyzőkönyvek, hibabejelentések, igénylések, orvosi vizsgálati lapok, stb.). Az ilyen dokumentumok tárolhatóak nem strukturált adattípusokat is tartalmazó relációs adatbázisokban és félig strukturált (XML) dokumentumok formájában is. Esetükben a keresés során a strukturált (vagy félig strukturált) és a nem strukturált adatokban történő keresés módszereinek kombinációjára van lehetőség.

Az információkeresés napjainkban *új kihívások* előtt áll. Mint azt érzékeltettük, a különböző strukturáltságú adatokban történő keresés sokszor jelentősen eltérő lehetőségeket biztosít, eltérő módszerekre, megoldásokra épül. Egyre növekszik azonban az igény az egymástól független, vagy elosztott *heterogén forrásokban történő keresés* lehetőségére, amely az egyes adattípusok sajátosságaira épülő, eltérő kereső módszerek összekapcsolását, harmonizálását igényli.

Egy másik kihívás az ún. "*Nagy Adatok*"[20] megjelenése. Az eredetileg a nagymennyiségű, minden korábbinál részletesebb, sokféle – elsősorban nem vagy félig strukturált – adatok kezelését és elemzését leíró kifejezés divatszóvá vált, egységes értelmezése még nem alakult ki. Témánk szempontjából fontos kiemelni, hogy a Nagy Adatnak nem egyedüli, bár kétségkívül alapvető kritériuma a méret. Legalább olyan fontos változatossága és keletkezésének gyorsasága is. [11, 4. o.] Nagy Adat alatt ma széles körben olyan nagy adathalmazt értünk, amely mérete és összetettsége miatt a rendelkezésre álló eszközökkel és módszerekkel nehezen kezelhető (tárolható, kereshető, elemezhető, vizualizálható, stb.). Mindez tehát új keresési módszereket is igényel.

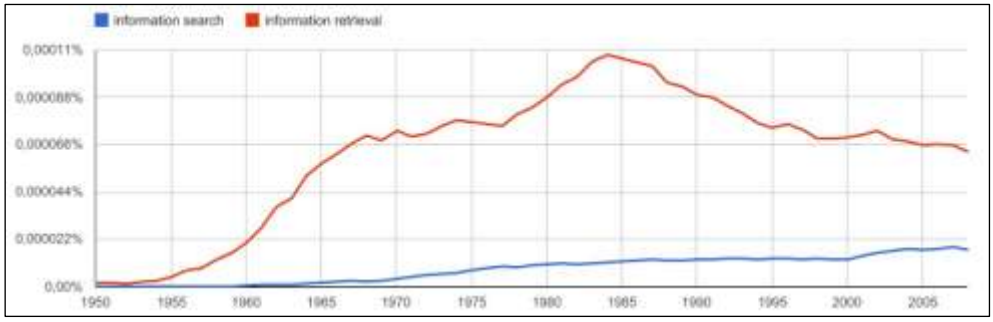
ÖSSZEGZÉS, AZ INFORMÁCIÓKERESÉS FOGALMA, ÉRTELMEZÉSE

Az eddigiekben elmondottak alapján indokoltnak látszik meghatározni az információk kereséséhez kapcsolódó alapfogalmat és annak tartalmát. Ezt megelőzően azonban röviden tekintsük át a 'visszakeresés' és 'információ visszakeresés' kifejezések használatát, értelmezését. A *visszakeresés* köznapi értelemben több jelentést is takar, de a magyar nyelvben közvetlenül az információkereséshez kapcsolódik: "<Adatot, vmely mutató v. utalás alapján> az eredeti helyen (könyvben, táblázatban) megkeres." [12, 481. o.] Angol nyelven az informatikához kapcsolódóan hasonló értelmezéssel találkozhatunk: " 9. (adat) helyének megállapítása és beolvasása tárolóból, pld. képernyőn történő megjelenítésre."[21] [3, 1644-1645. o.] Az információ visszakeresés kifejezés a Magyar Nyelv Értelmező Szótárában nem szerepel, angolul pedig meghatározott információk tárolt adatokból történő visszanyerését

[19] SPARQL Protocol and RDF Query Language.
[20] Big Data.
[21] To locate and read (data) from storage, as for display on a monitor.

értjük alatta: "3. Adatok szisztematikus tárolása és visszanyerése ügyiratból, cédulakatalógusból, vagy egy számítógép memóriájából."[22] [3, 980. o.]

Az *információkeresés és információ visszakeresés* kifejezések használata, mint az előző pontokban elmondottakból is érzékelhető, elsősorban elkülönülő szakterületek terminológiai gyakorlatára, értelmezésére épül. A relációs adatbázisokban történő keresés a széles körben elfogadott értelmezés szerint nem tartozik az információ visszakereséshez (mivel strukturált adatokhoz, relációs adatbázisokhoz kapcsolódik), pedig a köznapi értelmezés tartalmának teljesen megfelel. Mint az a következő ábrából is látható, az információ visszakeresés kifejezés jóval elterjedtebb, mint az információkeresés, bár használata az 1990-es évektől visszaesőben van.



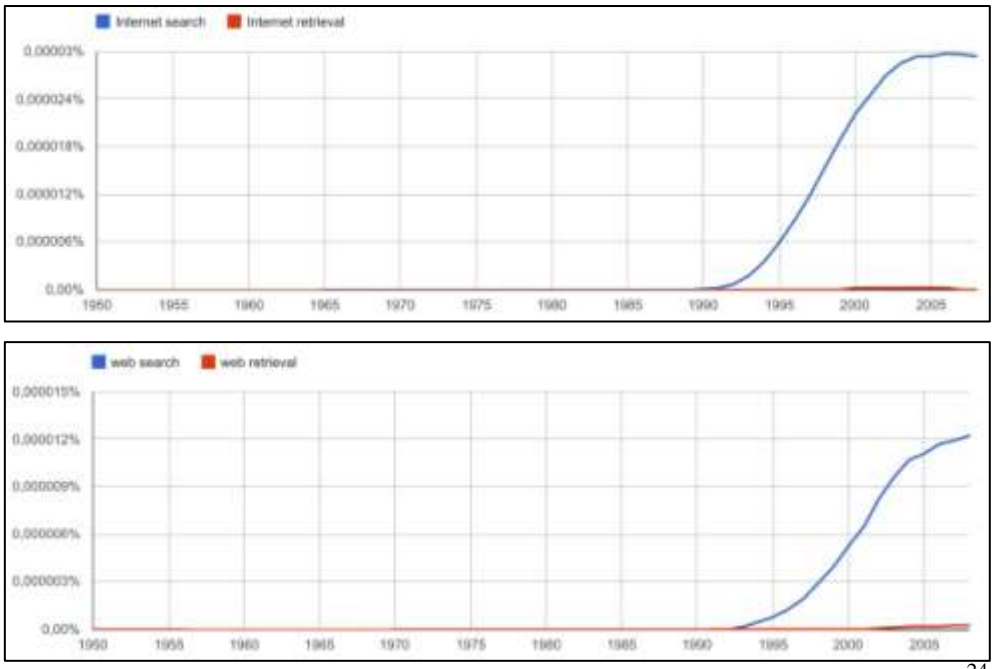
2. ábra. Információkeresés és visszakeresés kifejezések előfordulása 1950-2008 között[23]

A szakirodalomban találkozhatunk a két kifejezés más szempontok szerinti megkülönböztetésével is, amely szerint a keresés egy emberi tevékenység, amelynek során információ visszakereső rendszerek is felhasználásra kerülnek, az információ visszakeresés pedig a keresés technikai megvalósítását jelenti. Az előbbi az emberre és annak az információ visszakereső rendszerhez kapcsolódó viselkedésére, feladataira (keresési stratégia megválasztása, visszanyert információk relevanciájának megítélése), míg az utóbbi a visszakereső rendszer funkcióira, működésére fókuszál. [13, 1517. o.] Bár e megközelítésben van logika, témánk szempontjából nincs előnye és széles körben nem is terjedt el.

Az információkeresés (vagy információ visszakeresés) fogalmát megítélésünk szerint olyan tágan célszerű meghatározni, amely magában foglal minden tevékenységet, amelynek rendeltetése meglévő információreprezentációk (adatok), információforrások kiválasztásával és rendelkezésre bocsátásával hozzájárulni információigények kielégítéséhez. Ennek indokát abban látjuk, hogy a felhasználó szempontjából érdektelen, hogy az információigényeit milyen formátumban – relációs adatbázisokban, vagy szöveges visszakereső rendszerekben – kezelt, tárolt adatok segítségével elégítjük ki és az eltérő lehetőségektől, szolgáltatásoktól eltekintve érdektelenek a megvalósításbeli különbségek is. Ezen felül napjainkban már egyre inkább alapvető jelentőségűvé válik a számos különböző forrást felhasználó összevont keresés.

Ezt követően dönteni kell arról is, hogy a fenti tartalmat hordozó fogalom megnevezése *információkeresés, vagy visszakeresés* legyen. A 2. ábra tartalma alapján az információ visszakeresés lenne a logikus megoldás, azonban napjainkban az információk keresése (vagy visszakeresése) már jellemzően nem egy adott rendszerből, hanem az Interneten, illetve a World Wide Web-en történik. Ehhez kapcsolódóan viszont – mint azt a következő ábra is szemlélteti – a két kifejezés gyakoriságában már más a helyzet. Az angol terminológiában az ok talán abban rejlik, hogy nem az általunk tárolt információkat 'keressük vissza', hanem egy 'ismeretlen helyen' keresünk.

[22] The systematic storage ad recovery of data, as from a file, card catalog, or the memory bank of a computer.
[23] Forrás: Google Ngram Viewer.



3. ábra. Internet és web keresés kifejezések előfordulása 1950-2008 között[24]

A fentiekre építve az *információkeresés fogalma* alatt átfogó értelemben olyan tevékenységet javaslunk érteni, amely információreprezentációk (adatok) meghatározott köréből meghatározott információigény kielégítését segítő információreprezentáció(k), adat(ok) megtalálására, kiválasztására irányul. A definíció nem határozza meg, nem korlátozza a kezelt adatok strukturáltsági típusát, így magában foglalja valamennyi, korábban már említett keresési típust. Az információreprezentációk lehetnek táblázatos formába rendezett (relációs) adatok, dokumentumok teljes szövegű változatai, vagy dokumentumokat leíró tömör reprezentációk ('katalógus cédulák', publikáció referátumok, stb.). Az egyes keresési típusok, változatok a meghatározó sajátosságok beépítésével ebből a fenti fogalomból könnyen származtathatóak. A javasolt fogalom így megfelelő kiinduló alapot szolgáltat az információkereséshez és ezen belül a szemantikus kereséshez kapcsolódó kutatások számára.

Felhasznált irodalom

[1] A magyar nyelv értelmező szótára. Harmadik kötet. H-Kl. – Akadémiai Kiadó, Budapest, 1965.

[2] Oxford Dictionaries Online. – Oxford University Press, 2012. www.dcs.bbk.ac.uk/research/.../bbkcs-00-14.pdf, letöltve: 2012.12.05.

[3] Webster's Encyclopedic Unabridged Dictionary of the English Language. – Gramercy Books, New Work/Avenel, 1996.

[4] MUNK Sándor: Információs színtér, információs környezet, információs infrastruktúra. – Nemzetvédelmi Egyetemi Közlemények, 2002 (VI.) /2. (133-154.o.)

[5] MUNK Sándor: Katonai informatika I. A katonai informatika alapjai. Egyetemi jegyzet. – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2003.

[6] SINGHAL, A.: Modern information retrieval: a brief overview. – IEEE Data Engineering Bulletin, 2001 (24.)/(4) (35-43. o.)

[24] Forrás: Google Ngram Viewer.

[7] MANNING, Christopher D.–RAGHAVAN, Prabhakar–SCHÜTZE, Hinrich: An introduction to information retrieval. – Cambridge University Press, 2009.

[8] RIJSNBERGEN, C. J. van: Information retrieval. 2nd edition. – Butterworth, London, 1979.

[9] BAEZA-YATES, R.–RIBERIO-NETO, B.: Modern information retrieval. – ACM Press, New York, 1999.

[10] KING, P. J. H.–POULOVASSILIS, A.: Enhancing database technology to better manage and exploit partially structured data. Research Report BBKCS-00-14. – Birkbeck University of London, 2000. www.dcs.bbk.ac.uk/research/techreps/2000/bbkcs-00-14.pdf, letöltve: 2012.12.07.

[11] Oracle Information Architecture: An Architect's Guide to Big Data. – Oracle Corporation, 2012.

[12] A magyar nyelv értelmező szótára. Hetedik kötet. U-Zs. – Akadémiai Kiadó, Budapest, 1966.

[13] JANSEN, Bernard J. – RIEH, Soo Yung: The seventeen theoretical constructs of information searching and retrieval. – Journal of the American Society for Information Science and Technology, 2010 (61)/8., 1517-1534. o.

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Nagyné Takács Veronika
takacs.veronika@nav.gov.hu

ADATVAGYON-GAZDÁLKODÁS A KÖZIGAZGATÁSBAN - A FOGALMI TISZTÁZÁSTÓL A STRATÉGIAALKOTÁSIG I.

Absztrakt

A közfeladatot ellátó szervek által kezelt adatokban megtestesülő érték jelentőségét, az adatvagyon védelmének, megőrzésének és hasznosításának szükségességét ma már senki nem vitatja. Az elvi kérdések és a gyakorlati problémák akkor merülnek fel, amikor az adatok minél teljesebb körű és minél hatékonyabb felhasználásának megtervezésével és végrehajtásával kapcsolatos feladatok meghatározására kerül a sor.

Today no one disputes the need of protection, conversation and utilization the value of data which appears in the public service missions. Many theoretical issues and practical problems arise when the design and implementation tasks of data using is determined.

Kulcsszavak: *adat, adatvagyon-gazdálkodás, közfeladatot ellátó szervek adatai, közadat ~ data, data asset management, public sector information*

BEVEZETÉS

Az adatvagyon-gazdálkodás viszonylag újkeletű fogalom a közigazgatás területén. A kifejezés az üzleti szférából érkezett, és egyértelműen utal arra a vitathatatlan tényre, hogy a gyűjtött, feldolgozott adatokban megtestesülő tudás olyan érték, amelyet tervezetten, szervezetten és megfelelő biztonsági követelmények érvényesítése mellett kell kezelni, felhasználni.

A napjainkban népszerű fogalmat sokan, sokféleképpen használják. A legelterjedtebb megközelítés szerint alapvetően informatikai tevékenység: a jellemzően elektronikus formában létező adatok informatikai eszközökkel történő kezelését biztosító eljárások összessége. Ez a felfogás azonban felülvizsgálatra szorul, ugyanis figyelmen kívül hagyja azt a tényt, hogy az informatikai tevékenység – bár a közigazgatás eredményes működése szempontjából alapvető jelentőségű – nem lehet öncélú és önmagában nem lehet eredményes.

A közigazgatási adatvagyonnal történő gazdálkodás céljai és tartalma a közigazgatási alaptevékenység céljaiból és tartalmából vezethetők – vezetendők – le, módszereinek és eszközeinek az igazgatási tevékenység ad keretet. Az informatikai tevékenység az előbbiekben meghatározott célokhoz, tartalomhoz és keretekhez illeszkedve segíti elő a maga sajátos eszközrendszerével a közigazgatási szervezetrendszer jogszerű, szakszerű és hatékony feladatellátását.

Az előzőekből következően nemcsak az adatvagyon-gazdálkodás mint közigazgatási tevékenység fogalmát szükséges meghatározni; tisztázásra szorul kapcsolódása más – adat- és információkezeléssel, illetve -védelemmel összefüggő – közigazgatási tevékenységekhez is.

A kétrészes tanulmány első fele az adatvagyon-gazdálkodással kapcsolatos alapfogalmak tisztázását és rendszerezését, második fele a stratégiaalkotás előkérdéseinek áttekintését tűzte ki célul.

AZ ADATVAGYON-GAZDÁLKODÁS ALAPFOGALMAI

Az adat

Évtizedek óta nyitott kérdés az *adat – információ – tudás* fogalom-hármas meghatározásának, elhatárolásának problémája. A fogalomtörténeti áttekintést mellőzve – jelen tanulmány tárgyára tekintettel – az alábbiakat célszerű átgondolni.

Sem az adat, sem az információ, sem a tudás fogalma vonatkozásában nem áll rendelkezésre olyan definíció, amely általános kiindulópontként szolgálhatna.

Konszenzus van abban, hogy az *adat* fizikailag érzékelhető (látható, hallható), más megfogalmazás szerint rögzített tény (létező vagy létezett dolog). Az *érzékelhetőség* helyett célszerűbb a *rögzítettség* kifejezés alkalmazása, a kettő közötti – lényeges – különbség a megőrzöttség, a visszakereshetőség, az egynél többszöri lehetőség az érzékelésre. Az adat fogalmának további elemei tekintetében már erős „szóródás” tapasztalható; a meghatározások az „önmagában jelentéssel nem bíró” valóságdarabtól [1] az „ismert vagy feltételezett dolog, valószínűsítés vagy feltevés” fogalmáig [2] terjednek.

Az *információ* meghatározásának nehézségeire Fülöp Géza mutat rá, amikor Schradert és Ottent idézve megállapítja, hogy a száznál is több definíció az információnak csak egy-egy aspektusára ad fogalmi választ, [3] majd kiemeli a matematikai (információelméleti) és a filozófiai (ontológiai és ismeretelméleti) megközelítést.

Az adat és az információ közös jellemzője az önálló lét (rögzíthetők, tárolhatók, törölhetők, mások számára hozzáférhetők stb.), elhatárolásuknál jellemzően két elem hangsúlyos. Az adathoz képest az információ egyrészt értelmezett, értékelt (valamiféle szellemi tevékenységet, szellemi többletet feltételez), másrészt „újat” tartalmaz, ami változást idéz elő a befogadó tudatában, ebből következően gyakran a viselkedésében is.

Mindkét megállapítás igaz – egy adott időpontban. Történetileg szemlélve az információt az újabb adatok és információk felülírják, újdonsága elvész, kiindulópont jellege megerősödik, egyre jobban „hasonlít” az adatra.

Míg az adat és az információ „kézzelfogható”, a *tudás*ra - az adatok és az információk kezelésének képességére – az jellemző, hogy „nehéz explicitté tenni, rögzíteni, továbbadni”. [4]

Jelen tanulmány az adat jogszabályi definíciója hiányában – fentiekre is tekintettel, de a megoldatlan kérdés megválaszolásra nem vállalkozva – a közigazgatás számára egy gyakorlati megközelítésű definíció-javaslatot tesz: *az adat: rögzített tény vagy tényből kiinduló értékelés, következtetés, feltételezés* - ami egyébként újabb értékelések, következtetések, feltételezések alapja lehet.

Az *adat* – tartalom és ezzel szoros összefüggésben nyilvánosság (megismerhetőség) alapján elhatárolható – *fajtái*t jogszabályok nevesítik. Törvények határozzák meg a *személyes adat*, a *közérdekű adat*, a *közérdekből nyilvános adat*, [5] az *üzleti titok*, [6] az *adótitok*, [7] a *vámtitok*, [8] a *banktitok*, [9] az *értékpapírtitok*, [10] a *biztosítási titok*, [11] a *foglalkoztatói nyugdíjtitok*, [12] *fizetési titok*, [13] a *minősített adat* [14] és a *döntés-előkészítő nem nyilvános adat* [5] fogalmát, továbbá összefoglaló megnevezésként megjelenik a *törvény által védett titok* kategóriája is. [15] A szabályozás széttagoltságából is adódóan a meghatározások eltérő szempontrendszert tükröznek, mélységük változó, az egyes fogalmak között átfedések, olykor ellentmondások találhatók, ezek részletes bemutatása és értékelése meghaladná jelen tanulmány kereteit.

Az adat *megjelenési formái*t tekintve – az adathordozótól függően – lehet papír alapú vagy elektronikus, illetve hang-, kép- vagy audiovizuális.[16]

Az adatkezelés és az adatfeldolgozás

Az *adatkezelés* és az *adatfeldolgozás* fogalmát 1992 óta határozta meg jogszabály; [17] az eredeti definíciókat a jogalkotó 2011-ben kisebb korrekcióval továbbra is fenntartotta. [5]

Az adatokat a közfeladatot ellátó szerv azok teljes életciklusán át *kezeli*. Az adatkezelés magában foglalja az adatok *gyűjtését* (*felvételét*, *fogadását* vagy *létrehozását*), *rögzítését*, *rendszerezését*, *megváltoztatását*, *tárolását* és *őrzését* (mentését és archiválását), *felhasználását* (ügyintézésre vagy elemzésre), *lekérdezését*, *összekapcsolását* vagy *összehangolását*, *terjesztését* vagy *szolgáltatását* (*továbbítását*, *nyilvánosságra hozatalát*, *közzétételét* vagy *hozzáférhetővé tételét*), *megjelölését*, *zárolását*, *selejtezését*, *törlését* vagy *megsemmisítését,* valamint *további felhasználásának megakadályozását*. [5][1]

Az adatkezelés fogalmától elválik az *adatfeldolgozás* művelete; ez utóbbi *az adatkezelési műveletekhez kapcsolódó, technikai feladatok elvégzését jelenti, feltéve, hogy ezeket a technikai feladatokat az adatokon végzik*. [5]

2010-ben jelent meg jogszabályban az *elektronikus adatfeldolgozás* fogalma, ami a 2011-es módosítás óta *az elektronikus formában rögzített adatra vonatkozó adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzését jelenti, különösen az elektronikus úton vezetett nyilvántartás létrehozásának, működtetésének és üzemeltetésének technikai műveletét* (lásd később). [18]

Az adatkezelés jogalapját, célját, időtartamát, feltételeit, az adatkezelés jogszerűsége ellenőrzésének módját ugyancsak jogszabályok rögzítik, továbbá részletes szabályok vonatkoznak az adatfeldolgozásra is.

[1] A felsorolás alapja az Info tv.-ben szereplő *értelmező rendelkezés*, amely kiegészítésre került az adatkezeléssel összefüggő, más jogszabályokban szereplő tevékenységek megnevezésével.

Az adatvagyon

Az adatvagyon fogalmára 2010 óta létezik jogszabályi definíció, amely szerint nemzeti adatvagyon: a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége. [18] A jogszabályi meghatározás jelentős szűkítést tartalmaz: csak meghatározott adatfajtákat tekint az adatvagyon körébe tartozóknak.

Egyes adatfajták nevesítésével a jogalkotó figyelmen kívül hagyta a közfeladatot ellátó szervek által kezelt minősített adatokat, a nem nyilvános kategóriába sorolt, döntéselőkészítő dokumentumokban szereplő adatokat és a törvény által védett titok körébe tartozó, személyes adatnak nem minősülő adatokat. A közfeladatot ellátó szervek adatvagyonába azonban beletartozik (bele kell, hogy tartozzon) az általuk kezelt valamennyi adat, függetlenül tartalmuktól és nyilvánosságuktól (megismerhetőségüktől).

A közfeladatot ellátó szervek adatvagyona kapcsán szükséges jelezni azt is, hogy ezt a vagyont a feladatellátáshoz szükséges valamennyi adat alkotja, így részei a szakmai (alap)tevékenységbe, továbbá a szakmai tevékenységet támogató funkcionális (személyügyi, pénzügyi, ügyviteli stb.) tevékenységbe tartozó feladatok ellátásához szükséges adatok is.

A jogszabályban rögzített meghatározásnál lényegesen tágabb megfogalmazást nyújt egy szintén 2010-ben született kormányzati dokumentum, amely szerint: „mindazok az adatok és információk a nemzeti adatvagyon részét képezik, amelyek a társadalom, a gazdaság az állam működéséhez, a nemzethez és annak kultúrájához tartoznak”. [19] Ez a definíció inkább deklarációnak tűnik; olyan sokféle tartalmú és eltérő értéket képviselő elemekből álló adathalmazt jelent, amelynek egységes kezelése – gyakorlati oldalról – megvalósíthatatlan.

Ez utóbbi fogalom-meghatározás deklaráció-jellegét erősíti, hogy a jogalkotó a nemzeti vagyon elemeinek jogszabályi meghatározásakor a nemzeti adatvagyon említése során egyértelműen a jogszabályi definícióra utal vissza. [20]

Az adatvagyon-gazdálkodás

Az *adatvagyon-gazdálkodás* mint közigazgatási tevékenység meghatározásakor kiindulópontként szolgálhat Henri Fayol klasszikus definíciója, amely szerint *igazgatás: tervezés, szervezés, közvetlen irányítás (parancsnoklás), koordinálás és ellenőrzés*, [21] és amelyet a *gazdálkodás* fogalmának meghatározó eleme, a *költséghatékonyság* egészíthet ki.

Az *adatvagyon-gazdálkodás első (legalsó) szintjét a közfeladatot ellátó szerv adatvagyon-gazdálkodása jelenti*. Eszerint: *adatvagyon-gazdálkodás: a közfeladatot ellátó szerv – szakmai és funkcionális (különösen jogi-igazgatási és informatikai) szakterületeinek együttműködésével megvalósuló – tevékenysége. Célja, hogy a feladatellátáshoz szükséges adatok a megfelelő minőségben, mennyiségben, időben, helyen és költséggel álljanak rendelkezésre. Ennek érdekében az adatvagyon-gazdálkodás biztosítja, hogy az adatkezelés folyamatai, az adatkezelési tevékenységek tervezett, szervezett, szabályozott és ellenőrzött módon valósuljanak meg, és így elősegíti, hogy a közfeladatot ellátó szerv a tevékenységét jogszerűen, szakszerűen és hatékonyan lássa el, továbbá – amennyiben feladata – megfelelő színvonalú információk szolgáltatásával támogassa a kormányzati tevékenységet* (döntéselőkészítés és döntéstámogatás).

A közfeladatot ellátó szerv adatvagyon-gazdálkodásán túl, az „állami (nemzeti) gazdálkodás” keretein belül további két szint különböztethető meg.

Az *adatvagyon-gazdálkodás második szintjét az adatokat kezelni jogosult, közfeladatot ellátó szervek közötti adatmegosztás* (adatcsere) *és egységes* (rendszerszinten tervezett, azonos elvek szerint szabályozott, hasonló – kompatibilis – eszközrendszerrel megvalósított stb.) *adatkezelés képviseli*, ami két okból is szükséges: egyrészt az előállítás, ellenőrzés és rendszerezés költségei csak egyszer jelentkeznek a közszférában, másrészt – amennyiben az ügyfelek általi adatszolgáltatás eredményeiről van szó – az ügyfelek tehermentesítése is biztosított az egyszeri adatbekéréssel. Ez utóbbi kérdéskör kapcsán egy tanulmány

megállapítja, hogy „a magyar vállalkozások teljes adminisztrációjának csupán 30 %-a eredményez konkrét üzleti hasznot, a többit csak a törvényi kötelezettségnek való megfelelés miatt végzik”, majd hozzáteszi, „az adminisztratív teher indokolatlan, ha például ... azonos információt több szervhez és több formátumban – elektronikus úton és papíron is – el kell juttatni”. [22]

Ezen a szinten két elvi kérdés merül fel. Vitathatatlan, hogy a közfeladatot ellátó szervek adatvagyonát egységesen kell kezelni annak érdekében, hogy a párhuzamosságok miatti többlet-ráfordítások kiküszöbölhetők legyenek, az egységes kezelés azonban nem érintheti az egyes közigazgatási szereplők feladat- és hatásköri önállóságát.

Ezzel függ össze a másik felvetés is. Az egységes kezelés átfogó és egységes szabályozást és központi közigazgatási irányítást igényel, jelenleg azonban még nem látható, hogy milyen vagy melyik (már létező vagy újonnan létrehozandó) közigazgatási szerv lehet az, amelyik megfelelő kompetenciával bír ahhoz, hogy – ésszerű időn belül – felmérje, értékelje a jelenlegi adatkezelési folyamatokat, az egyesítés és egységesítés elveit kidolgozza, majd az elveknek megfelelően konszolidálja és megújítsa az adatkezeléssel összefüggő tevékenységeket, esetenként döntsön a párhuzamosságok megszüntetéséről, feladat- és hatáskörök, eljárások módosításáról. Az átalakítások nyilvánvalóan szervezetek (sőt tárcák) közötti érdekellentéteket, konfliktusokat hozhatnak felszínre.

Az *adatvagyon-gazdálkodás harmadik szintje a nemzeti szint*, *amelybe* – a már idézett meghatározás szerint – *a nemzethez és annak kultúrájához tartozó valamennyi adat kezelése beletartozik*. Ezen a szinten az adatvagyon-gazdálkodási tevékenység elsősorban a kormányzati politikaalkotást és az ágazati jogszabályok konzisztenciájának biztosítását jelenti, az operatív irányítás értelemszerűen nem hangsúlyos.

AZ ADATVAGYON-GAZDÁLKODÁS TARTALMA, TERÜLETEI

Az adatvagyon-gazdálkodás tartalma és területei a már említett cél – a feladatellátáshoz szükséges adatok a megfelelő minőségben, mennyiségben, időben, helyen és költséggel álljanak rendelkezésre – alapján határozhatók meg.

A feladatellátáshoz szükséges adatok kezelése egyrészt a megfelelő jogalap (jogszabályi rendelkezés vagy az érintett beleegyezése) alapján, másrészt a célhoz kötöttség elvének érvényesítésével történő adatkezelést jelenti.

A megfelelő minőségű adatok biztosítása az egyes adatok esetében a valódiságot, a pontosságot, a (történetileg változó) időszerűséget, a teljességet, több forrásból származó azonos adatok esetén a konzisztenciát jelenti.

A megfelelő mennyiségű adat biztosítása két kérdéskört érint: egyrészt a túl kevés, másrészt a túl sok adat és információ okozhat gondokat. Az adat- és információhiányból adódó hibás (egyedi ügyben hozott vagy stratégiai) döntés és az emiatt bekövetkező kár közismert probléma. Az adat- és információbőség nemcsak szakmai kérdés (mennyi idő alatt és milyen kapacitással lehet a szükséges – releváns – adatot, információt előállítani illetve „megtalálni” az „adatrengetegben”)[2], hanem informatikai kihívás is (a tároláshoz, feldolgozáshoz, kezeléshez szükséges, elsősorban informatikai infrastruktúra folyamatos fejlesztést és bővítést igényel).

Az adatok térbeli és időbeli elérhetőségének garantálása alapvetően informatikai feladat; magában foglalja az adatok bizalmasságát (csak az arra jogosultak általi megismerhetőségét), sértetlenségét (védettségét az illetéktelen módosítástól, beavatkozástól), rendelkezésre állását

[2] Az *adatrengeteg* kifejezés az angol *big data* javasolt magyarítása. Elhangzott a HTE Infokom 2012 konferencián (Mátraháza, 2012. október 10-12.), Molnár Szilárd *E-demokrácia, és ami nincs mögötte* c. előadásán

(jogosultak általi zavartalan elérését) és hitelességét biztosító eszközök, módszerek és eljárások alkalmazását.

Nem elhanyagolható szempont a költséghatékonyság sem: az adatkezelés költségei legyenek optimalizálva és legyenek arányban a közigazgatási céllal és eredménnyel.

A fentiek teljesítése szakmai oldalról a szakmai tevékenység áttekintését, a szakmai folyamatok pontos és részletes leírását, szükség szerinti újratervezését és -szervezését, a feladatellátáshoz szükséges adatok körének rögzítését, tartalmi meghatározását, minőségi jellemzőik, érvényességi idejük definiálását, az adatgazdák és a jogosult felhasználók körének kijelölését jelenti.

A szakmai áttekintés és újragondolás alapvető jelentőségű. A közigazgatási adatkezelés tervezésében, szervezésében és szabályozásában a technikai fejlődésre tekintettel elengedhetetlen a szemléletváltás; el kell szakadni a papíralapú ügyintézés, adatkezelés és dokumentálás képzetétől, és a korszerű közigazgatás működési elveit és gyakorlatát az e-közigazgatás, a digitális írástudás fogalmaiból kiindulva kell meghatározni.

A szakmai szempontú adatvagyon-gazdálkodást funkcionális oldalról egyrészt a jogi-igazgatási, másrészt az informatikai támogató tevékenység egészíti ki. Az előbbibe tartozik a feladatellátás külső (szervezeten kívüli) és belső (szervezeten belüli) szabályozásának előkészítése illetve szabályozása, azaz a tevékenységre vonatkozó jogszabályok és közjogi szervezetszabályozó eszközök előkészítése és kiadása, valamint az előírások érvényesülésének, érvényesítésének figyelemmel kísérése (beleértve az ellenőrzést és a szükségessé váló korrekciók végrehajtását is).

Az adatvagyon-gazdálkodás akkor lehet sikeres, ha a szakmai és jogi-igazgatási szakterületek által meghatározott és szabályozott folyamatokat korszerű informatikai infrastruktúra szolgálja ki (az infrastruktúra kifejezést a lehető legtágabb értelemben célszerű használni; beletartoznak a fizikai létesítmények, eszközök, rendszerek, hálózatok, alkalmazások, az ezeket működtető szervezetek és ezek személyi állománya, továbbá az általuk alkalmazott eljárások is). [23]

Az adatvagyon-gazdálkodás sikerességét az ismertetett funkcionális tevékenységek mellett más funkcionális területek feladatellátása is befolyásolja (pl. a személyügyi tevékenység a szakemberek kiválasztását, képzését érintően, valamint a gazdálkodási tevékenység a pénzügyi háttér biztosítását tekintve). Ez utóbbiak hatása azonban általános (a közigazgatás, a közfeladatot ellátó szerv minden tevékenysége kapcsán megjelenik) és általában közvetett.

AZ ADATVAGYON MEGISMERÉSE ÉS HASZNOSÍTÁSA

Az adatvagyon-gazdálkodás eredményeként létrejött adatállomány felhasználása több irányban túlmutat [24] a közfeladatot ellátó szervek adatkezelésén; céljában, tartalmában és a felhasználók körét tekintve is markánsan kettéválik.

Az adatok megismerése

A modern demokráciák egyik alapelve az állam működésének átláthatósága. A közfeladatot ellátó szervek által kezelt közérdekű adatok (információk, dokumentumok) megismerésének joga az információszabadság alapvető eleme. Ez az Alaptörvény VI. cikkében megjelenő alapjog úgy érvényesülhet, ha a nemzeti adatvagyon e körbe tartozó elmeihez való hozzáférést a közfeladatot ellátó szervek biztosítják. A hozzáférés biztosítása történhet egyedi adatigénylés teljesítésével és adatok nyilvánosságra hozatalával (közzétételével).

Jogszabály határozza meg a közzéteendő adatok körét, a közzététel frissítésének gyakoriságát és az adatok megőrzési idejét (általános, különös és egyedi közzétételi listák), és jogszabály rendelkezik arról is, hogy mely esetekben korlátozható az adatok megismerésének joga. A korlátozást indokolhatja közérdek és magánérdek védelme is. Az előbbi körbe tartozik

a honvédelmi, nemzetbiztonsági, központi pénzügyi és devizapolitikai, környezet- vagy természetvédelmi érdekből, bűncselekmények üldözése vagy megelőzése érdekében vagy külügyi kapcsolatokra, nemzetközi szervezetekkel való kapcsolatokra, továbbá bírósági vagy közigazgatási eljárásra tekintettel történő, az utóbbira példa a szellemi alkotásokhoz fűződő jogokra tekintettel történő korlátozás.

A közfeladatot ellátó szervek által kezelt személyes adatok esetében a megismerés korlátai sokkal erősebbek. Az adatok továbbadása korlátozott, ezen kívül a személyes adat „tulajdonosa" (a jogszabály szerint: az érintett) tájékoztatást kérhet adatai kezeléséről, és meghatározott esetekben (amennyiben nem jogszabály által előírt, kötelező adatkezelésről, adatgyűjtésről van szó) rendelkezhet is arról.

A közszféra adatainak további felhasználása (újrahasznosítása)

A közfeladatot ellátó szervek által kezelt adatok további felhasználása az adatok piaci szféra (természetes vagy jogi személyek, jogi személyiséggel nem rendelkező szervezetek) általi – kereskedelmi vagy nem kereskedelmi célú – felhasználását jelenti. [25]

Az Európai Unió – felismerve egyrészt, hogy „a belső piac kialakításából és működéséből eredő gazdasági és társadalmi integráció szükségszerűen a személyes adatok határokon keresztüli áramlásának lényeges növekedéséhez fog vezetni", másrészt, hogy „az egyes tagállamokban végzett személyesadat-feldolgozás terén az egyének jogai és szabadságai, különösen a magánélet tiszteletben tartásához való jog védelmének szintjei közötti eltérések akadályozhatják az ilyen adatok egyik tagállamból a másikba történő továbbítását, ... ebből eredően akadályt jelentenek számos közösségi szintű gazdasági tevékenység elvégzésében, torzítják a versenyt" – 1995-ben elfogadott adatvédelmi irányelvében a tagállami szabályozások harmonizálását tűzte ki célul, rögzítve a személyes adatok kezelésére és feldolgozására vonatkozó alapvető rendelkezéseket. [26]

Az adatvédelmi előírások egységesítését követően a közszféra információinak (angolul: public sector information, PSI) további felhasználására vonatkozó elvárásokat és előírásokat az Európai Unió 2003-ban született ún. PSI-irányelve rögzítette. [25] Az irányelv célja „a közösségi szintű információs piac fejlesztése", [25] aminek eredményeként a közszféra által gyűjtött és kezelt adatállomány a tudásipar értékes alapanyagaként, határokon túlnyúló egységes megközelítés és szabályozás szerint (a versenytorzító hatásokat elkerülve) segíti elő a gazdasági növekedést. Az adatok ugyanis akár nyers, akár feldolgozott (értéknövelt) formában jelentős vagyont képviselnek, ami további növekedés és vagyonképzés alapja lehet (a leginkább hasznosítható adatállományok a térképészeti-földmérési, ingatlan-nyilvántartási, meteorológiai, céginformációs, jogi, statisztikai stb. adatok).

Az adatok további felhasználásának elősegítését a gazdasági érvek mellett az is indokolja, hogy a közfeladatot ellátó szervek adatgyűjtését és adatkezelését elsősorban közpénzekből finanszírozzák, másrészt a magánszektor adatszolgáltatási kötelezettségét maga az állam írja elő jogszabályokban. [24]

Az irányelv magyar jogba átültetése 2012-ben valósult meg. [27] A jogszabály a közadatok további felhasználása – újrahasznosítása – feltételeinek biztosítása érdekében meghatározza az adatok rendelkezésre bocsátásának elveit és folyamatát. Rendelkezik arról, hogy mely adatok lehetnek újrahasznosíthatók (az újonnan bevezetett közadat fogalmába a közérdekű és a közérdekből nyilvános adat tartozik), ugyanakkor az egyes közfeladatot ellátó szervek által újrahasznosításra rendelkezésre bocsátható adatok körét – a jogszabály felhatalmazása alapján – miniszteri illetve önkormányzati rendeletek tartalmazzák majd.

A jogalkotó az adatátadás formátumának meghatározásakor (az irányelvvel összhangban) előnyben részesítette az elektronikus átadás vagy hozzáférés biztosítását, rendelkezett a díjazásról (az adatátadásért megállapítható díj nem haladhatja meg a bekerülési költség 5 %-os nyereséghányaddal növelt összegét), és lehetővé tette a hasznosítás különös feltételeinek a

meghatározását is (elkerülendő az esetleges visszaélésszerű felhasználást, pl. a versenytorzító adatmonopólium kialakítását, a kedvezményesen szerzett adatok továbbértékesítését extraprofittal, a jogszerűen átvett adatok jogellenes továbbadását stb.).

Az adatok további felhasználása – ahogyan az a szabályozás indokából, céljából és tartalmából is látható – meghaladja a nemzeti kereteket (a piaci szereplők érintettsége országhatáron túlnyúló dimenziót jelent), és központilag nem tervezhető és szervezhető (tekintettel a piaci szereplők szerteágazó tevékenységére és igényeire).

AZ ADATVAGYON-GAZDÁLKODÁS ÉS A LÉTFONTOSSÁGÚ INFOKOMMUNIKÁCIÓS RENDSZEREK VÉDELME

Az adatvagyon-gazdálkodás korábban említett informatikai meghatározottsága alapján adódik az adatvagyon-gazdálkodás és a *létfontosságú infokommunikációs rendszerek védelme* összefüggéseinek vizsgálata is. (Ez utóbbi kifejezés a tárgykört szabályozó, 2012-ben elfogadott törvény [28] alapján a korábbi *létfontosságú* vagy *kritikus információs infrastruktúrák védelme* megnevezést [29] [30] váltja/válthatja fel.)

A nemzeti adatvagyon és a létfontosságú infokommunikációs rendszerek összefüggései leginkább a „tartalom és hordozója” kapcsolatával írhatók le, hiszen az adatkezelés művelete a technikai, technológiai fejlődés eredményeként szinte teljes mértékben infokommunikációs eszközökkel támogatott. Az már más kérdés, hogy a nemzeti adatvagyon és a létfontosságú infokommunikációs rendszerek – figyelemmel ez utóbbi fogalomban a létfontosságú jelzőre – mennyiben esnek egybe.

A fogalmi tisztázást nagyban nehezíti, hogy a létfontosságú infokommunikációs rendszerek védelmére vonatkozó dokumentumokban az *információs rendszer* és az *informatikai rendszer* fogalmát nem használják következetesen. [23] Erre is tekintettel e helyen csak annyi állapítható meg, hogy az adatok jelentős hányada elektronikus formában áll rendelkezésre, ezeket az elektronikus adatokat infokommunikációs rendszerek kezelik – és amennyiben ezen adatok a nemzeti adatvagyon körébe tartoznak, és ezen infokommunikációs rendszerek létfontosságúak a társadalom, a gazdaság vagy az állam működése szempontjából, akkor a nemzeti adatvagyon és az azt kezelő létfontosságú infokommunikációs rendszer egybeesik.

A két fogalom azonban nem feltétlenül kapcsolódik össze, és jelenleg még pontosan nem is tisztázott egymáshoz való viszonyuk. Míg a nemzeti adatvagyon esetében jogszabály tételesen meghatározza a nemzeti adatvagyon körébe tartozó nyilvántartásokat és ezek adatfeldolgozóit, [31] a létfontosságú rendszerek és létesítmények azonosítása (az érintett ágazatok, alágazatok meghatározása) és kijelölése (rendszerek, rendszerelemek meghatározása) hosszabb – a hivatkozott törvény [28] alapján több éven át tartó, nem lezárható – folyamat.

Bármekkora is a két fogalom és a hozzájuk kapcsolódó működtetési és védelmi tevékenység közös része illetve különbözősége, azonos a szabályozás és a felügyelet jellege (törvényi szintű szabályozás, központi közigazgatási felügyelet), és vélhetően azonos, de legalábbis hasonló lesz a kiszolgáló informatikai eszközrendszerre vonatkozó szakmai és igazgatási követelményrendszer is.

AZ ADATVAGYON-GAZDÁLKODÁS JOGSZABÁLYI KERETEI

Az adatvagyon-gazdálkodás nemzeti szintű szabályozását a már idézett Adatvagyon törvény [18] és a felhatalmazása alapján kiadott kormányrendelet [31] jelenti.

A törvény négy szakaszban rendelkezik a nemzeti adatvagyon védelméről. A fogalmi meghatározást (1.§) követően (lásd előbb) az elektronikus adatfeldolgozásra feljogosított vagy

feljogosítható személyek és szervezetek tekintetében három előírást fogalmaz meg. Eszerint törvény az elektronikus adatfeldolgozásra jogosultak körét államigazgatási szervekre illetve kizárólagos állami tulajdonú gazdálkodó szervezetekre korlátozhatja, illetve az adatfeldolgozásnak az adatkezelőtől különböző személy vagy szervezet általi ellátását kizárhatja; a Kormány rendeletben határozhatja meg az Adatvagyon törvény hatálya alá tartozó nyilvántartásokat, valamint az ezek tekintetében adatkezeléssel megbízható szervek és szervezetek körét; törvény lehetővé teheti az előzőekben ismertetett korlátozások alóli egyedi felmentés adását (2.§). A jogszabály alapján az érintett nyilvántartásokkal kapcsolatos adatfeldolgozó tevékenység csak Magyarország területén végezhető (3.§). A törvény rögzíti, hogy az érintett nyilvántartásokat elektronikusan kezelő és feldolgozó rendszerekre a *Korlátozott terjesztésű!* minősítési szintű adatok védelmére meghatározott személyi, fizikai és adminisztratív és elektronikus biztonsági előírások irányadók (4.§).

Ahogyan a törvény indokolásából kitűnik, a jogalkotói cél a „kiemelt jelentőségű állami nyilvántartások védelmének biztosítása annak előírásával, hogy a jövőben e nyilvántartásokkal kapcsolatban adatfeldolgozói tevékenységet is csak az állami szférába tartozó, ily módon az adatkezelő által közvetlenül ellenőrizhető szervezet láthasson el". [32]

Az idézett cél vitathatatlanul kiemelt jelentőségű, a jogszabályi rendelkezésekkel összefüggésben néhány elvi, illetve az alkalmazhatóságot érintő, gyakorlati megfontolást azonban célszerű áttekinteni.

A nemzeti adatvagyon fogalmába – a törvényi meghatározásból következően – beletartozik az *önkormányzati igazgatásban kezelt adatállomány* is, ennek kezeléséről, védelméről azonban még nem született jogszabályi rendelkezés.

Már említésre került, hogy a nemzeti adatvagyon körébe nem tartoznak bele a minősített adatok, jóllehet ez az adatfajta szinte kizárólag az államigazgatási szervek működése során keletkezik. Ebből következően a nemzeti adatvagyon körébe tartozó *nem minősített* adatok tekintetében az „állami feldolgozás" elvárás, azonban az állam szempontjából kiemelten védendő *minősített* adat esetében hasonló megszorítások nincsenek, ez utóbbi adatfajta védelme során külföldi eszközök, eljárások is alkalmazhatók.

A törvény meghatározza az *elektronikus adatfeldolgozás* fogalmát azzal a céllal, hogy a fogalomba tartozó, az adatkezelés folyamatait támogató technikai műveleteket – így *az elektronikus úton vezetett nyilvántartás létrehozásának, működtetésének és üzemeltetésének technikai műveletét* – meghatározott esetekben kizárólag államigazgatási szerv vagy kizárólagos állami tulajdonú vállalat által ellátható tevékenységként szabályozza. Mindazonáltal szükséges figyelembe venni, hogy az adatkezelés informatikai feltételeinek megteremtése során olyan tudás és eszközrendszer hasznosítására van szükség, amelyet a felhatalmazott szervek nem feltétlenül birtokolnak teljes körűen és korlátlanul, mivel a világ egyik legdinamikusabban fejlődő iparágának szinte naponta változó eredményeiről van szó, ahol meghatározó a külföldi tulajdon és befolyás. A „nem állami" tudás, technológia kizárása akár az eredeti szándékkal ellentétes eredményre is vezethet. Ezt a felismerést tükrözi a törvény módosítása is: a technikai műveletek példálózó felsorolásából – fél évvel a törvény hatályba lépését követően – törlésre került a *fejlesztés* kifejezés. Megfontolandó lehet a „könnyítés" a nyilvántartások *létrehozás*a esetében is, fenntartva a *működtetés* és az *üzemeltetés* független, kizárólagos állami jellegét.

Az „állami kizárólagosság" szigorát a stratégiai szempontból nem jelentős, manuális közreműködést igénylő, ún. kisegítő tevékenységek (adatrögzítés, digitalizálás stb.) esetében is célszerű lenne mérsékelni. A törvény 2011. évi módosítása már lehetőséget biztosít az *időszakosan jelentkező adatfeldolgozási feladatok* hatékony ellátása érdekében a jogszabályi korlátok alóli, határozott idejű, egyedi felmentés kérésére, e tevékenységek esetében az egyedi engedélyezési folyamatok helyett megfelelő lehetne az általános törvényi felhatalmazás biztosítása, bejelentési kötelezettség előírása mellett.

ÖSSZEGZÉS

Az adatvagyon-gazdálkodás a közigazgatásban szakmai elvárásokon alapuló, az alkalmazott infrastruktúrák alapján informatikailag erősen meghatározott, alapvetően igazgatási tevékenység, amelynek elmélete és gyakorlata most van kialakulóban. Fogalomhasználata, tartalma, területei sem szakmai, sem szabályozási szempontból még nem tisztázottak. Bár a tevékenység egyes részterületeit érintően már történtek lépések, átfogó tapasztalatokról, komplex eredményekről, jó (bevett) gyakorlatokról még nem lehet beszámolni. Jelen tanulmány a rendelkezésre álló ismeretek rendszerezésével és kiegészítésével elméleti alapot kívánt nyújtani a gyakorlati megvalósítás felé vezető úton.

Felhasznált irodalom

[1] Sándori Zsuzsanna: Mi a tudásmenedzsment? – Adat, információ és tudás. http://mek.niif.hu/03100/03145/html/km1.htm Letöltve: 2012.04.11.

[2] Rövid Oxfordi Szótár. Idézi: Adatmenedzsment. Kormányzati ajánlás. MTA Információtechnológiai Alapítvány, Budapest, 2009. november 16.

[3] Fülöp Géza: Az információ. 2. bővített és átdolgozott kiadás, Budapest, 1996.

[4] Bőgel György: Verseny az elektronikus üzletben. Melyik békából lesz herceg? Műszaki Könyvkiadó, Budapest, 2000.

[5] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Info tv.)

[6] A Polgári Törvénykönyvről szóló 1959. évi IV. törvény (Ptk.)

[7] Az adózás rendjéről szóló 2003. évi XCII. törvény (Art.)

[8] A közösségi vámjog végrehajtásáról szóló 2003. évi CXXVI. törvény (Vtv.)

[9] A hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény (Hpt.)

[10] A befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény

[11] A biztosítókról és a biztosítási tevékenységről szóló 2003. évi LX. törvény

[12] A foglalkoztatói nyugdíjról és intézményeiről szóló 2007. évi CXVII. törvény

[13] A pénzforgalmi szolgáltatás nyújtásáról szóló 2009. évi LXXXV. törvény

[14] A minősített adat védelméről szóló 2009. évi CLV. törvény (Mavtv.)

[15] A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.)

[16] Az Európai Parlament és a Tanács 1049/2001/EK Rendelete (2001. május 30.) az Európai parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről

[17] A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.). Az Info tv. hatályba lépésével 2011. január 1-jétől hatályát vesztette.

[18] A nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény (Adatvagyon tv.)

[19] Digitális Megújulás Cselekvési Terv 2010-2014. Nemzeti Fejlesztési Minisztérium, Budapest, 2010.

[20] A nemzeti vagyonról szóló 2011. évi CXCVI. törvény

[21] Henri Fayol: Ipari és általános vezetés. Közgazdasági és Jogi Könyvkiadó, Budapest, 1984.

[22] Dr. habil. Bordás Mária: A felhőinformatika alkalmazása a magyar közigazgatásban – az Obama-kormány példája alapján – Új Magyar Közigazgatás, 2012. január, 5. évfolyam 1. szám, 24-34. o.

[23] Nagyné Takács Veronika: A nemzeti kritikus információs infrastruktúrák védelmének szabályozási és szervezeti kérdései - Helyzetkép az EU irányelv 2012-ben esedékes felülvizsgálata előtt – Hadmérnök, 2012. (VII.)/1., 179-191. o.

[24] Hüttl Antónia – Dr. Milassin László – Nagy Ágnes – Nagy Katalin – Pásztori Veronika: Az állami adatvagyon hasznosítása: nemzetközi tapasztalatok, javaslatok a hazai alkalmazásra. KOPINT-DATORG Konjunktúra Kutatási Alapítvány, Budapest, 2002. március 28.

[25] Az Európai Parlament és a Tanács 2003/98/EK Irányelve (2003. november 17.) a közszféra információinak további felhasználásáról

[26] Az Európai Parlament és a Tanács 95/46/EK Irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról

[27] A közadatok újrahasznosításáról szóló 2012. évi LXIII. törvény

[28] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.)

[29] Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról (COM (2005) 0576 végleges), 2005. november 17.

[30] 1249/2010. (XI. 19.) Korm. határozat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról

[31] 38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról

[32] 2010. évi CLVII. törvény indokolása a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Prisznyák Szabolcs
prisznyak.szabolcs@bv.gov.hu

A TÖBB TELEPHELLYEL RENDELKEZŐ BÜNTETÉS-VÉGREHAJTÁSI INTÉZETEK INFORMATIKAI TÁMOGATÁSA

Absztrakt

A cikk bemutatja az egy és a több telephellyel rendelkező büntetés-végrehajtási intézetek informatikai támogatásának eltéréseit. A szerző megvizsgálja egy komplex megoldás lehetőségét, elemzi a megvalósíthatóság feltételeit. Ennek eredményeképpen javaslatot tesz egy megoldásra, amely valamennyi hasonló típusú börtönben alkalmazható. A cikk végén összegzi a tapasztalatokat, továbbá javaslatot tesz a módszer más rendvédelmi szervezeteknél történő alkalmazásra.

The article presents the different types of information technology support provided for prisons with one establishment and for those that have several premises. Based on the examination of the possibility of an integrated solution and the analysis of the conditions for its realization, the author suggests a solution applicable in all similar types of prisons. At the end of the article he summarizes the experience gained and also makes a proposal to apply the method in other law enforcement organizations.

Kulcsszavak: *rendvédelem, büntetés-végrehajtás, börtön, információ-technológia, információs rendszer ~ law enforcement, prison service, prison, information technology, information system*

BEVEZETÉS

A büntetés-végrehajtási szervezet informatikai támogatásának történetében mérföldkőnek számít a „Felelősen, felkészülten a büntetés-végrehajtásban” elnevezésű, EKOP-1.1.6-09-2009-0001 azonosítószámú, az Európai Unió támogatásával megvalósult informatikai fejlesztési projekt [1]. A projekt keretében a több, mint 1,2 milliárd forint értékben megújult a büntetés-végrehajtási szervezet teljes informatikai rendszere. A fejlesztés rövid tartalmát publikációm egy fejezetében mutatom be.

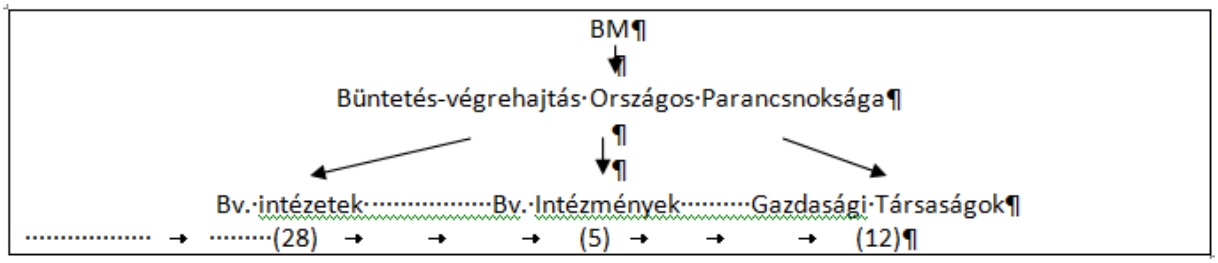
Jelen publikációban a több telephellyel rendelkező büntetés-végrehajtási intézetek informatikai működésének problémáit, illetve az egységes megoldásának lehetőségét mutatom be. A módszer kidolgozásánál a fő vezérlőelv – mint említettem – az egységesség volt, azaz a több telephelyes intézetek működése semmiben ne különbözzön egymástól, illetve az egy telephellyel rendelkező intézetekétől. Különösen fontosnak tartom, hogy az informatikai szolgáltatásokat igénybevevő végfelhasználók esetében se legyen semmilyen eltérés, szolgáltatáscsökkenés, tehát valamennyi – az informatikai rendszeren alapuló – szolgálati feladatukat maradéktalanul képesek legyenek elvégezni. A másik oldalon, azaz a vezetői szinten, a vezetői döntések megfelelő informatikai rendszerrel történő támogatásához egységesen – ne csak telephelyenkénti bontásban – álljanak rendelkezésre az egész intézetre vonatkozó információk. Ennek analógiáján további követelményként fogalmaztam meg, hogy az üzemeltető informatikai szakállomány feladataiban se legyen alapvető különbség.

Publikációm elkészítése során igyekeztem a témához illeszkedő szakirodalmat, továbbá – ennek szűkössége okán – a kapcsolódó rendvédelmi, kormányzati informatikával foglalkozó egyéb tudományos publikációkat is tanulmányozni. Munkám során feldolgoztam a kapcsolódó jogszabályokat, illetve a nemzeti és a közösségi stratégiákat, ajánlásokat.

A BÜNTETÉS-VÉGREHAJTÁS SZERVEZTI FELÉPÍTÉSE

A büntetés-végrehajtás állami, fegyveres, rendvédelmi szerv, amely külön jogszabályban meghatározott szabadságelvonással járó, büntetéseket, intézkedéseket, valamint büntetőeljárási kényszerintézkedéseket, továbbá elzárást hajt végre [2].

A büntetés-végrehajtás a legtöbb magyarországi közigazgatási- és rendvédelmi szervezettől eltérően nem három, hanem kétszintű szervezet. A büntetés-végrehajtási szervezet központi vezető szerve a Büntetés-végrehajtás Országos Parancsnoksága, amely főosztályai révén a büntetés-végrehajtási intézetekben folyó szakmai munka felügyeletét, ellenőrzését végzi. A büntetés-végrehajtási intézetek ellátják a büntetések és intézkedések végrehajtásával kapcsolatos feladatokat. A büntetés-végrehajtási szervezet működéséért felelős miniszter – jelenleg a Belügyminiszter – dönt büntetés-végrehajtási szerv létrehozásáról, átalakításáról, valamint megszüntetéséről.



1. ábra. A büntetés-végrehajtás szervezeti felépítése (forrás: szerző)

Magyarországon 28 önálló jogállású büntetés-végrehajtási intézet és 5 – egészségügyi és oktatási – intézmény, valamint 12 gazdasági társaság működik. Az informatikai szakterület kompetenciája a gazdasági társaságokra nem terjed ki, azok a büntetés-végrehajtási szervezet

informatikai rendszerétől független önálló, elszigetelt rendszereket alakítottak ki, így ez a terület nem képezi vizsgálatom részét. Az öt intézmény közül három intézmény a büntetés-végrehajtási szervezettel munkaviszonyban álló alkalmazottak oktatási, továbbképzési feladatait hajtja végre, így ez sem része vizsgálatomnak.

A 28 intézet és a vizsgált 2 intézmény közül 7 intézet működik több telephellyel. A telephelyek száma 2-4. Az intézet központi telephelyes és az alárendeltségébe tartozó egyes telephelyek közti távolság valamennyi esetben 5-30 km. Ezek az intézetek vagy már több telephellyel alakultak, vagy – elsősorban gazdasági okokból történt – racionalizálással, szervezet átalakítással több intézmény összevonásaként jöttek létre.

Büntetés-végrehajtási Intézet	Intézet központi telephelye	további telephely(ek)
Állampusztai Országos Büntetés-végrehajtási Intézet	Állampuszta	Solt
Szegedi Fegyház és Börtön	Szeged, Mars tér	Szeged, Dorozsmai út Nagyfa
Közép-dunántúli Országos Büntetés-végrehajtási Intézet	Baracska	Székesfehérvár
Pálhalmai Országos Büntetés-végrehajtási Intézet	Pálhalma	Mélykút Bernátkút Sándorháza
Fővárosi Büntetés-végrehajtási Intézet	Budapest Nagy Ignác utca	Budapest, Gyorskocsi utca Budapest, Maglódi út
Bács-Kiskun Megyei Büntetés-végrehajtási Intézet	Kecskemét, Mátyási út	Kecskemét, Wéber Ede utca
Borsod-Abaúj-Zemplén Megyei Büntetés-végrehajtási Intézet	Miskolc	Szirmabesenyő

2. ábra. Több telephellyel rendelkező büntetés-végrehajtási intézetek (forrás: szerző)

Az informatikai rendszer működése szempontjából azokat az intézeteket tekintem több telephelyesnek, ahol a telephelyek közti távolság helyi adathálózati összeköttetéssel nem áthidalható. Tehát a Budapesti Fegyház és Börtön – az informatikai működés szempontjából - egy telephelynek tekintendő, annak ellenére, hogy a gyakorlatban két telephellyel (A és B objektum) rendelkezik. Ennek oka, hogy a két telephely a csupán egy-két száz méteres távolsága miatt – optikai összeköttetés alkalmazásával – képes egy helyi hálózatban működni.

Néhány büntetés-végrehajtási intézet, intézmény esetében a fenti vázolt helyzettel éppen ellentétesek a körülmények, azaz egy telephelyen működik több intézet, intézmény. Ebben az esetben teljesen más informatikai fejlesztési és üzemeltetési problémák jelentkeznek, így ezek az esetek nem képezik a vizsgálat tárgyát.

MŰKÖDÉSBELI HASONLÓSÁGOK, KÜLÖNBSÉGEK BÜNTETÉS-VÉGREHAJTÁSI SZEMPONTBÓL

A több telephelyes büntetés-végrehajtási intézetek működésük szerint nem csak az egy telephellyel rendelkező intézményektől térnek el, hanem egymástól is. Ezek az eltérések adódhatnak valamilyen „szokásjogon” alapuló működésen, továbbá szinte valamennyi intézet esetében van olyan speciális körülmény, ami – elsősorban a speciális szabályozás révén – alapvetően meghatározza, befolyásolja a működést. Ilyenek lehetnek a női és a férfi, a fiatalkorú és a felnőtt, az egészséges és a beteg, az előzetesen illetve a jogerősen fogvatartott személyek elkülönítésére vonatkozó szabályok [3]. Egy intézet működését ezeken felül – az informatikai támogatás szükségessége szerint – az alábbi büntetés-végrehajtási szaktevékenységek határozzák meg leginkább: fogvatartottak nyilvántartása, befogadása, körszállítása, előállítása. Ezek a szabályozott szaktevékenységek egymással is összefüggésben vannak, hiszen a befogadási, körszállítási, előállítási feladatok szorosan kapcsolódnak a

fogvatartottak – informatikai rendszerben történő – nyilvántartásához. Így megállapítható, hogy a több telephelyes büntetés-végrehajtási intézetek szakfeladat végrehajtásában – így annak informatikai támogatásában is – az az alapvető különbség, hogy hány telephelyen működik – részben önálló – nyilvántartási szervezeti egység. A vizsgált hét intézet közül egyedül a Közép-dunántúli Országos Büntetés-végrehajtási Intézetben működik valamennyi telephelyen – Baracskán és Székesfehérváron is – nyilvántartási szervezeti elem. Ennek az intézetnek a működése abban is eltér a további intézetektől, hogy a korábban két önálló intézet 2007-ben történt integrációja előtt a székesfehérvári telephely megyei intézetként, a baracskai pedig országos intézetként működött. A működésben a legfontosabb különbség, hogy a megyei intézetekben elsősorban előzetesen letartóztatottakat tartanak fogva, az országos intézetekben pedig a jogerős büntetésüket töltőket. A két csoporthoz pedig alapjaiban eltérő további büntetés-végrehajtási szabályok, szaktevékenységek kapcsolódnak, amelyek összehangolása egy szervezeti egységben rendkívül bonyolult. Ennek értelmében megállapíthatjuk, hogy a Közép-dunántúli Országos Büntetés-végrehajtási Intézet két telephelyének szakmai tevékenysége – az integrációt követően is – úgy működik, mint egy önálló megyei, illetve egy önálló országos intézet, de egy szakmai vezetéssel rendelkeznek.

AZ EKOP-1.1.6 INFORMATIKAI FEJLESZTÉSI PROJEKT

Az EKOP-1.1.6-09-2009-0001 informatikai fejlesztési projekt a büntetés-végrehajtási szervezet eddigi legnagyobb informatikai beruházása, melynek során jelentős fejlesztés történt mind a hardver, mind a szoftver vonatkozásában, és természetesen egyidejűleg változott az eszközökhöz, feladatokhoz kapcsolódó szabályozás is. A fejlesztés magába foglalta az egyes intézetek lokális adathálózatainak fejlesztését, bővítését, egységes aktív eszközparkjának kialakítását, a teljes hardver infrastruktúra megújítását, amely szerver oldalon a teljes eszközpark homogén eszközökkel történő kiváltását jelentette, munkaállomás oldalon pedig az elavult számítógépek döntő többségének cseréjét [4]. Fejlesztésre kerültek a rendelkezésre állást támogató eszközök is, így a szünetmentes tápegységek, a több generációs mentést – és szükség esetén egy korábbi állapot visszaállítását – biztosító mentőrendszerek is. A fejlesztési projekt kulcspontja volt a büntetés-végrehajtás törvényes munkájának alapját jelentő informatikai rendszer kiváltása, funkcionális bővítése egy új – a XXI. századi igényeknek megfelelő technológiájú, szolgáltatási képességű - információs rendszerrel. Újdonság a humán-erőforrás gazdálkodás adminisztrációt támogató integrált programrendszer is.

A megelőző dokumentációs és pályázati szakaszt is figyelembe véve a projekt időtartama több mint három év volt. A munkában, mint a Büntetés-végrehajtás Informatikai Főosztályának fejlesztési osztályvezetője vettem részt. A fejlesztés során sok – több esetben előre nem látott, váratlan – megoldandó problémával szembesültünk, melyeket minden esetben igyekeztünk a büntetés-végrehajtási szervezet egészét, illetve azon belüli kompetenciáinkat tekintve egységesen kezelni, megoldani. Az egyik ilyen koncepcionális kérdésként felmerülő probléma a több telephellyel rendelkező büntetés-végrehajtási intézetek informatikai működése, annak szakmai támogatása volt. Erre a szervezetet tekintve egységes módszertani elképzelést alakított ki az informatikai szervezet. A gyakorlatban azonban az érintett büntetés-végrehajtási intézetek egymástól is eltérően működő feladatstruktúrájának változatlanul hagyása mellett, illetve a szervezettől független külső körülmények, adottságok miatt ez nem volt megvalósítható. Ez főként a fogvatartottak nyilvántartását kezelő szoftver fejlesztése során okozott problémát, így ott egy áthidaló megoldás került alkalmazásra. A probléma emellett jelen van a szerver elhelyezésben, központi szolgáltatások elérésében, működésében, az intézeten belüli csoportmunka megvalósításában, a vezetői információk gyors, korszerű módon történő szolgáltatásában is.

INFORMATIKAI SZEMPONTOK SZERINTI ÖSSZEHASONLÍTÁS

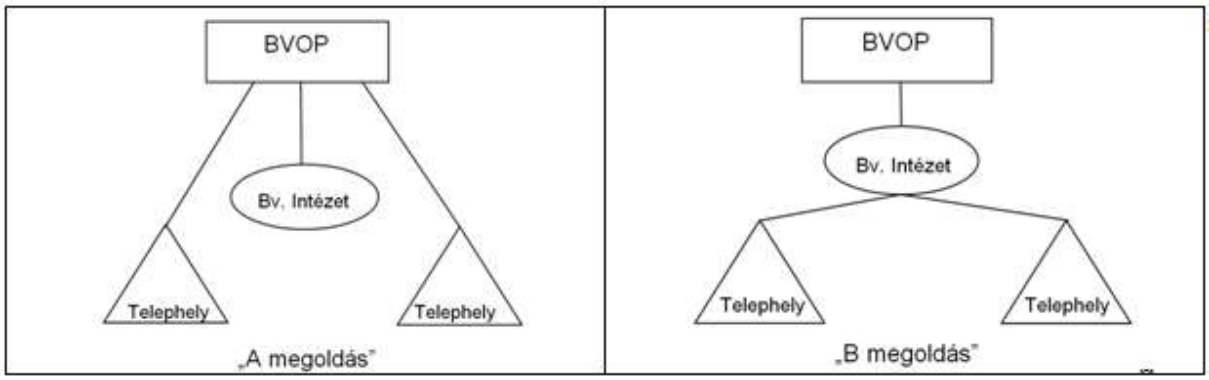
A büntetés-végrehajtás országos parancsnokának 1/2011 (V.6.) számú utasításával kiadott Büntetés-végrehajtás Országos Parancsnoksága Szervezeti Működési Szabályzata [5] szerint az Informatikai Főosztály feladata többek között szervezni és összehangolni a büntetés-végrehajtási szervezet informatikai működését, szakirányítani az országos parancsnokságon, valamint a büntetés-végrehajtási szerveknél informatikai feladatokat ellátó személyek tevékenységét, tervezni, szervezni és lebonyolítani az informatikai beruházási projekteket, elvégezni a rendszerintegrációt. Ezen előírások értelmében az Informatikai Főosztály feladata az országosan egységes infrastruktúra, a homogén informatikai rendszer kialakítása. Munk Sándor szerint "Az informatikai szolgáltatások alapját képező tevékenységek tervezettsége, szervezettsége, egységes irányítása alapvetően határozza meg a szervezetek, szakterületek működésének eredményességét, minőségét." [6]

A BVOP Informatikai Főosztálya a fenti utasítás előírásait betartva, illetve az idézett tudományos megállapítást szem előtt tartva igyekezett megvalósítani az EKOP-1.1.6-09-2009-0001 azonosítószámú Európai Unió által támogatott informatikai fejlesztési projektet. A több telephely problémaként jelentkezett a fogvatartotti nyilvántartást megvalósító – FŐNIX elnevezésű – programrendszer fejlesztése során. A fő gondot a többi intézettől eltérő modellel működő Közép-dunántúli Büntetés-végrehajtási Intézet okozta. Az intézet működésének átstrukturálására gazdasági illetve humán erőforrás rendelkezésre állási okokból, valamint a büntetés-végrehajtási szakmai feladatok racionálisabb, ennek eredményeként biztonságosabb végrehajtása érdekében nem nyílt lehetőség. Így a program logikája oly módon került tervezésre, kifejlesztésre, hogy az intézeteken belül egy újabb szervezeti egység, a telephely került kialakításra. Ez – beállítás alapján – lehetőséget nyújt a telephely önálló egységként történő kezelésére, így biztosított, hogy egy intézet telephelyén befogadás történjen, vagy az körszállítás kiinduló, vagy célállomása legyen. Ez a döntés nem csak megoldott egy problémát, hanem előre biztosítja az esetleges későbbi hasonló helyzetek kezelését is.

A projekt keretében a több telephelyes intézetek egységes szerverparkkal történő ellátása nem volt lehetséges, elsősorban anyagi okokból. Az ellátással kapcsolatos döntésekben jelentős szerepet játszottak egyéb adottságok, ezek közül is kiemelten a távoli adatátviteli hálózat (WAN) strukturális kialakítása. Ennek eredményeként nem született egységes megoldás.

A 346/2010 (XII.28.) Kormányrendelet 3.§ (1) bekezdés értelmében „…kormányzati célú hírközlési tevékenységet kizárólag a kormányzati célú hírközlési szolgáltató és az elkülönült hírközlési tevékenység végzésére jogosultak végezhetnek." [7] A hivatkozott kormányrendelet nevesíti a kormányzati célú hírközlési szolgáltató, amely a Nemzeti Infokommunikációs Szolgáltató Zrt.

A táv-adatátviteli hálózat kialakítása nem egységes a több telephelyes intézetek esetében.



3. ábra. A táv-adatátviteli hálózat lehetséges kialakításai (forrás: szerző)

Az ábrán látható „A megoldás” esetében a telephelyek önálló Nemzeti Távközlési Gerinchálózati (NTG) végpontként működnek, a „B megoldás” esetében az intézet központi telephelye az NTG végpont, és ehhez – a szervezeti struktúrának megfelelően – csatlakoznak az intézet telephelyei. Az „A megoldás” alkalmazása esetében az intézet valamennyi telephelyére önálló szerver infrastruktúrát kell biztosítani. Ez a megoldás rendkívül drága megoldás, mind az egyszeri kialakítás, mind a későbbi üzemeltetési költségek, és az ehhez szükséges erőforrások vonatkozásában. Járulékos problémaként jelentkezik, hogy a szervezeten belüli csoportmunka megvalósítása is nehézkes, így a vezetői információk biztosítása is összetettebb, bonyolultabb, idő- és munkaigényesebb.

A „B megoldás” megvalósítja a szervezeti felépítésnek megfelelő logikai struktúrát, de az intézet és a telephelyek között minden egyes esetben eltérő saját megvalósítás került alkalmazásra, amely jellemzően alacsony sávszélességű.

A „B megoldás” került kialakításra az Állampusztai Országos Büntetés-végrehajtási Intézetben, a Szegedi Fegyház és Börtönben, a Pálhalmai Országos Büntetés-végrehajtási Intézetben, a Fővárosi Büntetés-végrehajtási Intézetben az „A megoldás” és a „B megoldás” kombinációjaként egy hibrid megoldás került kialakításra (úgynevezett full mesh), így a telephelyek közvetlen kapcsolatban vannak a BVOP-val és az intézet központjával is, mindkét szolgáltatás az NTG-n valósul meg. Az 1. ábrán szereplő további három intézetben az „A megoldás” került alkalmazásra.

EGYSÉGES INFORMATIKAI MEGOLDÁS

Az felmerült probléma egységes informatikai megoldása – a lehetséges megoldásokat mérlegelve – a szerver infrastruktúra központosítása a több telephelyes intézet központi telephelyére. A megoldás mellett szól, hogy ezzel valamennyi büntetés-végrehajtási intézetben homogén rendszert alakíthatunk ki. Több telephely esetén is csak egy helyen kell kialakítani a szerver infrastruktúrát, illetve a működését biztosító környezetet, úgy, mint klimatizált gépterem, szünetmentes áramforrás, központi mentőrendszer [8]. Nagyon lényeges szempont a humánerőforrással történő hatékony gazdálkodás is, hiszen ebben az esetben csak egy helyen kell kialakítani a megfelelő működési környezetet, egy helyen kell karbantartani, szükség esetén hibát elhárítani, mindezek hatékonyabb, tervezhetőbb, egyszerűbb logisztikájú informatikai üzemeltetést eredményeznek. Nem utolsósorban a központosított megoldás magas szinten támogatja a csoportmunkát, és a hatékony információszolgáltatást a vezetői döntések előkészítéséhez.

A megvalósításnak azonban természetesen feltételei is vannak. A táv-adatátviteli hálózatot logikailag úgy kell kialakítani, hogy valamennyi telephely a 3. ábrán látható „B megoldás”-sal kapcsolódjon az intézeti központhoz. A kialakítást célszerű a NISZ Zrt.-vel együttműködve megvalósítani, hiszen így jó minőségű hálózaton, megfelelő sávszélességű, nagy rendelkezésre állású hálózati kapcsolat alakítható ki, amely a minőségi munkavégzéshez elengedhetetlen. A megfelelő hálózat kialakítása egyszeri magas költséggel jár, de egyrészt „az információ létrehozás és összeállítása természetesen költséges” [9], másrészt - a korábban ismertetett megtakarításokat is figyelembe véve – hosszú távon gazdaságos, műszakilag előremutató megoldás.

A kialakításnak egyéb feltételei is vannak, ezért a központi szerver infrastruktúra kialakíthatóságának felmérésére elkészítettem egy táblázatot. A kidolgozott módszerrel nem csak a büntetés-végrehajtási, hanem bármely más – rendvédelmi, közigazgatási – hasonló problémával küzdő szervezet is felmérheti, hogy a több telephelyes szervezeti egységeknél kialakítható-e a központi szerver infrastruktúra.

Ssz.	Kérdés	válasz (igen/nem)
1	A telephelyek táv-adatátviteli hálózaton logikailag kapcsolódnak-e a szervezet központi telephelyéhez?	igen/nem
2	A táv-adatátviteli hálózaton rendelkezésre áll-e a megfelelő sávszélesség? (az alkalmazott rendszerek, illetve a felhasználók számának függvényében önálló felméréssel meghatározható egy-egy szervezetre vonatkozóan, napjainkban a bv. szervezetnél jellemzően 30-100 Mb/s elegendő)	igen/nem
3	Rendelkezésre áll-e a szervezet kiszolgálására a megfelelő hardver infrastruktúra?	igen/nem
4	Rendelkezésre állnak-e a szerverközpont kialakításához a szükséges szoftverlicencek?	igen/nem
5	Valamennyi kliens számítógép megfelelő hardverrel rendelkezik?	igen/nem
6	Valamennyi kliens számítógép képes megfelelő technológiával kapcsolódni a központi szerver(ek)hez? (távoli asztal, RDP kapcsolódási képesség és/vagy virtuális gép futtatási képesség)	igen/nem
7	A felhasználók azonosítása a teljes szervezet esetében központi címtárban történik?	igen/nem
8	Amennyiben klasszikus szerver - kliens alkalmazások is használatban vannak, ezek működése megvalósítható-e terminal server és/vagy virtuális gép alkalmazásával?	igen/nem
9	Megfelelően szabályozott-e az új munkakörnyezetben történő munkavégzés?	igen/nem

4. ábra. Központi szerver infrastruktúra megvalósíthatósági kérdőív (forrás: szerző)

A több telephelyes intézetek esetében a szerver-szolgáltatások központosítása csak abban az esetben kezdődhetnek meg, ha valamennyi kérdésre „igen” a válasz. Az egyes kérdések egymással is összefügghetnek, hiszen ha a központban – a meglévő kliens-szerver alkalmazások miatt – a virtuális kliens megoldást kell használni, abban az esetben rendelkezni kell ehhez megfelelő licencekkel mind a szerver, mind a kliens oldalon, sőt adott esetben a hardver is eltérhet (pl.: virtuális kliens esetén elegendő a zéró kliensek alkalmazása, de terminál szerver alapú megoldás esetén nem).

ÖSSZEGZÉS

Jelen publikációban bemutattam egy informatikai problémát, amely a büntetés-végrehajtási szervezetnél több intézet esetében is jelen van. A problémát előtérbe helyezve bemutattam a büntetés-végrehajtási szakmai, illetve az informatikai fejlesztési, üzemeltetési sajátosságokat. A körülményeket, a tapasztalatokat, és a lehetséges megoldásokat figyelembe véve javaslatot tettem egy egységes, szabványos, előremutató megoldásra, amely nem csak informatikai szempontból lehet jó megoldás. A szerver-központosítással, és a szolgáltatások távoli telephelyekről, jó minőségű hálózaton történő elérésével – az informatikai szolgáltatás minősége mellett-, javul a csoportmunka színvonala, és pozitív hatásai lesznek a vezetői információk rendelkezésre állásának is.

Mindezeken túlmenően ez lehetne az egyik első lépés az informatikai rendszerek központosítása – azaz a felhő alapú megoldások – felé, hiszen itt egy központi helyen kerülnének tárolásra az adatok, és a programok is, a kliensek pedig csak ennek a központnak az elérési képességével rendelkeznének. Így a fejlesztés illeszkedne a Nemzeti Fejlesztési Minisztérium által kiadott Digitális Megújulás Cselekvési Tervhez (2010-2014), amely szerint „A géptermi szolgáltatások tervezésekor meg kell vizsgálni a számítási felhő (cloud computing) mint új számítógépes paradigma alkalmazhatóságát.” [10]. A fejlesztési elképzelés összhangban van az Európai Digitális Menetrenddel (Brüsszel, 2010. augusztus 26.) is [11].

Véleményem szerint a rendvédelemben és a közigazgatásban sok helyen áll fenn hasonló probléma – elég csak a rendőrségnél, valamint a katasztrófavédelemnél a közelmúltban

végrehajtott szervezet átalakításokra gondolni –, amelyre a publikációban bemutatott módszer megoldást nyújthat.

Felhasznált irodalom

[1] SEBESTYÉN Attila: *Büntetés-végrehajtás informatikai fejlesztési projekt.* = Kommunikáció 2009, 2009 Zrínyi Miklós Nemzetvédelmi Egyetemi Kiadó - ISBN 978-963-7060-70-0

[2] 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről

[3] 6/1996. (VII. 12.) IM rendelet a szabadságvesztés és az előzetes letartóztatás végrehajtásának szabályairól

[4] *EKOP-1.1.6-09-2009-0001 informatikai fejlesztési projekt Előzetes megvalósíthatósági tanulmány*. Bp. 2009, Kiadó nélkül

[5] A büntetés-végrehajtás országos parancsnokának 1/2011. (V.6.) BVOP utasítása a Büntetés-végrehajtás Országos Parancsnoksága Szervezeti és Működési Szabályzatának kiadásáról

[6] MUNK Sándor: *Az informatikai irányítás rendje, feladatai.* = Hadmérnök 2012. 7. évf. 1. szám -pp 169-178. – ISSN 1788 - 1919

[7] 346/2010 (XII.28.) Kormányrendelet a kormányzati célú hálózatokról 3.§ (1)

[8] A büntetés-végrehajtás országos parancsnokának 1-1/13/2011.(III. 22.) OP intézkedése a büntetés-végrehajtási szervezet informatikai biztonsági szabályainak kiadásáról

[9] SHARPIO, Carl – R. VARIAN Hal: *Az információ uralma.* - Bp.: Geomédia Szakkönyvek, 2000. -ISBN 963 7910 74 3, -ISSN 1585-9703

[10] Nemzeti Fejlesztési Minisztérium: Digitális Megújulás Cselekvési Terv (2010-2014) (56.o.)

[11] Európai Digitális Menetrend, Európai Bizottság, Brüsszel 2010.08.26. COM(2010) 245 végleges/2

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Tibor Szabó
szabo.tibor@nbsz.gov.hu

NETWORK SECURITY PROBLEMS ON LAYER 2

Abstract

IT, communications equipment and systems - that are part of the critical infrastructure components - communicate with each other over the Internet and are available to anyone anywhere in the world, and thus become the target of attacks. The method of attack is usually infected documents, malicious emails, Trojan programs, but less is said about the cases of attack of Layer 2. As a result, even between the professionals we can find someone who is just focusing on the security of the device itself and not on the security of the management system during the implementation of the information security, the data elements are omitted. According to experience, I need to draw your attention to some security problems of the Layer 2, when those are ignored, it can increase the vulnerability of the critical infrastructure, including the information systems and the national security systems.

Az informatikai, a kommunikációs eszközök és rendszerek - melyek részei a kritikus infrastruktúrát alkotó rendszerelemeinknek – kommunikálnak egymással az interneten és elérhetőek a világ bármely pontjáról bárki számára, ezáltal támadások célpontjává válhatnak. A napi sajtóban látott támadások módszerét tekintve többnyire fertőzött dokumentumokról, kártékony email tartalmakról, rosszindulatú trójai programokról értesülünk, azonban kevesebb szó esik azokról az esetekről, amikor Layer 2 szinten történik a támadás. Ennek hatására még a szakemberek között is található olyan, aki informatikai biztonság megvalósítása során az adatokat kezelő rendszerelemek közül kihagy néhányat és magára az eszközrendszerre koncentrál és azon törekszik csak a biztonság megvalósítására. Tapasztalatok alapján szükségesnek tartom cikkemmel felhívni a figyelmet néhány olyan Layer 2 szintű biztonsági problémára, melyek figyelmen kívül hagyása növeli kritikus infrastruktúráink, információs rendszereink sebezhetőségét beleértve a nemzet biztonsága szempontjából fontos rendszereket.

Keywords: *layer 2, spanning tree protokoll, VLAN támadás, MAC cím tábla, Wi-Fi, ~ DHCP starvation attack, CAM table, MAC spoofing, 802.1q*

INTRODUCTION

Day by day we can read news about hackers who attacked banks, various diplomatic missions, government portals, research institutes, airports or taken relevant information from oil companies. Nowadays such events are more and more frequent, because – it is well known - that the IT and communications equipment and systems became part of our lives. At home, at work, on the way, even while doing the housework we use them.

In addition, it is more and more usual to entrust to them such functions like perception, control. They are available from anywhere in the world and they communicate with each other through telecommunication or local connections. Those equipment and systems can be available with few clicks. All these features make our daily life more convenient, but it can cause risk to us, to the institutions and to our country - thinking on the critical infrastructures, which are also a popular target for the attackers. [1], [2]

The method of attack is usually infected documents, malicious emails, Trojan[1] programs, but less is said about the cases of attack of Layer 2[2]. As a result, even between the professionals we can find someone who is just focusing on the security of the device itself and not on the security of the management system during the implementation of the information security, the data elements are omitted. [5]

According to experience, I need to draw your attention to some security problems of the Layer 2, when those are ignored, it can increase the vulnerability of the critical infrastructure, including the information systems and the national security systems.

Because the Layer 2 attacks are relatively more difficult to accomplish from outside, from the Internet, they are only concentrate on the other layer of OSI[3], they think that the LAN[4] and the backbone network provided by the internet service provider is safe, but it isn't. There are some well-known technics which allows reaching the elements of the LAN network in short time from outside: For example: Backdoor[5], Wi-Fi[6] hacking[7].

LAYER 2

Before explaining the vulnerabilities of the Layer 2, please find below a few words about what is this – for those who are less experienced in this field.

The Layer 2 is one part of the OSI – seven-layer hierarchical – model. The ISO (International Organization for Standardization) developed the OSI model, so that they can determine the requirements of mutual cooperation the communication devices – including computers – between each other with individual layers. In fact, the same communication functions are grouped into logical layers. A layer serves the layer above it and is served by the layer below it. Main concern was that the different manufacturer's products (hardware, software) work together at the border of different layer.

Find below the list of levels with short explanation: (Figure 1.)

---

[1] Trojan is a type of malware which appears to perform a desirable function but instead prepare an unauthorized access to the user's computer. [4]

[2] The Layer 2 (data link layer) is one part of the OSI model. It will be explained below in more detail.

[3] Open Systems Interconnection model is an abstract reference model of networking. [3]

[4] Local Area Network is a computer network that connects computer in a limited area. This area can be extended with special equipment.

[5] Backdoor is a method of bypassing normal authentication, securing illegal remote access to your computer. [6]

[6] Wi-Fi is a popular technology that allows an electronic device to exchange data via radio waves based on IEEE (Institute of Electrical and Electronics Engineers) standards. [7]

[7] In this context, the activity in which hacker seeks and exploits a computer or computer network weaknesses (in this case the Wi-Fi).

Figure 1. OSI Reference Model [16]

The names of the individual layers are obvious, but please find below few explanation to obtain a more complete picture about the function of the layer.

The *physical layer* defines electrical and physical specifications for devices. In particular, it defines the relationship between a device and a transmission medium, such as a copper or fiber optical cable. The major functions and services performed by the physical layer are: Establishment and termination of a connection. Modulation or conversion between the representations of digital data in equipment.

The layer we are interesting in is the *datalink layer* provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the physical layer. Following are the functions of data link layer:

- Framing
- Physical Addressing
- Flow Control
- Error Control
- Access Control
- Media Access Control (MAC)

The *network layer* provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network (remember to the data link layer which connects hosts within the same network), while maintaining the quality of service requested by the transport layer.

The *transport layer* provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control.

The *session layer* controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application.

The *presentation layer* establishes context between application-layer entities, in which the higher-layer entities may use different syntax and semantics if the presentation service provides a mapping between them. (for example: MIME[8] decoding.)

The *application layer* is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component.

[8] Multipurpose Internet Mail Extensions - is an Internet standard that extends the format of email to support: Text in character sets other than ASCII, Non-text attachments, Message bodies with multiple parts, Header information in non-ASCII character sets. [9]

ATTACK TECHNIQUES

The attack techniques on Layer 2 can be so efficient and "invisible", because there is a fundamental problem in the OSI model which was built to allow different layers to work without knowledge of each other and the information flows up and down to the next subsequent layer as data is processed. If one layer is hacked, the communications are compromised without the other layers being aware of the problem. In this case the Layer 3 and Layer 1 will not be aware if Layer 2 is attacked. (Figure 2.) [10] [11]

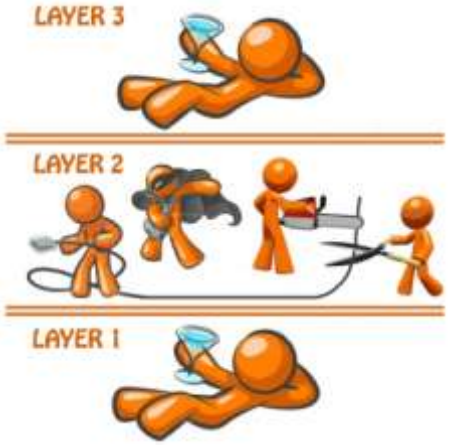


Figure 2. Layer 2 is attacked

There are three main classes of attacks:

- Spanning Tree Protocol
- Cisco VLAN[9]/Trunking Protocols
- Other attacks[12]

Spanning Tree Protocol

Spanning-Tree Protocol (STP) prevents loops from being formed when switches[10] or bridges[11] are interconnected via multiple paths. Spanning-Tree Protocol implements the 802.1D IEEE algorithm by exchanging BPDU[12] messages with other switches to detect loops, and then removes the loop by shutting down selected bridge interfaces. This algorithm guarantees that there is only one active path between two network devices. [13] Within this framework the bridges negotiate between them, who will be the „root" bridge in the network, determine the least cost paths and disable all other paths.

The attack technique of this protocol, the *Spanning Tree Protocol manipulation attack*, within this framework the attacker sends BPDUs to become „root" bridge (or switch) in the network. Therefore the attacker can influence the flow of data. Requires attacker is dual homed to two different bridges (or switches) or one of the two connections is WLAN[13] access point which is not connected to the same bridge (or switch).

[9] Virtual LAN: A VLAN has the same attributes as a physical LAN. One network cable can have more grouped VLANs on the same network switch port (interface). [15]
[10] Switch is a computer networking device that links network devices.
[11] A bridge is a device which connects two parts of a network together at the data link layer (layer2).
[12] Bridge Protocol Data Unit: When STP is enabled, bridges send and receive spanning-tree frames, called BPDUs, at regular intervals and use the frames to maintain a loop-free network. [14]
[13] Wireless LAN

Attacker can eavesdrop all messages of victims; he can inject new ones in MITM[14] position. (Figure 3.)

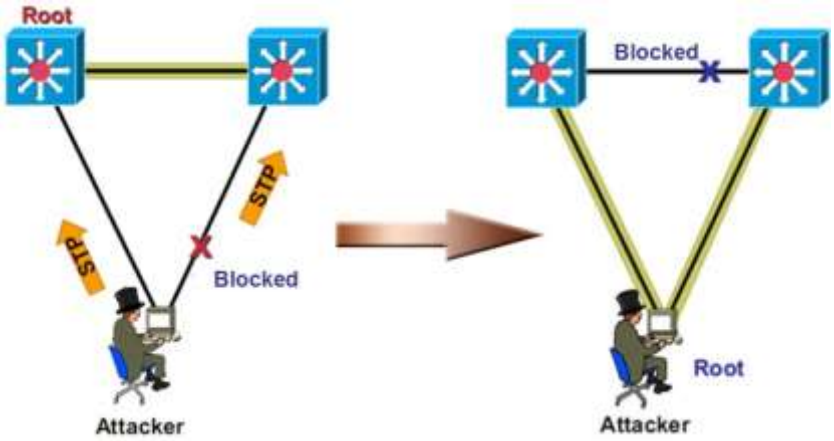


Figure 3. Spanning Tree Protocol manipulation [10]

Cisco VLAN/Trunking Protocols

VLAN's allow a network manager to logically segment a LAN into different network of departments such as marketing, sales, accounting, and research. There are lots of VLANs over the backbone switches of Internet connecting different site of company. The attacker has two method of *VLAN hopping attack* in order to be a member of other VLANs:

1. Basic VLAN hopping attack:The switches connected to a trunk[15] link, which has access to all VLANs by default. The attacker station can spoof as a switch with DTP[16] signaling, and the station will be a rogue switch – member of all VLANs and all traffic can be monitored. The „Yersinia" software is very useful for this task. (Figure 4.)

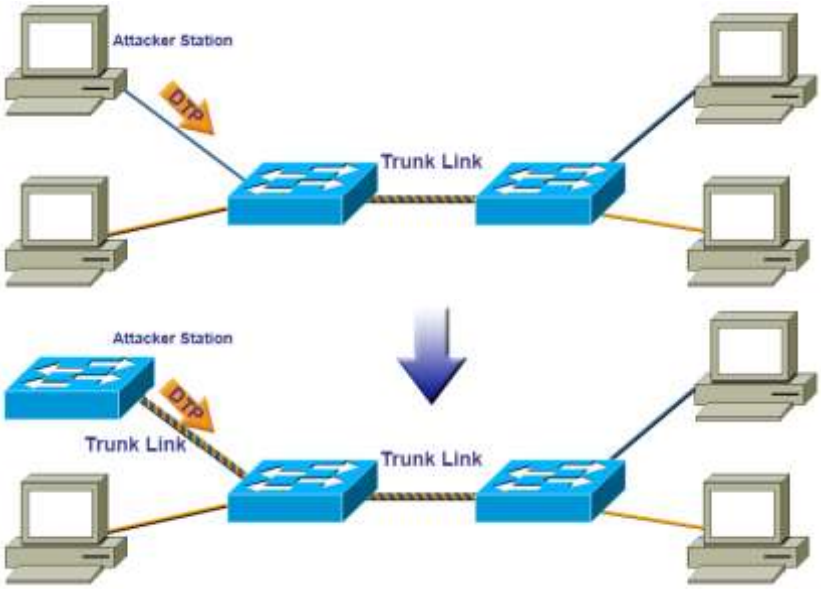


Figure 4. Basic VLAN hopping attack [10]

[14] Man-in-the-middle
[15] It is used to route traffic for multiply VLANs across the same physical link.
[16] Dynamic Trunk Protocol: Automates (802.1q/ISL) trunk configuration and operates between switches. DTP usually enabled by default. 802.1q is the networking standard that supports VLANs on an Ethernet network. ISL is a Cisco proprietary protocol that maintains VLAN information.

2. Double tagging VLAN hopping attack*:* A widely used VLAN networks operate with an additional 802.1q header, or VLAN tag to distinguish the VLANs. VLAN tag changes the information frame. The service-provider infrastructures are double-tagged, with the outer tag containing the customer's access VLAN ID, and the inner VLAN ID being the VLAN of the incoming traffic. When the double-tagged packet enters another trunk port in a service-provider core switch, the outer tag is stripped as the packet is processed inside the switch. The attacker sends „Double tagging" frame. The first belongs to the own VLAN and the second one belongs to the target VLAN. The switch performs only one level decapsulation (strip off first tag) and the attacker can use unidirectional traffic to the Victim. This method works if trunk has the same VLAN as the attacker and the trunk operates with 802.1q. (Figure 5.) [10]

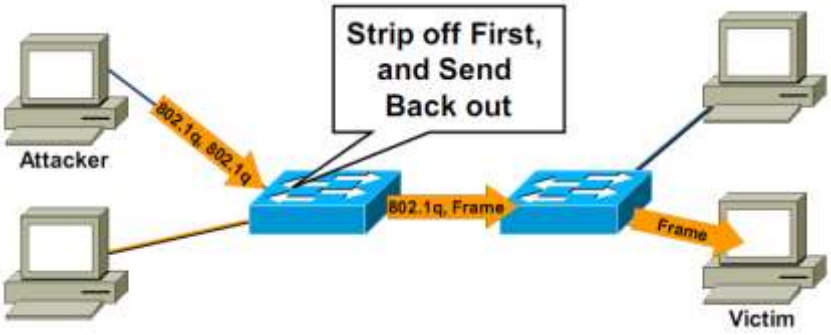


Figure 5. Double tagging VLAN hopping attack [10]

Other attacks

In this section, only those relevant attack techniques will be explained - in addition to the previous ones - which are widely known and worth considering at the developing of the system-wide security policy and at work out of the basic safety procedures.

Cisco Discovery Protocol (CDP) attack

The Cisco Discovery Protocol (CDP) is a proprietary protocol that all Cisco devices can be configured to use. CDP discovers other Cisco devices that are directly connected, which allows the devices to auto-configure their connection in some cases. CDP messages are not encrypted. Most Cisco routers[17] and switches have CDP enabled in the default configuration.

Can be used to learn sensible information about the CDP sender (IP address[18], Cisco IOS[19] software version, router model, capabilities...).

Besides the information gathering benefit CDP offers an attacker, there was vulnerability in CDP that allowed Cisco devices to run out of memory and potentially crash if you sent it tons of bogus CDP packets.

CDP is unauthenticated: an attacker could craft bogus CDP packets and have them received by the attacker's directly connected Cisco device. (Figure 6.) If the attacker can get access to the router via Telnet, he can use the CDP information to discover the entire topology of your network at Layer 2 and 3, and he could launch a very effective attack against your network.[10], [17]

[17] A router is a device that forwards data packets between computer networks. A router is connected to two or more data lines from different networks.

[18] Internet Protocol address is a numerical label assigned to each device (e.g. computer, printer) in a computer network. [18]

[19] Internetwork Operating System is software used on most Cisco Systems routers and switches.

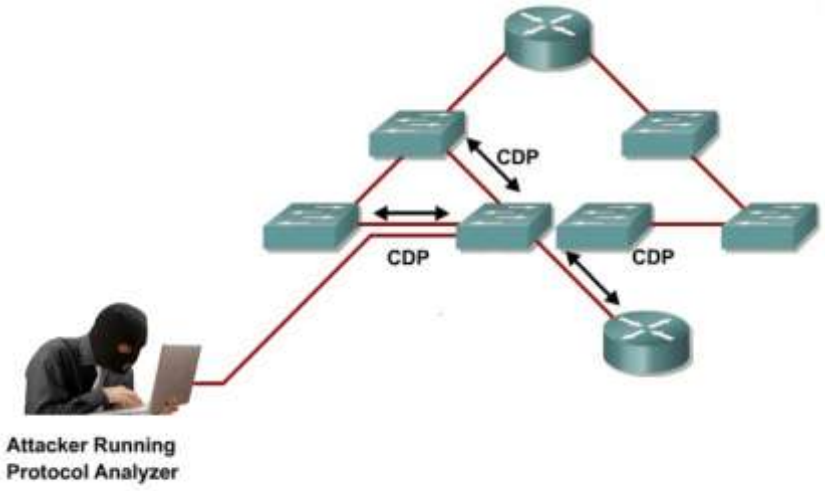


Figure 6. CDP attack

CAM[20] table overflow attack

Widely used Cisco switch models use the CAM table, which stores information such as MAC[21] addresses available on physical ports. CAM tables (sometimes called MAC address table) have a fixed size (19KB...128KB, it can store about 100…100000 MAC entries).

When frames arrive on physical ports, the source MAC addresses are learned from Layer 2 packet header and recorded in the CAM table. All entries have a default aging timer which is 300 seconds. If a host does not send frames toward the port, the entries will be removed after 5 minutes.

The switch forwards the frame to the MAC address port designated in the CAM table. If the MAC address does not exist, the switch acts like a hub[22] and forwards the frame out every other port on the switch.

There is a common tool that performs CAM overflow. This tool can generate 155000 MAC entries on a switch per minute. A CAM overflow attack turns a switch into a hub, which enables the attacker to reach every host on the network, to eavesdrop on a communication and perform MITM attacks. This method is applicable to attack the neighbor switches. (Figure 7.) [10]

[20] Content Addressable Memory

[21] Media Access Control - is a unique identifier assigned to network interfaces for communications on the physical network.

[22] Hub is a device for connecting multiple Ethernet devices together. A hub works at the Layer1 If a frame introduced at one port appears at every another port.

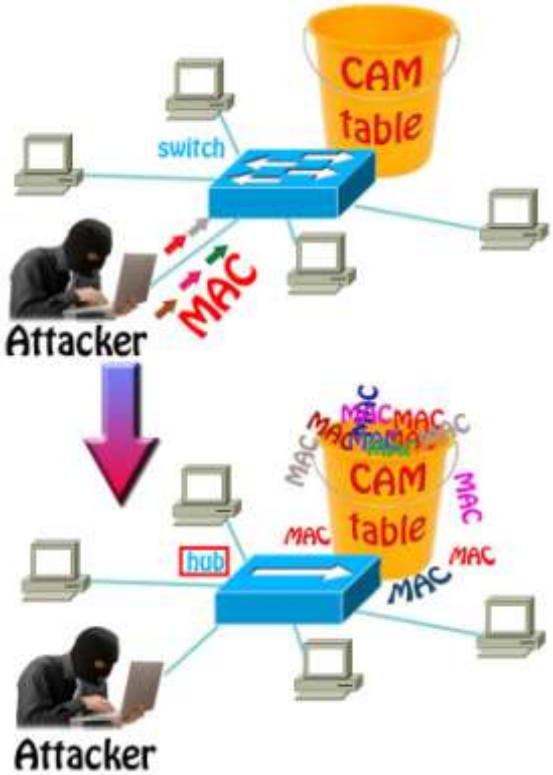


Figure 7. CAM table overflow attack

MAC Spoofing (ARP[23] poisoning)

How many people think that to see the ARP packets on your own computer? Everybody can answer to this question differently.

MAC spoofing attacks are launched by attacker on a Layer 2 network. The attacker can send out a gratuitous ARP (GARP) to the network. GARP is used by hosts (computers) to „announce" their IP address to the local network and avoid duplicate IP addresses on the network. Computers, routers and other network hardware may use cache information gained from gratuitous ARPs. Because ARP has no methods for authenticating ARP replies on a network, ARP replies can come from other system which is expected.

In one common attack the attacker says „my PC is the default gateway" so that users send their traffic through the attacker rather than the default gateway. The attacker then forwards user traffic to the real default gateway so that victims do not notice any change in their network access. An attacker on a fast enough host can capture the traffic and can modify them. Figure 8. [10]

[23] Address Resolution Protocol is a request and reply protocol. It is used to map of MAC address to IP address.

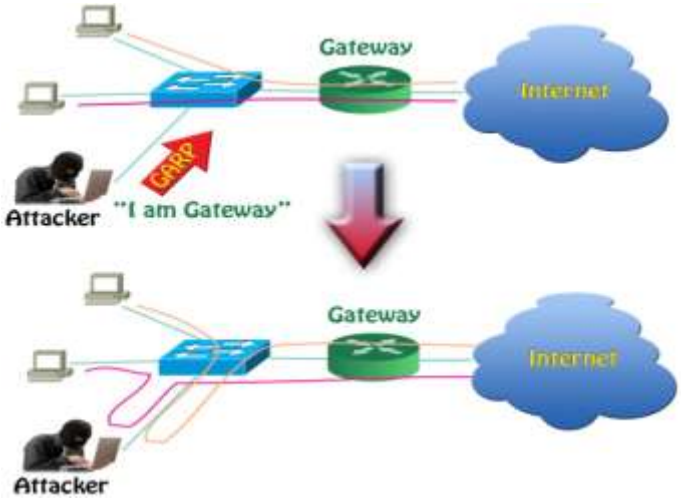


Figure 8. MAC Spoofing

DHCP[24] starvation attack

The DHCP server is used to configure network devices so that they can communicate on computer network. The clients and a server are operating in a client-server model. DHCP client sends a query requesting necessary information (IP address, default gateway[25], and so on) to a DHCP server. On receiving a valid request, the server assigns the computer an IP address, and other IP configuration parameters.

This is special kind of attack where attacker sends tons of requests to the DHCP server with a false MAC address. If enough requests flooded onto the network, the attacker can completely exhaust all of the available DHCP addresses. Clients of the victim network are then starved of the DHCP resource

The network attacker can then set up a Rogue DHCP Server on the network and reply modified IP configurations to the victims. (Figure 9.) These parameters ensure the MITM possibilities to the attacker. [10]

Figure 9. DHCP starvation attack

[24] Dynamic Host Configuration Protocol is a network protocol.

[25] Typically is a router on a computer network that serves as an access point to another network (e.g. public internet)

Wireless 802.11[26] (Wi-Fi) attack

Everyone is familiar with the Wi-Fi networks. Wi-Fi can be less secure than wired (ethernet) connections because an attacker does not need a physical connection, since only need one antenna and a laptop to compromise one.

In this type of attack, the attacker can execute:

- to insert himself in the MITM position (client's data can be modified,
- to deny the service,
- to capture all traffic.

In order to insert oneself in the middle of the communication, one has two possibilities:

- Send deauthentication packets to one or more clients which are currently associated with an AP and set up a rouge AP with the same credentials as the original for purposes of allowing the client to connect to it.
- Set up a rouge AP with a big signal (bigger than the original) and same credentials as the original for purposes of allowing the new client to connect to it.

The subject of another article could be: how can we access the security protocol of Wi-Fi.

In order to deny service there are two possibilities:

- There are several commercial devices available today that can bring down the wireless LAN with a lot of noise at wireless operation frequency.
- The affected AP can be rejected that user access by flooding network traffic.

In order to capture traffic of victim with network interface card, there are two possibilities (even from huge distance):

- Card is used in normal mode.
- Card is set up in monitor (promiscuous[27]) mode. [7], [19], [20]

5. CONCLUSIONS

This article is an overview of the most well-known attack techniques on Layer 2 and draw attention to the vulnerabilities of this level emphasizing that the other layers being aware of the problem. A lot of attention is paid to securing the higher layers of the OSI reference model with network-level devices such as firewalls, intrusion protection systems (IPS), and applications such as antivirus and host-based intrusion protection (HIPS).

The attacker can

- eavesdrop traffic,
- manipulate data,
- deny the information flow, and
- use combination of the above mentioned.

Apply any of these options pose a serious threat to critical infrastructure, state institutions or governmental systems, even if no attacking intent is used. Certain critical infrastructure is controlled via the Internet which is maintained by wired and mobile telecommunication carriers.

[26] Wireless communication protocol on Layer 1 and Layer 2.

[27] Promiscuous mode is a mode for a wired network interface controller or wireless network interface controller. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.

Transmission of the information is important to emphasize, as also can cause disaster. For example, the control information cannot reach to endpoints due to unavailability of service. The attacker is easy to achieve this position. For instance powerful jamming equipment is used in wireless or mobile technology. In view of the rapidly developing technology background of Wi-Fi area, where the marketed devices already have 7Gbps data transmission speeds at the end of year and one of the dominant mobile manufacturer's vision of the mobile transmission, you can easily see that the data flow will significantly rise. [8], [21]

In addition these methods are mentioned in the article are likely to access IDs and passwords, which is also threat. Of course, the attack techniques are known by manufacturers and they do everything to mitigate them. For example Cisco implemented a technology into IOS called Port Security that mitigates the risk of a Layer 2 CAM overflow attack.

The above mentioned attacks can be used in only certain settings, therefore it should be mentioned the human factor, which plays a key role in the development and operation of those devices. This topic is worth a detailed another article.

In order to eliminate these attack techniques protection of LAN networks of critical infrastructures must be improved. The government should make a laws, which placed in a position of law enforcement and military organizations, which provide greater suasion over the security of telecommunications networks.

In summary we must be prepared to mitigate the methods of attacks when implementing security systems of critical infrastructure on all levels (including Layer 2) of OSI model.

References

[1] GReAT, Kaspersky Lab Expert: The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies https://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies (2013.01.14.)

[2] MTI: Hackerek támadták meg az Európai Bizottságot http://www.origo.hu/nagyvilag/20121110-hackerek-tamadtak-meg-az-europai-bizottsagot-azerbajdzsanban.html (2013.01.14.)

[3] OSI model, http://en.wikipedia.org/wiki/OSI_model (2013.01.12.)

[4] Trójai program, http://hu.wikipedia.org/wiki/Tr%C3%B3jai_program (2013.01.12.)

[5] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana (BOLYAI SZEMLE XVII. évf. 4., 2008)

[6] Backdoor computing, http://en.wikipedia.org/wiki/Backdoor_%28computing%29 (2013.01.16.)

[7] Wi-Fi, http://hu.wikipedia.org/wiki/Wi-Fi (2013.01.16.)

[8] Samsung Exynos 5 Octa & Flexible Display at CES 2013 Keynote http://www.youtube.com/watch?v=GDJ67df0p6A&feature=player_embedded (2013.01.15.)

[9] MIME, http://en.wikipedia.org/wiki/MIME/ (2013.01.16.)

[10] Sean Convery, Cisco Systems: Hacking Layer 2: Fun with Ethernet switches http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf (2013.01.18.)

[11] Yusuf Bhaji, Cisco Systems: LAYER 2 ATTACKS & MITIGATION TECHNIQUES http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11_603839.pdf (2013.01.21.)

[12] Enno Rey Lead Auditor, ERNW GmbH: Network Security on OSI Layer 2 and 3 http://pdfsb.com/readonline/62464a4c65677431586e522b4348706b55513d3d-4366147 (2012.10.04)

[13] Spanning Tree Protocol http://www.cisco.com/en/US/tech/tk389/tk621/tsd_technology_support_protocol_home.html (2013.01.19)

[14] Wifi Glossary OL-7080-01 http://www.cisco.com/en/US/docs/wireless/access_point/1300/12.3_7_JA/configuration/guide/b37glos.pdf (2013.01.22)

[15] Virtual LAN, http://en.wikipedia.org/wiki/Virtual_LAN (2013.01.18)

[16] How NAT Works, http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a008009484831.shtml (2013.01.17)

[17] Common Switch Securitty Attacks- CDP and Telnet Attacks http://ccnaanswers-khim.blogspot.hu/2011/05/common-switch-securitty-attacks-cdp-and.html (2013.01.23)

[18] IP address, http://en.wikipedia.org/wiki/IP_address (2013.01.12)

[19] SANS Institute: Understanding Wireless Attacks and Detection: http://www.sans.org/reading_room/whitepapers/detection/understanding-wireless-attacks-detection_1633 (2013.01.23)

[20] Ec-Council,Course Technology: Ethical hacking and Countermeasures Courseware volume 4. page 2124-2254.

[21] Jön a 7 Gbps-os WiFi http://www.sg.hu/cikkek/94678/vezetek_nelkuli_atvitel_hd_eszkozokre/ (2013.01.16.)

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Szabó Tibor
szabo.tibor@nbsz.gov.hu

CDP (CISCO DISCOVERY PROTOCOL) TÁMADÁS

Absztrakt

Korábbi cikkemben érintőlegesen ismertettem néhány, közismertebb Layer 2[1] szintű hálózatbiztonsági problémát és támadási formát, melyre érdemes odafigyelni mind a tervezési szakaszban, mind az implementálás során, amikor hálózatok és hálózatvédelmi berendezések topológiájának kialakítása folyik és a konfigurációk véglegesítésre kerülnek az eszközökben. [16] Az említett támadási formák közül ebben a cikkben magára a CDP (Cisco[2] Discovery Protocol) támadásra és annak megértésére koncentrálok – elhagyva azokat a technikai részleteket, melyek nem közvetlenül tartoznak a tárgyhoz.

In my previous article I presented some of most common Layer 2 level network security issues and attack method, which are worth paying attention. When planning and implementing the networks and network security equipment and finalizing the configuration we should pay attention in every stage. [16] I'm focusing now on the attack method of CDP (Cisco Discovery Protocol) – I avoid mentioning those technical details, which are not directly relevant to the issue in this article.

Kulcsszavak: *CDP, layer 2, memória túlcsordulás, sebezhetőség, Yersinia, ~ CDP, layer 2, memory overflow, vulnerability, Yersinia*

[1] Adatkapcsolati réteg az OSI modellben.
[2] A világ vezető hálózati eszköz gyártója.

1. BEVEZETÉS

Napjainkra az internet szolgáltatók országos lefedettséget biztosítanak, mindemellett az információ igény és a sávszélesség növekedése egyre csökkentette ár/sávszélesség arány értékét, mely elérhetőbbé tette a vállalatok, kisvállalatok és az egyének számára is a világhálóhoz való hozzáférés igénybe vételét. Ma már a szolgáltatás hozzáférési pontra csatlakozó egyedi végpontokat nagyvállalatokhoz hasonlóan kisvállalatoknál és egyéni vállalkozásoknál is felváltják a kisebb-nagyobb magánhálózatok, melyek az alkalmazottak részére is elérhetővé teszik a lokális adatbázisokat, számítógépes erőforrásokat és az internet szolgáltatást. Ellenben a hálózatok építése során viszonylag keveset foglalkozunk a biztonsággal és elég gyakran az eszközök alapbeállításával megelégszünk.

Korábbi cikkemben érintőlegesen ismertettem néhány, közismertebb Layer 2 szintű hálózatbiztonsági problémát, melyre érdemes odafigyelni mind a tervezési szakaszban, mind az implementálás során, amikor hálózatok és hálózatvédelmi berendezések topológiájának kialakítása folyik és a konfigurációk véglegesítésre kerülnek az eszközökben. [16] Az említett támadási formák közül ebben a cikkben magára a CDP (Cisco Discovery Protocol) támadásra és annak megértésére koncentrálok – elhagyva azokat a technikai részleteket, melyek nem közvetlenül tartoznak a tárgyhoz.

2. A CDP PROTOKOLL INFORMÁCIÓI

A CDP (Cisco Discovery Protocol) a Cisco által szabadalmaztatott protokoll az OSI Layer 2 szintjén, mely szinte minden Cisco által gyártott eszközön működik. [1], [3] Természetesen a Cisco berendezések széleskörű elterjedésének hatására voltak gyártók, melyek szintén alkalmazták ezt a protokollt a hálózatban való együttműködés megkönnyítése érdekében. Ilyen gyártó volt a HP (Hewlett Packard) is, mely a Procurve 2500 sorozatú switch[3] eszközeiben implementálta ezt a képességet. [2]

A legtöbb Cisco switch és router[4] (útválasztó) berendezésen alapértelmezetten engedélyezve van a CDP funkció, aminek segítségével a közvetlenül egymáshoz csatlakozó eszközök felderíthetik egymást, megtudhatják egymás konfigurációs beállításait és a hibaelhárítás gyorsabban és szakszerűbben végrehajtható.

Nézzük meg, milyen információkat tartalmaz egy router memóriája a hozzá közvetlenül csatlakozó CDP üzenetekből a „show cdp neighbors” utasítással:

```
Router_4#sho cdp neighbors

   Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                     S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Router3             Ser 1          120           R        2500      Ser 0
Router1             Eth 1          180           R        2500      Eth 0
Switch1             Eth 0          240           S        1900      2
```

A tárolt CDP üzenetek között szerepel:

- Device ID: a szomszédos eszköz neve.
- Local Intrfce: a helyi router eszközünk kapcsolódási pontjának típusa és száma, amin keresztül a CDP üzenet érkezik.

[3] Olyan számítógépes hálózatban alkalmazott aktív eszköz, mely összekapcsolja a hálózati eszközöket.

[4] Olyan útválasztó eszköz, mely továbbítja az adatcsomagokat a számítógépes hálózatok között. A router egy vagy több adatvonallal csatlakozik. a különböző hálózatokhoz.

- Holdtme: CDP üzenetek tárolásának ideje másodpercben.
- Capability: a szomszédos eszköz router vagy switch.
- Platform: a szomszédos eszköz típusa.
- Port ID: a szomszédos eszköz csatlakozási pontjának típusa és száma, amiről a CDP üzenet érkezik.

Kérdezzük le a szomszédos Router1 eszköz adatait kissé részletesebben a „show cdp entry Router1" paranccsal: [4]

```
Router_4#sho cdp entry Router1
   -------------------------

   Device ID: Router1
   Entry address(es):
    IP address: 10.0.10.2
   Platform: cisco 2500, Capabilities: Router
   Interface: Ethernet1,  Port ID (outgoing port): Ethernet0
   Holdtime : 180 sec

   Version:
   Cisco Internetwork Operating System Software
   IOS (tm) 2500 Software (2500-JS-L), Version 11.2(15)
   RELEASED SOFTWARE (fcl)
   Copyright (c) 1986-1998 by Cisco Systems, Inc.
   Compiled Mon 06-Jul-98 22:22 by tmullins
```

A tárolt CDP üzenetek között szerepel:

- Device ID: a szomszédos eszköz neve.
- Entry address (es): a szomszédos eszköz IP címe.
- Platform: a szomszédos eszköz típusa.
- Capabilities: a szomszédos eszköz router vagy switch.
- Interface: a helyi router eszközünk kapcsolódási pontjának típusa és száma, amin keresztül a CDP üzenet érkezik.
- Port ID: a szomszédos eszköz csatlakozási pontjának típusa és száma, amiről a CDP üzenet érkezik.
- Holdtme: CDP üzenetek tárolásának ideje másodpercben.
- Version: a szomszédos eszközön futó szoftver (OS) típusa.

A CDP információk un. multicast[5] üzenetekkel vannak szétküldve periódikusan a hálózat adatkapcsolati rétegén, ezért az útválasztók (router) ezeket már nem terjesztik tovább más hálózatok felé. A megérkező multicast üzenetek az egyes eszközök helyi CDP adatbázisát frissítik. A periódikusság mértékét az időzítések (timer) segítségével lehet beállítani, melyek meghatározzák, hogy:

- milyen gyakran (update timer) kell szétküldeni a CDP információkat és
- mennyi ideig (holdtime) kell tárolni a megkapott CDP üzenetet.

[5] Olyan kommunikációs forma, melyben egy adó és több vevő egy közös csatornán információt cserél. Ilyen például a hangközvetítés.

Nézzünk az időzítésekre egy példát lekérdezve „show cdp” paranccsal egy router adatait:

```
Router_4#show cdp
  Global CDP information:
          Sending CDP packets every 60 seconds
          Sending a holdtime value of 180 seconds
```

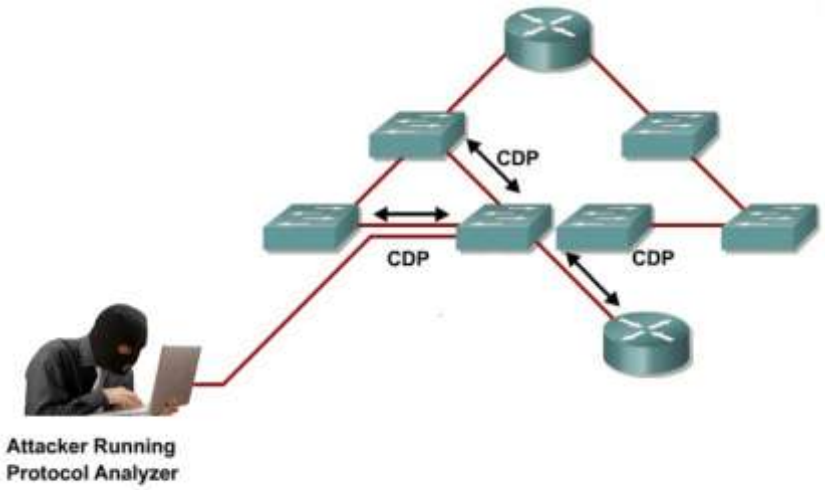
3. A CDP TÁMADÁS

A CDP támadás sajátosságainak egyszerűbb értelmezhetősége kedvéért érdemes felbontani azt két részre:

- memória túlcsordulást okozó módszerre és
- információszerzési módszerre.

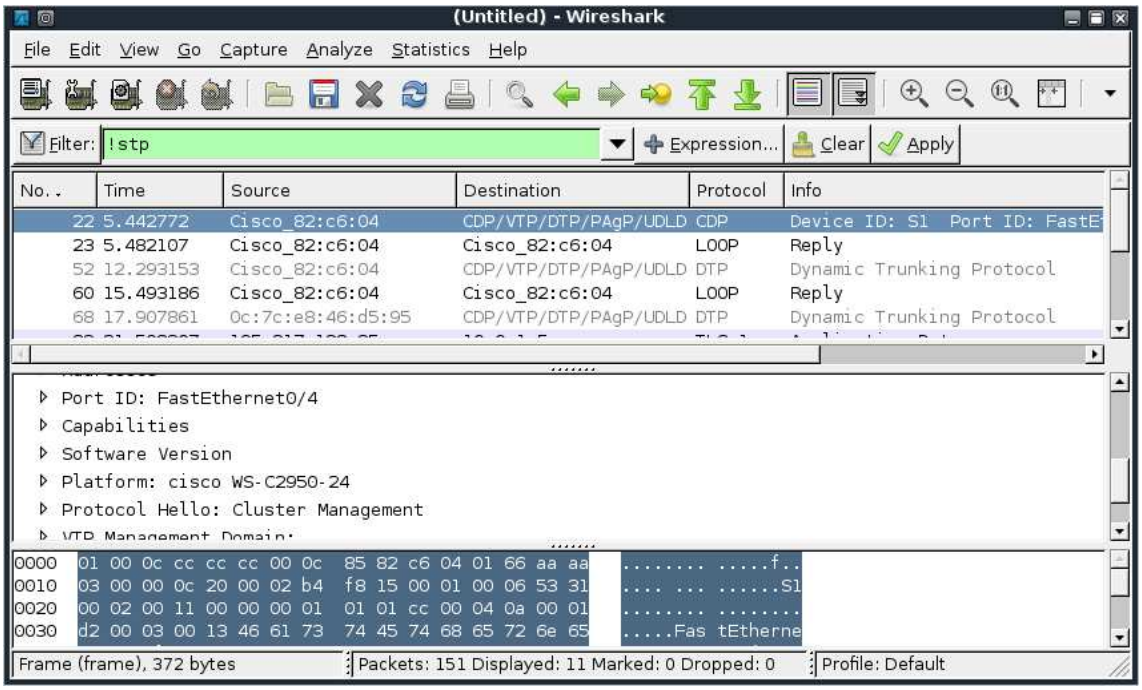
A memória túlcsordulást okozó módszer azt használja ki, hogy az eszközök memória allokációs képességei gyengék, ezáltal az eszközben futó, egyes folyamatok hajlamosak a másiknak a memória területére ráírni adatokat. Az inkoherens adatok értelmezésekor abnormális működés vagy teljes leállás következik be, amit hamis CDP csomagok hálózatba történő tömeges küldésével lehet elérni egyes hálózati elemeknél. [14]

Az információszerzési módszer azt használja ki, hogy a CDP üzenetek nincsenek titkosítva, ezért könnyen értelmezhetővé válik bárki számára, aki a hálózatra felcsatlakozva (vezetékkel vagy vezeték nélkül) passzívan monitorozza az IP forgalmat. (1. ábra).



1. ábra. CDP üzenetek monitorozása

A következő ábra azt szemlélteti, hogy mit láthat a támadó az IP forgalom monitorozása közben a közismert Wireshark – ingyenes hálózati forgalomanalizáló szoftver – kezelő felületén. (2. ábra)



2. ábra. Wireshark felülete [5]

A forgalom passzív monitorozásán kívül egy másik lehetséges megoldás a támadó számára, ha aktívan, saját számítógépéről hamis CDP üzeneteket küld szét a hálózatban, amire a közvetlenül csatlakozó Cisco eszközök a protokoll szabályai szerint válaszolnak. A fentiekben részletezett információk, melyeket az eszközök egymás között cserélnek, sok olyan értékes adatot tartalmaznak, amelyek hasznosak a támadó számára. Nézzük ezeket sorban egy-egy példával illusztrálva, hogy mire használhatóak fel az egyes adatok.

A *szomszédos eszköz IP címe*[6] (Entry address) alapján lehetősége van a támadónak leszűkíteni azt a tartományt, amire a későbbiekben koncentrálnia kell. Vegyük például a privát címeket (3. ábra), amik a LAN hálózatok címkiosztására vannak fenntartva:

Tartomány kezdete	Tartomány vége	Címek száma
10.0.0.0	10.255.255.255	16 777 216
172.16.0.0	172.31.255.255	1 048 576
192.168.0.0	192.168.255.255	65 536

3. ábra. Privát címek

A címek számában az egyes értékek közötti (alulról felfelé haladva) 16 szoros szorzó elég nagy érték, ha figyelembe vesszük, hogy egy automata biztonsági szkenner (mint pl.: nmap, Nessus) jelentős időt (több perc) tud eltölteni egy adott hálózati címen lévő eszköz biztonsági réseinek felderítésében. Amennyiben csak egy kisebb IP tartományra kell koncentrálni, akkor jelentős időt lehet megtakarítani, mindazonáltal kevesebb idő is elég a hálózati elemek sérülékenységeinek felderítéséhez.

Az *eszköz fajtája* (router vagy switch) további támpontot ad a hálózati topológia felderítéséhez, mivel a router eszközöket általában olyan helyre építik be, ahol különböző IP címtartományba eső hálózatokat, különböző protokollokat és/vagy csatlakozási felületeket alkalmaznak a hálózatban. A router egyik speciális funkciója a hálózati átjáró (gateway), melynél könnyen feltételezhető, hogy egy másik más IP cím tartománnyal rendelkező hálózat is létezik a közvetlenül láthatón kívül.

[6] Internet protokoll cím egy olyan numerikus jelölés, mely minden eszközhöz hozzá van rendelve a számítógépes hálózatban.

A *hálózati elem típusa* (Platform. pl.:WS-C2950-24) és a rajta futó operációs rendszer *verzió száma* (Version. pl.: 12.1(12c)EA1) alapján meghatározható, hogy feltártak-e korábban sérülékenységet az eszközön, aminek kiaknázásával hathatós támadás indítható a hálózati elem ellen. A meghatározást megkönnyíti, hogy az interneten sok olyan adatbázis található ma már, ahol összegyűjtik, rendszerezik és publikálják az eszközök és rendszerek sérülékenységeit. Egy közismert, sérülékenységekkel foglalkozó internetes honlap (www.securiteam.com) adatbázisából lekérdezhetőek a „Cisco" sérülékenységek, aminek eredményeként 922 különböző bejegyzést (2013. 02. 08) kapunk. Ez tovább szűkíthető a „Cisco ios" kérdéssel magára az operációs rendszerek sebezhetőségeire. Ekkor a felsorolás már csak 223 elemből áll, amik között sok figyelemre méltó található aktív támadás szempontjából.

Az eszköz konkrét típusa és sérülékenysége alapján kiválaszthatóvá válik az a módszer, amivel a támadó elérheti célját. Ki kell hangsúlyozni, hogy e célok között nem csak a számítógépes rendszerekhez való jogosultság megszerzése, az adatbázisokból történő információk kiszivárogtatása állhat, hanem a – ma már egyre gyakoribb – szolgáltatások vagy a hálózat megbénítása és elérhetetlenné tétele is. Széles körben ismert, hogy pont ez volt a cél 2007-ben Észtországban, ahol naponta bankok, médiacégek és kormányhivatalok szerverei voltak elérhetetlenek – többhetes támadássorozat alatt – órákon keresztül. Könnyen belátható mindenki számára, hogy ezzel a módszerrel hasonló mértékű károkat lehet okozni bárhol a világon a kritikus infrastruktúrákban annak ellenére, hogy jól képzett, professzionális informatikusok megtettek mindent a védelmi rendszerek képességeinek maximális szintre hozásában. Ennek a legegyszerűbb magyarázata az, hogy a rendszerek építésénél gyakran hagyatkozunk mások által gyártott berendezésekre és szoftverekre, melyeknek sérülékenységei ismeretlenek az adott pillanatban a védelmi rendszer szakértő építői számára.

Nézzünk egy-két konkrét példát sérülékenységekre:

1. A Cisco 6400 NRP2 modul Telnet sebezhetősége (dokumentálva: Cisco bug ID CSCdt65960) biztosítja a támadó részére, hogy jelszó nélkül lépjen be az eszköz kezelőfelületére, ha a jelszó eddig még nem volt beállítva. Amennyiben az üzemeltető úgy helyezi üzembe az eszközt, hogy ezt a jelszót nem állította be korábban, akkor a támadó hozzá tud férni az eszközhöz telnet protokoll segítségével a hálózaton keresztül 12.1(05)DC01 vagy annál korábbi Cisco IOS verzió esetén. [6], [7]
2. A Cisco IOS software Telnet opció kezelési sebezhetősége (dokumentálva: Cisco bug ID CSCdm70743) alapján a támadó – kereskedelmi forgalomban vagy ingyenes elérhető – informatikai biztonsági rések automatikus feltárására alkalmas szoftvercsomag alkalmazásával a Cisco router újraindulását éri el, miközben bizonyos UNIX alapú rendszerek specifikált sérülékenységeinek (Telnet ENVIRON option) jelenlétét teszteli. Mielőtt a router jelezné, hogy elfogadja a jelzett opciót váratlanul újraindul, miközben a hozzá csatlakozó infrastrukturális elemek természetesen elérhetetlenek lesznek. A hiba érinti az alábbiakban felsorolt eszközöket bizonyos (11.3AA, 12.0(2)…12.0(6) és – egyes verzió számú – 12.0(7)) Cisco operációs rendszerek esetén:
    a) AS5200, AS5300, és AS5800 sorozatú hálózati beléptető szerver,
    b) 3660, 7100, 7200 és 7500 sorozatú router,
    c) uBR7200 kábel modem végződtető router,
    d) SC3640 rendszer vezérlő a hálózati beléptető szerverek részére,
    e) AS5800-as sorozatú Voice Gateway,
    f) AccessPath LS-3, TS-3, és VS-3 integrált beléptető rendszerek különböző szolgáltatásokhoz. [8], [9]

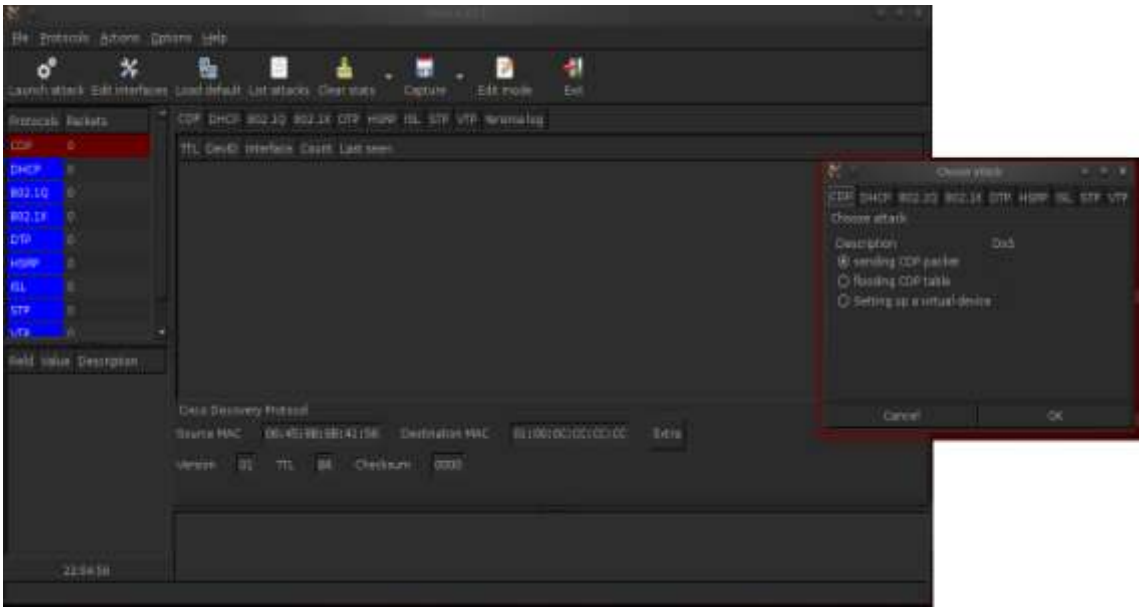
A felsorolt hálózati elemek számossága arra utal, hogy „szinte” független volt a platformtól az operációs rendszer kódjában található hiba, amit a gyártó az újabb verziók kiadásakor megismételt.

A CDP támadás eszköze

Amennyiben a támadó kevésbé akar fáradozni a hálózaton áramló IP csomagok – Wireshark programmal történő – monoton és esetenként kimerítő analizálásával, és drága szabadidejét szeretné más, ennél nagyobb kihívást jelentő támadási vektorok alkalmazásával tölteni, akkor számára kézenfekvő, hogy a CDP támadás kivitelezésére az egyik, széles körben ismert, *Yersinia* – ingyenesen letölthető – szoftvert fogja fegyvertárából elővenni.

A Yersinia egy speciális keretrendszer, mely Layer 2 szintű támadások végrehajtására lett kialakítva. Létezik parancssoros, interaktív karakteres és – ma még csökkentett funkciókkal rendelkező – grafikus felületű változata is. Az alkalmazás CDP menü pontja további funkciókat kínál:

- CDP csomagok küldésére a hálózatba,
- a szomszédos Cisco eszköz CDP táblájának elárasztására és
- virtuális eszköz létrehozására. (4. ábra)



4. ábra. A Yersinia grafikus felülete

A keretrendszer emellett lehetőséget biztosít támadások és penetrációs vizsgálatok végrehajtására különböző protokollok (VTP[7], ISL[8], HSRP[9], DHCP[10], DTP[11], STP[12], IEEE 802.1Q[13] és IEEE 802.1X[14]) esetén, melyek részletes – és egyben érdekességekben bővelkedő – kifejtése messze túlmutat a cikk keretein. [10]

[7] VLAN Trunking Protocol
[8] Inter-Switch Link Protocol
[9] Hot Standby Router Protocol
[10] Dynamic Host Configuration Protocol
[11] Dynamic Trunking Protocol
[12] Spanning Tree Protocol
[13] Hálózati szabvány Virtual LAN-ok számára. [11]
[14] Szabvány Port alapú hálózat hozzáférés vezérlésekről. [12]

4. VÉDEKEZÉS CDP TÁMADÁS ELLEN

A CDP támadások módszerétől függően a Cisco különböző védekezési eljárást, módszert javasolt és/vagy új, javított operációs rendszereket készített. Memória túlcsordulást okozó probléma esetén a gyártó – saját szempontjából – a legkézenfekvőbb megoldást javasolta: meg kell szüntetni a CDP funkciót az egész eszközön „no cdp run" utasítással. Amennyiben a helyi hálózati adminisztrátoroknak továbbra is szüksége van erre a funkcióra, akkor csak bizonyos (számítógép farmok felé vagy internet szolgáltató felé néző) csatlakozási felületeken kell megszüntetni „no cdp enable/set cdp disable" utasítással a CDP csomagok további áramlását.

Természetesen lehetnek olyan esetek, amikor ez utóbbi javaslatot sem lehet elfogadni – ekkor kell a hálózati eszközünk operációs rendszerét lecserélni az alábbiakban felsorolt vagy annál újabb verzióra: [13], [15]

- 12.2(3.6)B
- 12.2(4.1)S
- 12.2(3.6)PB
- 12.2(3.6)T
- 12.1(10.1)
- 12.2(3.6)

5. ÖSSZEGZÉS

Jelen cikk célja leginkább a figyelem felkeltése volt, mivel egyre gyakrabban tapasztalható, hogy a rohamosan fejlődő (pl.: átvitel-technikai sávszélesség, szolgáltatás) igényeket kielégíteni kívánó informatikai menedzsmentnek csak arra marad ideje – mind vállalati, mind állami szektorban egyaránt – a fejlesztés és kivitelezés „szélviharában", hogy a rendszermérnökökkel közösen épphogy üzembe helyezze határidőre a hálózati elemeket. Ennek többnyire az az eredménye, hogy a biztonsági kérdésekre már nem jut elég idő és a router valamint a switch eszközök többnyire gyári (default) beállításokkal és némi alapkonfigurálás után kezdik továbbítani az első biteket. Ez érvényes a hálózatvédelmi eszközök nagy részére is.

A hálózati eszközök gyártói hasonló időprésben vannak az új eszközök mihamarabbi piacra bocsátása miatt, ezért a fejlesztéskor a programkódokban lévő hibák felkutatására és kiszűrésére már nem marad elegendő idő. A szoftverhibák és sérülékenységek előbb vagy utóbb felszínre kerülnek, amiket a támadók kihasználnak terveik végrehajtásához. Mindazok ellenére, hogy a gyártók elismerik eszközeik hibáit, nyilvántartják azokat és gondoskodnak a javításról, még a későbbiekben szembesülhetünk újabb, esetleg korábban nem létező hibákkal is.

Nyilvánvaló, hogy a CDP támadhatósága elég régi keletű, egy kis odafigyeléssel védhető, ellenben most is léteznek sérülékenységek, ami rávilágít arra, hogy az eszközök alkotói ma is tévedhetnek, tehát létezhetnek olyan hibák, amiket mi nem, viszont a támadó ismerhet. Ebből kifolyólag különösen figyelmet kell fordítani a kritikus infrastruktúrák hálózatvédelmi eszközrendszerének kialakítására és a hálózati forgalom elemzésére.

Felhasznált irodalom:

[1] Cisco Discovery Protocol, Posted on July 6, 2011: http://ciscoskills.net/2011/07/06/cisco-discovery-protocol/ (2013.02.05.)

[2] ProCurveSwitch2500Series: http://www.hp.com/rnd/pdfs/datasheets/switch_2500_series.pdf (2013.02.04.)

[3] Using Cisco Discovery Protocol, First Published: February 1, 1995, Last Updated: August 12, 2010: http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cdp_discover.pdf (2013.02.05.)

[4] Cisco Discovery Protocol: http://netcert.tripod.com/ccna/switches/cdp.html (2013.02.05.)

[5] Bobs Double Penetration Adventure - Part 2: http://synjunkie.blogspot.hu/2009_10_01_archive.html (2013.02.05.)

[6] Cisco 6400 NRP2 Telnet Vulnerability: http://www.securiteam.com/securitynews/5GP0D204KA.html (2013.02.03.)

[7] Cisco 6400 NRP2 Telnet Vulnerability, Revision 1.0, For Public Release 2001 June 14 15:00 UTC (GMT): http://www.cisco.com/en/US/products/csa/cisco-sa-20010614-nrp2-telnet.html (2013.02.03.)

[8] Cisco IOS Software TELNET Option Handling Vulnerability, Advisory ID: cisco-sa-20000420-ios-telnet, Revision 1.0, For Public Release 2000 April 20 13:00 UTC (GMT): http://www.cisco.com/en/US/products/csa/cisco-sa-20000420-ios-telnet.html (2013.02.03.)

[9] Cisco IOS Software TELNET Option Handling Vulnerability: http://www.securiteam.com/securitynews/5AQ0G000GI.html (2013.02.03.)

[10] Yersinia: http://www.yersinia.net/doc.htm (2013.02.03.)

[11] Media Access Control (MAC) Bridges and Virtual Bridge Local Area Networks, IEEE Standard for Local and metropolitan area networks, 31 August 2011 — http://standards.ieee.org/getieee802/download/802.1Q-2011.pdf (2013.02.04.)

[12] Port-Based Network Access Control, IEEE Standard for Local and metropolitan area networks 5 February 2010: http://standards.ieee.org/getieee802/download/802.1X-2010.pdf (2013.02.04.)

[13] Sean Convery, Cisco Systems: Hacking Layer 2: Fun with Ethernet switches http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf (2013.01.18.)

[14] Yusuf Bhaiji Understanding, Preventing, and Defending Against Layer 2 Attacks 2009: http://www.cisco.com/web/ME/exposaudi2009/assets/docs/layer2_attacks_and_mitigation_t.pdf (2013.02.16.)

[15] Cisco's Response to the CDP Issue, Document ID: 13621, For Public Release 2001 October 10: http://www.cisco.com/application/pdf/paws/13621/cdp_issue.pdf (2013.02.18.)

[16] Szabó Tibor: „Network security problems on Layer 2”

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Szentgáli Gergely
gergely.szentgali@gmail.com

AZ EURÓPAI UNIÓ KIBERBIZTONSÁGI TÖREKVÉSEI ÉS SZERVEZETEI II.

Absztrakt

Napjainkra a kiberbiztonság kérdése az első számú biztonságpolitikai kihívások között szerepel. Az információs társadalmak biztonságát meghatározó informatikai környezet és a hozzá kapcsolódó kihívások minden államot arra sarkallnak, hogy építsék ki a megfelelő védelmi szerveket és alkossák meg a szükséges jogszabályokat. Ezt a felelősséget az Európai Unió is felismerte és megkezdte a felkészülést ezen új típusú biztonsági kihívás kezelésére. Írásom első részében bemutattam az Unió jogi lépéseit, illetve a Digitális Menetrendet és az ahhoz kapcsolódó feladatszabást. Jelen tanulmányomban az uniós kiberbiztonsági szervezeteket és a lehetséges partnereket fogom megvizsgálni.

In the recent years, the conception of cybersecurity developed into a critical security policy matter. Security challenges associated with the informatical environment, which are determining the security of informational societies, are reinforcing states to create their own enforcement agencies and to materialise the requisite legal measures. The European Union has acknowledged this sort of responsibility, and it began to prepare the management of new forms of security challenges. In the first part of my paperI presented the EU's legal steps as well as the Digital Agenda for Europe and the tasking linked to it. In the current writing I am trying to examine the EU's cybersecurity organizations and its possible partners.

Kulcsszavak: *kiberbiztonság, Számítástechnikai bűnözés elleni küzdelem európai uniós központja,Európai Unió, NATO ~ ENISA,European Cybercrime Centre, cybercrime, NATO*

BEVEZETÉS

Tanulmányom első részében[1] az Európai Unió kiberbiztonsággal kapcsolatos jogi lépéseivel és különböző stratégiáival foglalkoztam.Bemutattam a vizsgált kérdéshez tartozó jogi kereteket és stratégiákat. Bár sok esetben ezek csupán ajánlás jellegűek, de kétségtelenül fontos lépések. Tanulmányom második és egyben záró részében azt fogom megvizsgálni, hogy melyek azok a szervek, amelyek az uniós kiberbiztonságot garantálják, illetve kik azok a partnerek, akik jelentősen hozzájárulnak az európai biztonság ezen szegmensének erősítéséhez.E kapcsolatok és összefüggések feltárása, illetve a figyelem felhívása az esetleges hiányosságokra, kulcskérdés a hatékony és közös védelem kiépítésének tárgyalásakor.

Európai Hálózat- és Információbiztonsági Ügynökség

Minden szervezet felépítésében komoly szerep jut az informatikai kiszolgáló rendszerek védelme érdekében létrehozott szerveknek. Az Unió esetében ez a szerv az Európai Parlament és az Európai Tanács 460/2004/EK rendelete által létrehozott Európai Hálózat- és Információbiztonsági Ügynökség,[2] amely jogilag 2004. március 10-én jött létre.

Az Ügynökség rendkívül széles feladatkörrel bír. Elsődleges feladata az Unió központi informatikai rendszerének felügyelete és védelmének támogatása, illetve a kiberbiztonság erősítése különböző válságmenedzselési feladatok ellátásával; a Bizottságnak adott tanácsokkal és a tagállamok számára nyújtott segítséggel egyaránt. Célja továbbá, hogy erősítse az együttműködést a különálló szervek és tagállamok között, illetve mint kapcsolatfenntartó szerv is működik az Unión kívül kibervédelmi szervezetekkel.

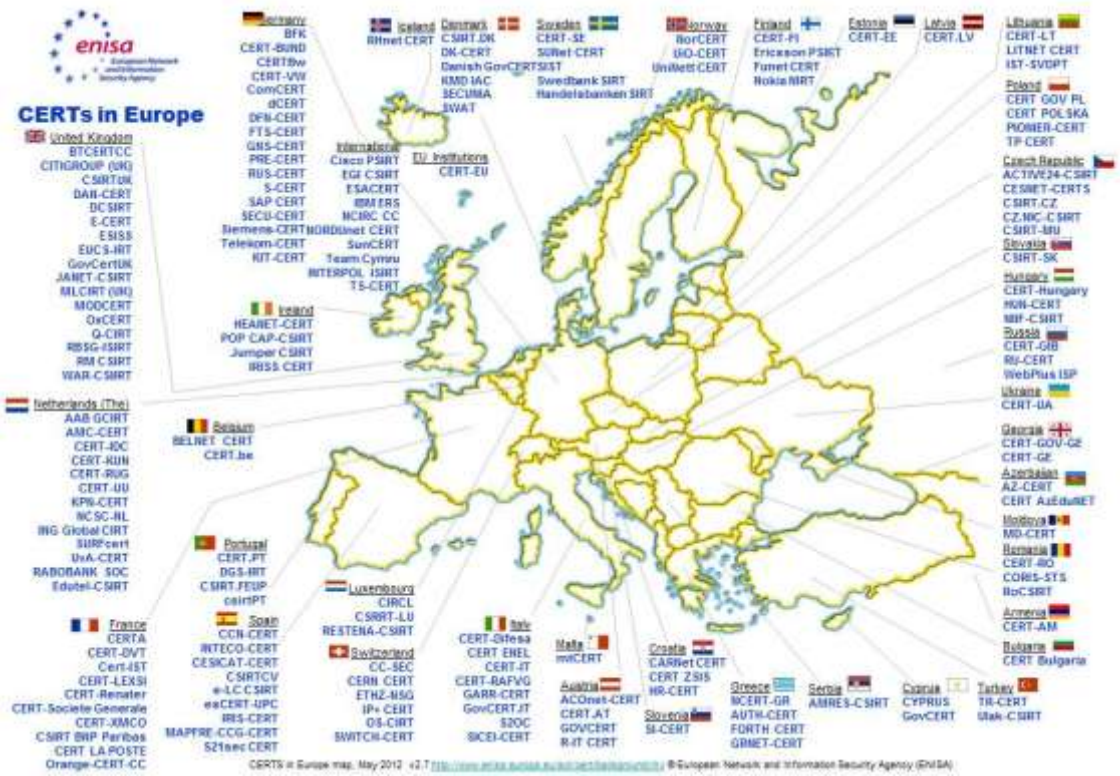
Az Ügynökség egy önállóan működő európai ügynökség, azonban nagyban támaszkodik a tőle függetlenül működő Computer EmergencyResponseTeam-ek (CERT), magyarul a Számítástechnikai Sürgősségi Reagáló Egységek munkájára. A CERT koncepció 1988-ban jelent meg a Carnegie Mellon Egyetemen, az Egyesült Államokban, melynek az volt a lényege, hogy egy szakértőkből álló csoportot hoztak létre, melynek feladata a nemzeti hálózatok felügyelete és valós idejű védelme. A CERT-ek nincsenek alárendelve az Ügynökségnek, azonban együttműködnek vele. Magyarán az Ügynökség jelen esetben koordinációs segítséggel erősíti az európai kibervédelmet.

Számos esetben a CERT mellett/helyett az államok Computer SecurityIncidentsResponse Team-et (CSIRT), azaz Számítógépes Biztonsági Incidensekre Reagáló Csoportot tartanak fenn. Ezek a csoportok alapvetően csupán a nevükben különböznek az előbb említettektől, feladatukat és hatáskörüket tekintve azonban ugyanazok.

Sok esetben ezek a szervek látják el a nemzeti kibervédelmi felügyeletet, ez nagyban jellemző azon uniós tagállamokra is. Az európai megoszlásról lásd az 1. ábrát.

[1] SZENTGÁLI Gergely: *Az Európai Unió kiberbiztonsági törekvései és szervezetei I.*In: Hadmérnök. VII. évfolyam. 2012/4. 172-179. o.

[2] European Network and InformationSecurityAgency (ENISA)



1. ábra. Az európai CERT hálózat
(Forrás: http://www.enisa.europa.eu/activities/cert/background/inv/files/certs-in-europe-map/at_download/fullReport)

Magyarországon három CERT működik jelenleg: HUN-CERT SZTAKI, NIIF-CSIRT és a CERT-Hungary. Ezek közül a CERT-Hungary, azaz a Nemzeti Hálózatbiztonsági Központ az a kormányzati szerv, amely ellátja a nemzeti infrastruktúrák védelmét.

Ezek az egységek a kibervédelem zászlóshajói, nem egy esetben tettek már kiváló szolgálatot az államoknak, többek között Magyarországnak is. Velük kapcsolatosan valóban elmondható, hogy óriási hangsúly van az együttműködésen. Pontosan ez adja meg erejüket, hiszen az önálló műveletek kivitelezése mellett kiválóan képesek – számos esetben az Ügynökség koordinációs segítségével – uniós szinten is együtt dolgozni.[3] Mindezekhez kapcsolódóan üdvözölendő hír, hogy 2012. szeptember 11-én létrehozták az Unió ezen kiemelt szervét, az EU-CERT-et.[4]

A CERT/CSIRT szervek közötti európai és regionális együttműködést hivatott támogatni a TF-CSIRT szakmai platform, ami a hatékony információáramlás biztosításával kívánja fokozni ezen szervek hatékonyságát. Hasonló fórum az európai kormányokhoz kapcsolódó CERT/CSIRT szervek informális fóruma az ECG,[5] ami hasonló szerepkörrel bír, mint a már taglalt platformok.

A nemzetközi együttműködéselősegítése érdekében alakult meg a több mint 180 szervezetet tömörítő FIRST fórum. A cél a technikai eszközök, információk, eljárások és legjobb gyakorlatok megosztása, illetve új CERT/CSIRT szervezet létrehozásának

[3]CERT cooperation and itsfurtherfacilitationbyrelevantstakeholders.ENISA Report. 2006. 12. 01. 18-41. o.
[4]Sikeres kísérleti projekt hatására nőtt az uniós intézmények kiberbiztonsága. Sajtóközlemény. IP/12/949. Brüsszel, 2012. szeptember 12.
[5]European GovernmentCERTsgroup

elősegítése. A nemzetközi fórum a teljes skálát lefedi: tagjai között egyaránt megtalálhatjuk a kormányzati, vállalati és akadémiai incidenskezelő szervezeteket is.[6]

Véleményem szerint a sikeres felkészülés egyik legjobb eszköze a különböző kibervédelmi gyakorlatok kivitelezése. Az élesben lezajlott támadások könnyen rámutatnak a rendszerek sérülékenységeire, illetve a védelmi képesség hatékonysága is napvilágra kerül – mindez egy biztonságos környezetben. Ezt az Ügynökség is felismerte, és alapvetően NATO minta alapján, elsőként 2010-ben szervezte meg a *Cyber Europe 2010* gyakorlatot. Az esemény során a kritikus információs infrastruktúrák kerültek fókuszba, illetve az, hogy a tagállamok hogyan tudnak együttműködni egy komoly kibertámadás-sorozat alatt.

A gyakorlat hasznát és sikerét figyelembe véve, 2012. október 4-én került megrendezésre a *Cyber Europe 2012*, több mint 300 szakértő részvételével. A többek között Magyarország részvétel lezajlott hálózatbiztonsági gyakorlaton első ízben vettek részt bankok és internetszolgáltatók. Mindezen új szereplők részvétele tovább segíti a komplex kibervédelem kialakítását. A gyakorlat három célt tűzött ki maga elé:

1. Az európai hatóságok közötti együttműködés mechanizmusainak, eljárásainak ésinformációáramlásának tesztelése a hatékonyság és a méretgazdaságosság szempontjából.
2. Az európai köz- és magánszektorbeli szereplők közötti együttműködés vizsgálata.
3. A nagyszabású európai kiberbiztonsági incidensek kezelésére alkalmas hatékonyabbmódszerek kidolgozása a meglévő hiányosságok és kihívások azonosítása révén.[7]

A lezajlott gyakorlatot valamennyi résztvevője hasznosnak és sikeresnek ítélte meg.

További hasznos lépésnek tartom a különböző biztonságtudat erősítő programokat. Az Ügynökség alapfeladatai között is helyet kapó figyelem felkeltő események nagyban hozzájárulnak a hatékonyabb kiberbiztonság eléréséhez. Ezek közé illeszkedik az európai kiberbiztonsági hónap is, amely 2012 októberében kapott helyet. A program célja az volt, hogy EU-szerte felhívja a figyelmet a kiberbiztonság fontosságára, illetve a tudatos internet felhasználásra. A különböző szakmai programok mellett, egy komplett internetes kampány is folyt az események támogatása érdekében.

Összegezve a fent leírtakat, az Ügynökség rendkívül komplex feladatokat lát el.Fontos, hogy a feladatkörök jól elkülöníthetőek legyenek, megszűntetve ezzel a párhuzamos erőfeszítéseket. Gondolok itt például arra, hogy nem feltétlenülszükséges, hogy a kiberbűnözésre is összpontosítson komoly energiát, hiszen arra már megvannak a kijelölt szervek.

Tény, hogy az Ügynökség léte elengedhetetlen az Unió biztonsága tekintetében, tekintve, hogy a közvetlen védelem mellett jelentős szerepe van a biztonságfelfogás formálásában is. Ez pedig az egyik legfontosabb eleme a kibervédelem kérdésének, hiszen biztonsági rést legtöbbször a felelőtlen felhasználó jelent. Pontosan ezért továbbra is meg kell szervezni a tudatosságformáló programokat, illetve az ehhez kapcsolódó tagállami tanácsadást.

Érdemes lenne minden évben megszervezni a már taglalt kibervédelmi gyakorlatokat – valószínűsíthetően ez a trend fog megvalósulni –, de nem csak uniós szinten, hanem tagállami szinten is, annak érdekében, hogy világosan láthatóvá váljon, hogy milyen szinten állnak a nemzeti kiberképességek. Hangsúlyoznunk kell, hogy nincsenek azonos szinten a tagállamok, és ez sok esetben a közös munka akadálya is lehet. Ennek a megoldásában lehet kiváló partner az Ügynökség, aki tagállami szinten nyújtana támogatást a képességek kialakításához.

---

[6]HAIG Zsolt: *Az információbiztonság szabályzói és szervezeti keretei.*In: Hadmérnök. Robothadviselés 7. tudományos szakmai konferencia különszám. 2007. november 7. http://hadmernok.hu/kulonszamok/robothadviseles7/haig_rw7.pdf Letöltés ideje: 2013. február 22.

[7]*Cyber Europe 2012. Főbb következtetések és ajánlások.* ENISA, 2012. december. 4. o.

Mind az együttműködés, mind a kibervédelmi gyakorlatok hasznosságát felismerve, 2010-ben az uniós döntéshozók megerősítették az Ügynökséget, elfogadva az új információs rendszerek elleni támadásokról szóló irányelvet.[8] Ennek értelmében 2017-ig meghosszabbították az Ügynökség megbízatását.

SZÁMÍTÁSTECHNIKAI BŰNÖZÉS ELLENI KÜZDELEM EURÓPAI UNIÓS KÖZPONTJA

A kiberbűnözés fogalmának meghatározása nehéz feladat. A nemzetközi trendeket figyelve elmondhatjuk, hogy – hasonlóan a terrorizmus fogalmához – a törekvések inkább a fogalom tartalmának a meghatározására fókuszálnak egy egységesített definíció létrehozása helyett. Ebből kiindulva megállapíthatjuk, hogy a kiberbűnözés főbb kategóriái a következőek: számítógépes hálózatok és rendszerek feltörése és adatok lopása; hamis identitások használata pénzszerzés céljából; adathalászat; gyermekpornográfia, illetve szerzői jogi bűncselekmények.[9] Ezt erősíti meg a kriminológia is, ami hasonlóan jelöli meg a csúcstechnológiai bűnözés típusait: számítógépes hálózatok feltörése; ipari kémkedés; szoftverkalózkodás; gyermekpornográfia; elektronikus levélbombák; jelszószimatolók (keyloggerek) és hitelkártyacsalás.[10]

A kiberbűnözés veszélyének komolyságát az is mutatja, hogy a Symantec, informatikai biztonsággal foglalkozó cég 2012-es jelentése szerint a számítógépes bűnözés évente megközelítően 110 milliárd dollár veszteséget okoz az államoknak és az egyéni felhasználóknak.[11] Tovább nehezíti a kiberbűnözés elleni harcot, hogy az elkövetők spektruma rendkívül széles: a jól képzett hackerektől kezdve, terroristákon át, az egyszerű felhasználó is kiberbűnözővé válhat, az interneten terjedő elkövetési módszerek megismerésének segítségével.[12]

Az egyre kifinomultabb módszerek és az egyre növekvő esetek száma az Európai Uniót is arra ösztönözték, hogy létrehozzon egy önálló szervet, ami fókuszáltan a kiberbűnözés problematikájával foglalkozik. 2012. március 28-án történt meg ez a lépés: az Európai Rendőrségi Hivatal[13] szervezetén belül megalapították a Számítástechnikai Bűnözés Elleni Küzdelem Európai Uniós Központját,[14] amely 2013. január elsejére érte el teljes műveleti képességét. A szervezet jogelődje a három munkacsoporttal (gyermekek szexuális kizsákmányolása, bankkártyacsalás és kiberbűnözés) rendelkező Csúcstechnológiai Bűnözés Elleni Központ[15] volt.[16]

---

[8] A Bizottság megerősítené az informatikai támadásokkal szembeni védelmet Európában. Sajtóközlemény. IP/10/1239. Brüsszel, 2010. szeptember 30.

[9] SCHREIER, Fred – WEEKES, Barbara – WINKLER, Theodor H.:CyberSecurity: The RoadAhead. DCAF Horizon 2015 WorkingPaperNo. 4. DCAF, 2012. 9-11. o.

[10] ADLER,Freda – MUELLER, Gerhard O. W. – LAUFER, William S.:Kriminológia. Osiris Kiadó, Budapest, 2005. 403-405. o.

[11] 2012 Norton CybercrimeReport. http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf Letöltés ideje: 2013. február 10.vö. Gragido, WILL – Pirc, JOHN: Cybercrime and Espionage. An Analysis of SubversiveMultivectorThreats. Elsevier, 2011. 9-10. o.

[12] SZEGEDINÉ LENGYEL Piroska: Számítógépes bűnözés avagy fiatalok a cyber-térben.In: Hadmérnök. V. évfolyam. 2012/2. 371-373. o.

[13] European Police Office (Europol)

[14] European Cybercrime Centre (EC3)

[15] HighTechCrime Centre

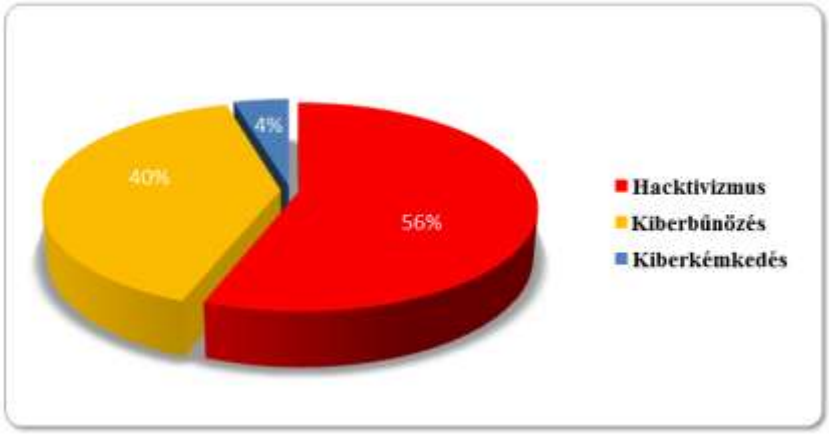
[16] TÓTH Tamás: *Az Europol tevékenysége II. (2010-2012).* http://www.biztonsagpolitika.hu/?id=16&aid=1264&title=az-europol-tevekenysege-ii-2010-2012- Letöltés ideje: 2013. február 11.

Az új Központ megalapításának előzménye a *Stockholmi Program*[17] egyik fontos eleme, a 2010. március 26-án elfogadott, *Az Európai Unió belső biztonsági stratégiája* című dokumentum. Bár a számítógépes biztonság kérdése már a 2008-ban elfogadott *Európai Biztonsági Stratégiában* is megjelent,[18] a kiberbűnözés jelensége, mint hangsúlyos belső probléma itt tűnt fel elsőként.[19] Azonban a Központtal kapcsolatos teendők végül nem a stratégiában, hanem az annak végrehajtásáért felelős akciótervben realizálódtak.[20]

A Központ feladata elsősorban a kiberbűnözés elleni harc koordinálása, különös hangsúlyt fektetve a nagy nyereséggel járó bűnözés elleni tevékenységre. A további feladatok között megtaláljuk még a személyazonosság-lopás elleni küzdelmet; az elektronikus bankszolgáltatásokat érintő bűncselekmények elleni harcot; a gyermekek szexuális kizsákmányolása elleni harcot, illetve az Európai Unió kritikus infrastruktúráinak és informatikai rendszereinek korlátozott védelmét.[21]

A koordinálási feladatokhoz kapcsolódóan a Központ kiemelt feladata, hogy figyelmeztesse a tagállamokat az esetleges fenyegetettségekre. Szintén lényeges lépés az online szervezett bűnözői csoportok felkutatásának és azonosításának támogatása, ezt erősítve a Központ tagállami szinten is képes segítséget nyújtani konkrét nyomozásokhoz.

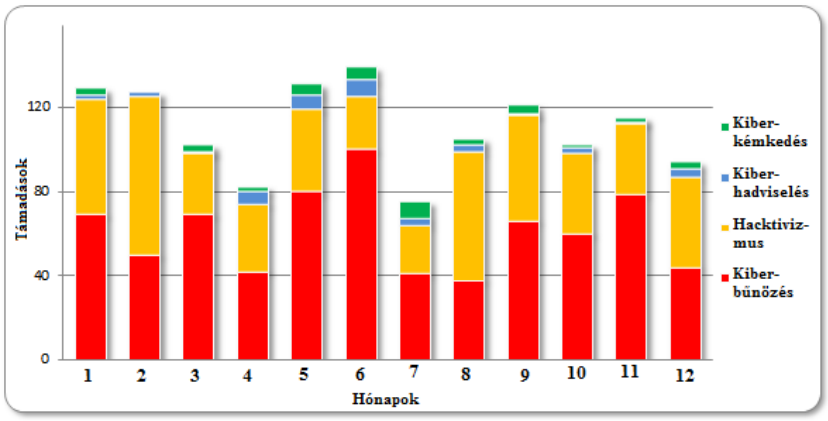
Erre a munkára pedig egyre nagyobb szükség van, tekintve, hogy a számítógépes bűncselekmények száma napról-napra növekszik. Paolo Passeri, a Lastline IT biztonsági cég munkatársa, minden hónapban statisztikát készít az elmúlt hónap globális, reflektorfénybe kerültkibertámadásairól.[22]A legfrissebb havi eloszlásért lásd a 2. ábrát.



2. ábra. 2013januárjában elkövetett kibertámadások motivációs háttere
(Forrás: http://paulsparrows.files.wordpress.com/2013/02/motivations-january-2013.png)

Érdemes megvizsgálnunk a már említett kutató 2012-re vonatkozó egyesített statisztikáját (3. ábra) is. Az általa készített diagramokat figyelembe véve elmondhatjuk, hogy a kiberbűnözés az egyik legjelentősebb eleme a rosszindulatú kibertéri jelenlétnek.

[17]Az Európai Tanács tájékoztatása.A Stockholmi Program – A Polgárokat Szolgáló Védő, Nyitott és Biztonságos Európa. 2010. 5. 4. (2010/C 115/01)
[18]Európai Biztonsági Stratégia. Biztonságosabb Európa egy jobb világban. Luxembourg, 2009. 13-14. o.
[19]Az Európai Unió belső biztonsági stratégiája. Az európai biztonsági modell felé. Luxembourg, 2010. 14. o.
[20]The EU InternalSecurityStrategyin Action: Fivestepstowards a more secure Europe. Press release. MEMO/10/598. Brussels, 22 November 2010.
[21]A számítástechnikai bűnözés elleni küzdelem európai uniós központja az internetes bűnözők elleni küzdelem és az e-fogyasztók védelme érdekében. Sajtóközlemény. IP/12/317. Brüsszel, 2012. március 28.
[22]PASSERI, Paolo: 2012 CyberAttacksStatistics.http://hackmageddon.com/2012-cyber-attacks-statistics-master-index/ Letöltés ideje: 2013. január 22.



3. ábra. A 2012-es év egyesített statisztikája
(Forrás: http://paulsparrows.files.wordpress.com/2012/06/2012-attack-distribution.png)

Magyarországon a Nemzeti Nyomozó Iroda alárendeltségébe tartozó Csúcstechnológiai Bűnözés Elleni Osztálya foglalkozik a leghangsúlyosabb módon a kiberbűnözés problémájával. Hazánk és a kiberbűnözés témája már szerepelt közös platformon, tekintve, hogy 2011. november 23-ánBudapesten írták alá a *Számítástechnikai Bűnözésről Szóló Egyezményt*,[23] ami az első jelentős európai szintű lépés volt a kiberbűnözés elleni harcban.

A politikai vezetés komoly eredményeket vár az újonnan felállított Központtól. Remélhetően a központi koordinálásban partnerek lesznek a tagállamok is, ezzel is segítve a felderítések hatékonyságát. Fontos szerep jut a magánszférának is, hiszen a magánkézben lévő IT biztonsági cégek mindig is partnerei voltak a kormányzati szerveknek a kiberbiztonság kérdésében. Mindezeken túl fontos lenne, hogy a nem kiberbiztonsággal foglalkozó magánvállalatok is felismerjék a kiberbűnözés fenyegetésének súlyát és kellőképpen vegyék figyelembe az ezzel kapcsolatos ajánlásokat, mert egy valami biztos: a Központ csak akkor lehet sikeres, hogyha az érintett államok és azok állampolgárai igyekeznek felelősségteljes és biztonságtudatos internet felhasználóvá válni.

EGYÜTTMKÖDŐ PARTNEREK

A kollektív és kooperatív biztonság garantálásának alapfeltétele, hogy az adott szövetség tagjai megfelelő garanciákkal rendelkezzenek egymás irányába, és hatékony módon tudjanak együttműködni egymással. Azonban rendkívül fontos, hogy a szervezet a saját keretein kívül is keressen partnereket, szövetségeseket. Az uniós kiberbiztonság kérdésének vizsgálatakor az egyik legkézenfekvőbb partner a NATO.

Az Európai Unió és a NATO között számos területen van együttműködés, a legfontosabb biztonságpolitikai folyamatok összehangolása már 2001-ben elindult. A katonai műveletek terén történő együttműködés 2003-ban vette kezdetét, tekintve, hogy ekkor indult az Európai Unió első, CONCORDIA elnevezésű válságkezelő missziója, ahol az uniós erők nagyban támaszkodtak a NATO támogatására.[24]

Kiberbiztonság tekintetében fontos állomás volt a 2011. november 19-én és 20-án lezajlott lisszaboni csúcstalálkozó, ahol a tagállamok elfogadták a NATO új Stratégiai Koncepcióját.[25]

[23] *Számítástechnikai bűnözésről szóló egyezmény.* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS%20185%20Hungarian.pdf Letöltés ideje: 2013. január 22.

[24] HORVÁTH Gábor: *NATO and EU: Cooperationorcompetition?*In: Academic and Applied Research in Military Science. VI. évfolyam. 2007/3. 480. o.

[25] *Aktív Szerepvállalás, Modern Védelem. Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és*

Mind a Koncepcióban, mind a csúcstalálkozó során kiemelték a NATO és az Európai Unió stratégiai együttműködésének fontosságát. Mindkét fél részéről egyezség született arról, hogy a hagyományosnak mondható együttműködéseken (terrorizmus, non-proliferáció stb.) túl, a kiberbiztonság területén is szorosabbra fűzi kapcsolatát a két szervezet.[26]

Az együttműködés fontossága a továbbiakban sem veszített súlyából, a 2012. május 20-án és 21-én lezajlott chicagói csúcstalálkozón szintén kiemelt partnerként beszéltek az Európai Unióról. Herman Van Rompuy, az Európai Tanács elnöke is részt vett a csúcstalálkozón, beszédében elmondta: az Unió továbbra is párbeszédet folytata kiberbiztonság kérdésében a NATO-val, ezzel is erősítve a térség biztonságát.[27]

Tekintve, hogy számos NATO tagállam egyben EU tagállam is, a párhuzamos kibervédelmi törekvések sok esetben gyengítik egymást, ezért is lenne szükség a folyamatos szinkronizálására. Elsősorban közös gyakorlatok megszervezése, a megszerzett tapasztalatok megosztása, illetve különböző konferenciákalkotják az együttműködés főbb pólusait. Ezt erősítette meg Iklódy Gábor is, a NATO új típusú biztonsági kihívásokkal foglalkozó főtitkár-helyettese, a Microsoft által szervezett kiberbiztonsági konferencián elmondott beszédében.[28] Hozzátette, hogy egy nagyobb támadás esetén növelné a hatékonyságot a közös fellépés, továbbá a rendszerek közös védelmét sem tartja kizártnak a jövőben.

A kiberbiztonsággal kapcsolatosegyüttműködési kérdésekben az Unió tekintetében az *Európai Hálózat- és Információbiztonsági Ügynökség, még a NATO tekintetében a Kooperatív Kibervédelmi Kiválósági Központ*[29] *a kiemelten felelős szerv.*

A Központ több ország kooperációjával jött létre: Észtország, Németország, Olaszország, Litvánia, Lettország, Szlovákia, Spanyolország voltak az alapító tagok, 2010-ben Magyarország is csatlakozott a Központhoz, 2011 novemberében pedig az Amerikai Egyesült Államok és Lengyelország vált támogató taggá.Aszervezet nem a NATO kibernetikai támadóerejét jeleníti meg, hanem mint kutatási és oktatási központ kíván működni. Kétségtelen, hogy kiváló kapcsolati pont lehet a NATO tekintetében. Továbbá figyelembe véve a már említett tagállami átfedéseket, logikus és a világgazdasági folyamatokat figyelve pedig szükségszerű lenne az együttműködés szorosabbá tétele.

Véleményem szerint a közös védelem kialakítása lenne az egyik legfontosabb és egyben az egyik legköltséghatékonyabb lépés. Tekintve, hogy mindkét szervezet azonos értékeket vall, ezért nem látom akadályát annak, hogy ilyen komoly szinteken is megvalósuljon a feladatok megosztása. A jövőben elképzelhetően ez lesz a legnagyobb feladat a két szervezet kibervédelmi együttműködésének tekintetében.

Másik kiemelt partner az Amerikai Egyesült Államok. Annak ellenére, hogy az USA tagja a NATO-nak, az Unió és Amerika között önállóan is kialakításra kerültek kiberbiztonsági kapcsolatok. Ebbe az együttműködésbe tartozik a *CyberAtlantic 2011*gyakorlat is. A hangsúly a transzatlanti együttműködésen volt, azaz azt vizsgálta, hogy egy esetleges támadás esetén az amerikai szervek hogyan tudnak segítséget nyújtani európai partnereiknek, illetve mindez fordítva hogyan valósulhat meg. A transzatlanti kiberbiztonsági kapcsolatok 2011-ben kaptak

---

*Biztonságról.*http://www.biztonsagpolitika.hu/documents/1291766875_NATO_Strat_Koncepcio_2010_hun_BSZK.pdf Letöltés ideje: 2013. február 10.

[26]*NATO-EU: a strategicpartnership*. http://www.nato.int/cps/en/natolive/topics_49217.htm Letöltés ideje: 2013. február 11.

[27]*Statement of thePresident of the European Council, Herman Van Rompuy, atthe Chicago NATO Summit.* Press release.EUCO 105/12. Chicago,20 May 2012.

[28]HALE, Julian: *NATO OfficialHighlightsAreasfor EU-NATO CyberCooperation.* http://www.defensenews.com/article/20120531/DEFREG01/305310005/NATO-Official-Highlights-Areas-EU-NATO-Cyber-Cooperation Letöltés ideje: 2013. január 25.

[29]NATO CooperativeCyberDefence Centre of Excellence (CCD CoE)

nagy lendületet, amikor létrehoztak egy közös munkacsoportot, amely alapvető informatikai biztonsági kérdésekkel, illetve a kiberbűnözéssel foglalkozik.[30]

Tény, hogy a kiberbiztonság tekintetében élen járnak az amerikaiak, tapasztalataikat pedig szívesen megosztják szövetségeseikkel. Sajnálatos módon a kártékony programokra és a különböző behatolásokra sok esetben csak reagálni lehet, kevesebb alkalommal lehet megelőzni azokat. Többek között ezért lenne fontos az együttműködést a munkacsoport szintjénél egy komolyabb dimenzióban megvalósítani.

KÖVETKEZTETÉSEK

A fent leírtak alapján elmondható, hogy az Európai Unió komolyan veszi a kiberbiztonság kérdését. Bár a fent leírt dokumentumok és szervezetek nem fedik le az összes lépést, amit az Unió tett polgárai védelmének érdekében, kétségtelenül jól példázzák az erőfeszítéseket.

Jól jelzi a folyamat dinamikáját, hogy még az előző cikkemben csupán tervként bemutatott kiberbiztonsági stratégia mára már valósággá vált: 2013. február másodikán bemutatták az Európai Unió kiberbiztonsági stratégiáját.[31]

Az új stratégia öt prioritást emel ki:

- a kibertámadásokkal szembeni ellenálló képesség megteremtése;
- a számítástechnikai bűnözés drasztikus visszaszorítása;
- a kibervédelmi politika kidolgozása és a közös biztonság- és védelempolitikát (KBVP) érintő képességek fejlesztése;
- a kiberbiztonsághoz szükséges ipari és technológiai erőforrások előteremtése;
- az Európai Unió által képviselt, a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozása, valamint az alapvető uniós értékek terjesztése.[32]

A dokumentum elemzése egy külön tanulmányt érne meg, az mindenesetre most is megállapítható, hogy rendkívül átfogó intézkedések gyűjteménye, kiemelt tekintettel a kiberbűnözés problematikájára, amely uniós tekintetben a legkomolyabb kiberbiztonsági kihívásnak számít. Továbbá a stratégia számos válaszlépést is tartalmaz a fellépő fenyegetések kezelésére. Ezen akció időtartalma azonban az esetek többségében hosszabbtávú politikai cselekvést igényel, így a stratégia helytállóságát később lehet csak lehet reálisan megítélni.

A bemutatottak alapján jól látható, hogy a jogszabályi környezet kiépítése megtörtént, 2013-ra a szükséges szervezetek is elérték a teljes műveleti képességüket. Magyarán a mostani év lesz az első éles főpróbája az európai kibervédelmnek. Az együttműködés iránti igény is jól látható, azonban véleményem szerint sok esetben szétaprózódáshoz vezethet a sokszoros átfedés. A CERT/CSIRT szervek esetén is jól látható, hogy több európai és nemzetközi fórumon kell összehangolniuk tevékenységüket, mindezeket az elsődleges nemzeti igényekhez igazítva. Véleményem szerint érdemes lenne csúcsszerveket/fórumokat létrehozni ennek érdekében, megszüntetve a számos, sok esetben párhuzamos (néha egymást kioltó) törekéveseket.

A kiberbiztonságot erősítő folyamatok azonban kétségtelenül elindultak, így remélhetjük, hogy az uniós szintű együttműködés eredményeképpen mindannyian egy biztonságosabbá váló Európa polgárai lehetünk.

---

[30]Cybersecurity: EU and US strengthentransatlanticcooperationinface of mountingglobalcyber-security and cyber-crimethreats. Press release. MEMO/11/246. Brussels, 14 April 2011.

[31]JointCommunicationtothe European Parliament, theCouncil, the European Economic and SocialCommittee and theCommittee of Regions. CybersecurityStrategy of the European Union: An Open, Safe and SecureCyberspace. 7.2.2013. JOIN(2013) 1 final.

[32]Uniós kiberbiztonsági terv a nyílt internet, valamint az online szabadság és lehetőségek védelmére. Sajtóközlemény. IP/13/94. Brüsszel, 2013. február 7.

Felhasznált irodalom

[1] *2012 Norton CybercrimeReport.* http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf Letöltés ideje: 2013. február 10.

[2] *A Bizottság megerősítené az informatikai támadásokkal szembeni védelmet Európában.* Sajtóközlemény. IP/10/1239. Brüsszel, 2010. szeptember 30.

[3] *A számítástechnikai bűnözés elleni küzdelem európai uniós központja az internetes bűnözők elleni küzdelem és az e-fogyasztók védelme érdekében.* Sajtóközlemény. IP/12/317. Brüsszel, 2012. március 28.

[4] ADLER,Freda – MUELLER, Gerhard O. W. – LAUFER, William S.:*Kriminológia.* Osiris Kiadó, Budapest, 2005. ISBN 963-389-793-9

[5] *Aktív Szerepvállalás, Modern Védelem. Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságról.*http://www.biztonsagpolitika.hu/documents/1291766875_NATO_Strat_Koncepcio_2010_hun_BSZK.pdf Letöltés ideje: 2013. február 10.

[6] *Az Európai Tanács tájékoztatása.A Stockholmi Program – A Polgárokat Szolgáló Védő, Nyitott és Biztonságos Európa.* 2010. 5. 4. (2010/C 115/01)

[7] *Az Európai Unió belső biztonsági stratégiája. Az európai biztonsági modell felé.* Luxembourg, 2010. ISBN 978-92-824-2685-2

[8] *CERT cooperation and itsfurtherfacilitationbyrelevantstakeholders.* ENISA Report. 2006. 12. 01.

[9] *Cyber Europe 2012. Főbb következtetések és ajánlások.* ENISA, 2012. december.

[10] *Cybersecurity: EU and US strengthentransatlanticcooperationinface of mountingglobalcyber-security and cyber-crimethreats.* Press release. MEMO/11/246. Brussels, 14 April 2011.

[11] *Európai Biztonsági Stratégia. Biztonságosabb Európa egy jobb világban.* Luxembourg, 2009. ISBN 978-92-824-2427-8

[12] Gragido, WILL – Pirc, JOHN: *Cybercrime and Espionage. An Analysis of SubversiveMultivectorThreats.* Elsevier, 2011. ISBN 978-1-59749-613-1

[13] HAIG Zsolt: *Az információbiztonság szabályzói és szervezeti keretei.*In: Hadmérnök. Robothadviselés 7. tudományos szakmai konferencia különszám. 2007. november 7. http://hadmernok.hu/kulonszamok/robothadviseles7/haig_rw7.pdf
Letöltés ideje: 2013. február 22.

[14] HALE, Julian: *NATO OfficialHighlightsAreasfor EU-NATO CyberCooperation.* http://www.defensenews.com/article/20120531/DEFREG01/305310005/NATO-Official-Highlights-Areas-EU-NATO-Cyber-Cooperation
Letöltés ideje: 2013. január 25.

[15] HORVÁTH Gábor: *NATO and EU: Cooperationorcompetition?*In: Academic and Applied Research in Military Science. VI. évfolyam. 2007/3. 479-489. o. ISSN 1588-8789

[16] *JointCommunicationtothe European Parliament, theCouncil, the European Economic and SocialCommittee and theCommittee of Regions. CybersecurityStrategy of the European Union: An Open, Safe and SecureCyberspace.* 7.2.2013. JOIN(2013) 1 final.

[17] *NATO-EU: a strategicpartnership*. http://www.nato.int/cps/en/natolive/topics_49217.htm Letöltés ideje: 2013. február 11.

[18] PASSERI, Paolo: *2012 CyberAttacksStatistics.*http://hackmageddon.com/2012-cyber-attacks-statistics-master-index/ Letöltés ideje: 2013. január 22.

[19] SCHREIER, Fred – WEEKES, Barbara – WINKLER, Theodor H.:*CyberSecurity: The RoadAhead.* DCAF Horizon 2015 WorkingPaperNo. 4. DCAF, 2012.

[20] *Sikeres kísérleti projekt hatására nőtt az uniós intézmények kiberbiztonsága.* Sajtóközlemény. IP/12/949. Brüsszel, 2012. szeptember 12.

[21] *Statement of thePresident of the European Council, Herman Van Rompuy, atthe Chicago NATO Summit.* Press release.EUCO 105/12. Chicago,20 May 2012.

[22] *Számítástechnikai bűnözésről szóló egyezmény.* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS%20185%20Hungarian.pdf Letöltés ideje: 2013. január 22.

[23] SZEGEDINÉ LENGYEL Piroska: *Számítógépes bűnözés avagy fiatalok a cyber-térben.*In: Hadmérnök. V. évfolyam. 2012/2. 366-379. o. ISSN 1788-1919

[24] *The EU InternalSecurityStrategyin Action: Fivestepstowards a more secure Europe.* Press release. MEMO/10/598. Brussels, 22 November 2010.

[25] TÓTH Tamás: *Az Europol tevékenysége II. (2010-2012).* http://www.biztonsagpolitika.hu/?id=16&aid=1264&title=az-europol-tevekenysege-ii-2010-2012- Letöltés ideje: 2013. február 11. ISSN 2062-4379

[26] *Uniós kiberbiztonsági terv a nyílt internet, valamint az online szabadság és lehetőségek védelmére.* Sajtóközlemény. IP/13/94. Brüsszel, 2013. február 7.

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Antal Örs
antal.ors@gmail.com

A FÖLDRENGÉSÁLLÓ ÉPÍTKEZÉS KORSZERŰ LEHETŐSÉGEI

Absztrakt

Haiti, Szecsuán, L'Aquila, Törökország; elég csak néhány esetet felsorolni az elmúlt évek súlyos földrengései közül, aminek következtében a felbecsülhetetlen anyagi károk mellett tízezrek vesztették életüket és százezrek váltak hajléktalanná. A földrengés megelőzésére és elkerülésére nincsen mód, azonban ismét bebizonyosodott, hogy a veszteségek a megfelelő építési technológia alkalmazásával minimalizálhatóak lehettek volna, a Japán mintát követve. Hazánk nem tartozik a magas földregés veszélyeztetettséggel bíró országok közé, azonban a régi, elavult technológiával épült épületek magas száma miatt egy kisebb erejű rengés is jelentős kockázatot jelenthet a jövőre való tekintettel. Jelen tanulmány bemutatja a földrengésálló építkezés főbb szempontjait, valamint a világszerte elterjedt és hatékonynak bizonyul technológiai megoldásokat. Emellett vizsgálja, hogy az uniós szabályozás tükrében milyen tendenciák mutatkoznak az európai, így a hazai földrengésbiztonsági építkezés tekintetében is.

Haiti, Sechuan, L'Aquila and Turkey are examples for devastating earthquakes from the recent years causing ten thousands of deaths and hundred thousands of homelesses besides the inestimable property damages. No applicable method exists to prevent or avoid the earthquakes, neverthelles it had been proved again that the losses could had been minimized with the suitable earthquake-resistant building technology, following the Japanese pattern.Our country does not belong to the significantly earthquake-endangered countries, however due to the high number of bulildings contstructed by old and traditional technology a smaller earthquake could cause high risk in the future, too. This study represents the most important aspects of earthquake-resistant building methods and the world-wide technologies that proved to be efficient. Furthermore it investigates the future european tendencies in point of the domestic and international earthquake-resistant building technologies.

Kulcsszavak: *horizontális erő, rengéshullámok, Japán, rugalmasság, méretezés ~ horizontal force, seismic waves, Japan, flexibility, sizing*

BEVEZETÉS

A legpusztítóbb, évente százezres nagyságrendben mérhető haláleseteket okozó természeti katasztrófák a földrengések, amelyek ellen - a magas technológiai fejlettség ellenére - a mai napig nem létezik hatékony előrejelzési módszer, emellett a rengések megelőzésére nincs mód, csak a pusztító hatás csökkentésére. Ennek kulcsa a földrengésálló építészeti technológia, ami szerves részét képezi a védelmi képességek növelésére, valamint a megelőzésre irányuló tevékenységeknek. Az építészeti eljárások jelentőségét jól alátámasztja Japán, amely földünk szeizmikusan legaktívabb zónájában helyezkedik el, mégis az elmúlt évek jelentős földrengései alig tettek kárt a szigetország építményeinek szerkezeteiben. A tanulmány során részletesen bemutatásra kerülnek ezen építészeti technológiák, kiemelten foglalkozva a könnyű acélszerkezetes megoldás jelentőségével. A technológia háttér tisztázása mellett vizsgálom ennek szabályozási hátterét, ami alapvetően meghatározza az európai földrengésbiztonsági építkezési tendenciákat is a jövőre való tekintettel. Fontos továbbá tisztázni, hogy melyek azok a legfontosabb szempontok és eljárások, amelyeket a tervezésnél figyelembe kell venni. Az olykor merésznek tűnő, ugyanakkor hatékony technológiai eljárásoknak köszönhetően az elmúlt évtizedekhez képest áttörés történt a földrengésálló építkezés terén, amit a növekvő urbanizáció kiemelten szükségessé tett.

A FÖLDRENGÉSEK KÖZVETLEN HATÁSAI AZ ÉPÍTMÉNYEKRE

Az épületek tervezésénél általában fő szempont a vertikális terhek elleni ellenálló képesség, így az előírásoknak megfelelően megépített építmények saját súlyuk mellett a beltéri és a csapadékból adódó esetleges külső terheknek is biztosan ellenállnak. A földrengések esetén a problémát azonban a rengéshullámokból eredő és épületszerkezetekre ható oldalirányú talajmozgás okozza. A hirtelen fellépő horizontális terhelés következménye legtöbb esetben az épület összeomlása, totális pusztítást okozva. A földrengéshullámok gyakori jellemzője - főként a puhább talajrétegek esetén - hogy több hullámban érkeznek, ami a masszívabb, ellenállóbb épületszerkezetek tartószerkezetinek teherbíró képességét is még intenzívebben redukálja.

Az elsődleges veszélyt tehát a földrengéshullámok vízszintes irányú gyorsulása okozza, mivel a teherhordó szerkezetekben nyírófeszültségeket hoznak létre, ami sok esetben az épületszerkezeteket nem lehet megfelelően méretezni. A másik, közvetlen károsodást kiváltó fizikai tényező a rezgés frekvenciája, amelyek általában 0 és 15 Hz közé tehetőek. Az épület akkor van kitéve a legnagyobb terhelésnek, ha a maximális rengés frekvencia megegyezik az épületek sajátfrekvenciájával, mivel ilyenkor rezonancia generálódik, ami nagy rezgés amplitúdót eredményez. [1]

Számos esetben fordult már elő, hogy az épület összeomlását a földrengéshullámok mellett az épületre ható túlterheltség okozta, (utólag beépített emelettel, elválasztó falakkal, körbe épített teraszokkal, belső raktározással stb.). Ez a probléma sokszor a földrengésálló épületek összedőléséhez is közvetlenül hozzájárul, mivel a plusz terhek meghaladták az épületszerkezet méretezéséből adott határokat. Bizonyított tény, hogy a túlterhelt épületszerkezetek jelentő mértékben sebezhetőbbek földrengésekkor, sok esetben az épület összedőlését egy kisebb, ugyanakkor az előzőekhez képest más irányból érkező utórengés, vagy a rezgések frekvenciájának változása okozza.

Az eddigi bekövetkezett földrengéskárok tapasztalati alapján az épületek gyors, „kártyavárszerű” összeomlásának további oka lehet, hogy az alsóbb szinteket magasabb belmagassággal és kevesebb teherhordó fallal, vagy oszloppal tervezték, amelyek a földrengéshullámok érkezésekor elsőként vesztik el teherhordó funkciójukat az egész épület teljes pusztulását következményezve. Emellett, rendkívül fontos a talaj keménység és az

alapozás helyes megválasztása is, mivel főként magasabb, több emeletes tömbházaknál jelentkezhet, hogy a puhább talaj futóhomokszerűen képes porladni a rezgések hatására.

Az épületek szerkezeti hiányosságai mellett a földrengéskárok általános oka az építőanyagok nem megfelelő megválasztása is. Hogy csak két releváns példát említsek, 2008-ban, a nyugat-kínai Szecsuan tartományban kipattanó, valamint a 2009-es észak-olaszországi L'Aquila városában pusztító földrengés által okozott jelentős épületkárok oka az előírásoknak nem megfelelő konstrukciók és anyagok használata volt. A mentésben résztvevő tűzoltók elmondásai szerint, olyan teherhordó szerkezetek zúzódtak porrá a földrengést követően, amelyek eltávolítására általában fűrészt vagy más speciális vágószerszámot kellett használjanak. Ebből arra lehetett következtetni, hogy sok építkezésnél - költségmegtakarítás céljából - a betonelemeket a cement magas ára miatt homokkal pótoltak ki, amik a rezgések hatására rövid időn belül szétporladtak.

A földrengésálló, rugalmas tulajdonságú építőanyagok használatának kulcsfontosságát már évszázadok óta ismerik a különösen veszélyeztetett térségekben élők, a következőben ezek részletes bemutatására is sor kerül.

A FÖLDRENGÉSÁLLÓ ÉPÍTKEZÉS MÚLTJA

Ahogyan az előbbiekben említettem, egyes területeken már évszázadok óta fontos szempontként kezelik a földrengés ellenálló képességet az építkezések során. Földünk szeizmikusan legaktívabb térségében, a Csendes-óceán partjainál szélesen, sávszerűen húzódó cirkumpacifikus övezetben található Fülöp-szigeteken már a XV. századtól tudatosan építkeztek a földrengésekre készülve. A helyiek által *„bahay-na-nipa"*-nak vagy *„bahay kubo"*-nak nevezett, többnyire egy légterű bambuszból épült és nádtetővel fedett kunyhók jelesre vizsgáztak az igen intenzív, 7-8-as magnitúdójú földrengések esetén is. A kunyhók tetejét egy fából épített dúcszerkezet a bambuszból készült könnyű falaktól függetlenül tartotta, ami ily módon megfelelő rugalmasságot és ingást tett lehetővé a földrengéseknek ellenállóvá téve az építményt. Később, a nagyobb településeken ugyanezt az elvet követve már masszívabb fagerendákból épített és cseréptetővel fedett házakat kezdtek a szigeteken élők építeni, ami kiszélesítette azok kihasználásának és funkcionális lehetőségeit.

A helyi építési kultúra fejlődésének, és az idegen telepeseknek is köszönhetően a városokban a nipa-kat fokozatosan felváltották a több szintes kőből és téglából épített „*bahay-na-batok"*, *(1. ábra)* amelyeknek - elődeik szerkezetén alapulva - masszívabb és merevebb szerkezetű kőfalai egy rugalmas faszerkezet beépítésével el voltak választva a tetőtől, így biztosítva azt, hogy a rezgéshullámok hatására ne omoljanak össze. A *„batok"* a mai napig biztonságos otthonként szolgálnak a Fülöp-szigeteken élők számára. [2]

1. ábra. „Bahay-na-bato" lakóház modern változata a Fülöp-szigeteken Forrás: http://www.bokkins3d.blogspot.hu/2008/03/bahay-na-bato.html Letöltés ideje: 2012.08.14.

KORSZERŰ FÖLDRENGÉSÁLLÓ ÉPÍTÉSI TECHNOLÓGIÁK

A földrengésálló építkezés alapja az építőanyagok megfelelő megválasztása. Az intenzív rezgéshullámoknak a rugalmas anyagok - mint a fa és az acél - ellenállnak, a tégla és a beton viszont egyáltalán nem biztosít megfelelő rugalmasságot, ami az esetek többségében épületszerkezet összeomlását eredményezi. Ismét felhozható példának az észak-olaszországi L'Aquilában pusztító, 6,3-as magnitúdójú - nem kivételesen nagymértékű energia felszabadulással járó - földrengés, amelynek következtében csaknem 70.000 ember vált hajléktalanná. A magas kár fő oka a sok merev építőanyagból készült lakóház és műemlék épület volt *(2. ábra)*, az újraépítés során már könnyűszerkezetes épületeket építettek. *[3]* A közép- és kelet-európai térségben, így hazánkban is jelentős a tégla és betonépítésű lakóházak aránya, míg a világ más tájain a könnyű acélszerkezetes építmények száma rohamosan terjed, szem előtt tartva a földrengések általi veszélyeztetettség mértékét, valamint az erre vonatkozó nemzetközi irányelveket és szabályozásokat.

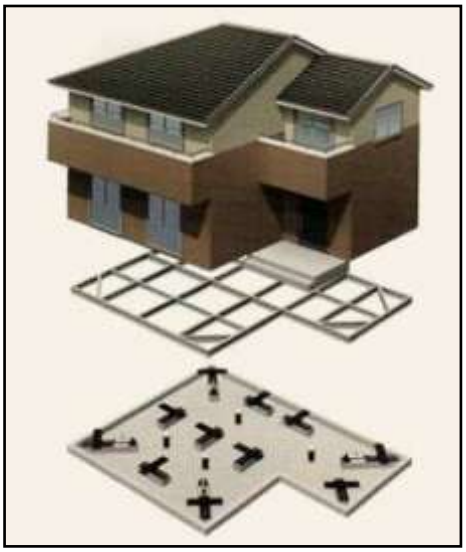
2. ábra. Santa Maria Suffragio templom romjai a 2009-es l'aquilai földrengést követően
Forrás: http://www.i-italy.org/bloggers/8564/invisible-victims-abruzzo-earthquake
Letöltés ideje: 2012.08.14. (Készítette: Samuele Pellecchia)

Hogy említsünk pozitív példát is, az építési technológia fontosságát kiválóan demonstrálja a 2011. március 11-i, 9-es magnitúdójú japán földrengés, ahol a megfelelő építési technológiának köszönhetően az épületek szerkezetében csak a legritkább esetben keletkezett komoly kár. Az, hogy ennek ellenére óriási pusztítást szenvedett el a „felkelő nap országa", a földrengés másodlagos hatásaként jelentkező szökőárnak volt köszönhető, ami ellen nem létezik technológiai eljárás.

A következő kép *(3. ábra)* egy klasszikus japán földrengésre tervezett lakóházat szemléltet. A biztonság és statikai tulajdonságok mellet a formatervezés is hangsúlyt kap az esetek többségében.

3. ábra. Földregésálló könnyűszerkezetes lakóház Japánban
Forrás: http://kp.hu/mibol-epitkeznek-a-japanok-mitol-foldrengesbiztos-egy-haz/
Letöltés ideje: 2012.08.12.

A védekezést tekintve két földrengésálló technológiai megoldás ismert, amely alapján létezik a rezgésálló megoldással épített ház, amikor az építménybe rugalmas teherbíró szerkezetek kerülnek beépítésre, valamint a földrengés szigetelés *(4. ábra),* mely esetben a talapzatba beépített acélszerkezet biztosítja a szeizmikus energia elnyelését. A különböző konstrukciós megoldásoknál fő szempont, hogy a talapzatot és az alapozást nem szabad egybeépíteni, mivel így megelőzhető, hogy a rezgések direkt átadódjanak a ház szerkezetére. A hatékonyság fokozása érdekében a két eljárás kombinálása is adott, mint lehetőség. A világon elterjedt védekezési építési megoldás, a könnyű acélszerkezetes technológia részletes bemutatására a következő fejezetben kerül sor. *[3]*

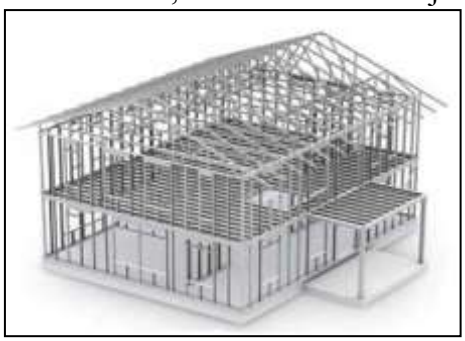


4. ábra. Földrengésálló szigetelés
Forrás: http://kp.hu/mibol-epitkeznek-a-japanok-mitol-foldrengesbiztos-egy-haz/
Letöltés ideje: 2012.08.14.

A könnyű acélszerkezetes technológia, mint a földrengéskárok elleni védekezés első számú lehetősége

Az eddigiekben tárgyaltak alapján megerősíthető, hogy az egetlen korszerű építőanyag a földrengésálló épületek létrehozására az acél. Az acélszerkezet jellemzője, hogy még a fánál is könnyűszerkezetesebb, ami annyit jelent, hogy egy azonos statikai mutatókkal rendelkező acélgerenda jóval kisebb súlyú (kb. 1/7), mintha fából készült volna.

Felépítésüket tekintve az acélszerkezetes épületek *(5. ábra)* falai vázszerkezetből állnak össze, amely közé hőszigetelő anyagok kerülnek beépítésre. Értelemszerűen a hőszigetelő anyagok szerepe a hőátbocsátás csökkentése, míg a hidegen hengerelt vékonyfalú acél U és C profilokból szerelt vázszerkezetnek statikai, teherhordó funkciója van. [4.]



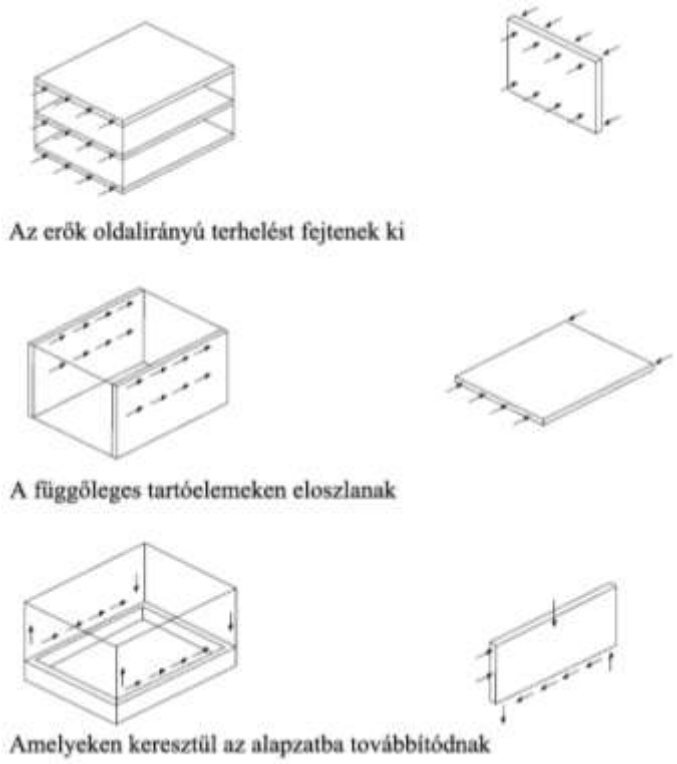
5. ábra. Acélszerkezetes épület szerkezeti rajza
Forrás: http://samarasbau.hu/wp-content/uploads/2012/01/acelszerkezetes-haz.jpg
Letöltés ideje: 2012.08.14. Készítette: nincs megnevezve

A könnyű acélszerkezetes házak száma ma már meghaladja a hagyományos építőanyagokból készül házakét a világon, mivel földrengés ellenállóságuk mellett számos más előnnyel rendelkeznek: [1]

- az acélszerkezet profiljainak gyártása során nem keletkezik hulladék,
- az egyes elemeket nem kell vegyszerrel kezelni (szemben a faszerkezettel),
- a szerkezet nem vetemedik a hőmérséklet és az öregedés hatására,
- az elemek nagy méretpontossággal gyárthatóak,
- környezetbarát megoldás, mivel nem kell fákat kivágni, alapanyaga újrahasznosítható,
- az acélszerkezet nem tűzveszélyes, valamint a bogarak és kártevők nem tudják károsítani.
- a szerkezetek könnyű súlya miatt egyszerűbb és olcsóbb a szállíthatóságuk.

A földrengésálló acélszerkezetes épületek jellemzői

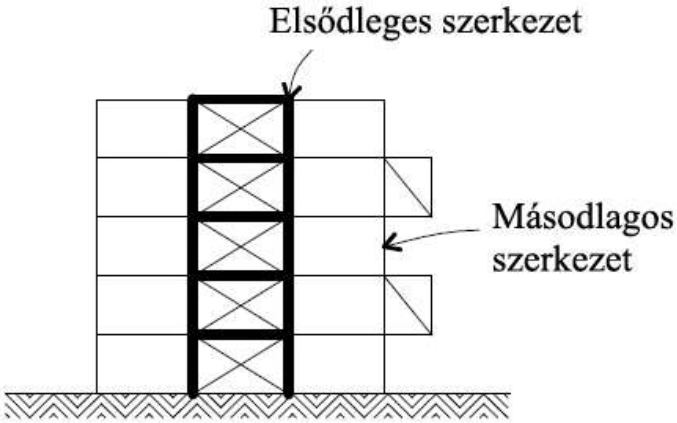
A könnyű acélszerkezetes építmények esetén a merev és ellenálló vízszintes épületelemek lehetővé teszik minden emeleten, hogy a horizontálisan ható erők szétszóródjanak a merőlegesen kapcsolódó függőleges szerkezeti elemeken, illetve válaszfalakon. A függőleges épületszerkezetek az így érkező erőhatásokat (pl. nagy erejű rezgéseket) az alapzatba továbbítják, a következő ábrán vázolt módon. [5]



Elsődleges-másodlagos szerkezetek

A védekezőképesség fokozása érdekében a függőleges acél tartóelemekbe beépítésre kerülhet egy ún. „elsődleges szerkezet”, melynek fő funkciója az összes földrengés terhelés elvezetése, és egy „másodlagos szerkezet”, amely csak a nehézségi erőkből származó terhek viselésére van tervezve. A másodlagos váz hosszanti ellenálló képessége és merevsége nem haladhatja meg az elsődleges szerkezet 15%-át, emellett a tervezésnél figyelmet kell fordítani a másodlagos szerkezet elsődlegeshez való csatlakozásainak illeszkedésére, a

földrengéshullámok okozta eltolódások esetén. Az említett szerkezeti felépítést az alábbi ábra *(6. ábra)* illusztrálja. [5]



6. ábra. Acélszerkezetes épület szerkezeti rajza
Forrás: http://www.arcelormittal.com/sections/fileadmin/redaction/4-Library/1-Sales_programme_Brochures/Earthquake/Earthquake_EN.pdf Letöltés ideje: 2012.08.14.

Az alapzatnak biztosítania kell, hogy földrengés esetén, a talajból érkező rezgéshullámok az épület egészén egyenletesen oszlódjanak el. Másik funkciójuk, hogy a talaj süllyedése esetén is megfelelő tartást biztosítson az épületnek, ami egyaránt elérhető sík- és mélyalapozással is. Cölöpök vagy lábazat beépítése esetén fontos, hogy a stabilitás érdekében a cölöpök kötőgerendákkal, vagy lemez alappal egymáshoz legyenek rögzítve.

Toronyházak földrengésvédelme

A lakóházak, felhőkarcolók, hidak és vasúti pályák földrengésálló építészeti megoldásainak alkalmazásában Japán világelsőnek számít, ami szoros összefüggésben van a szigetország magas veszélyeztetettségével és technológiai fejlettségével. Az egyszerű lakóházak földrengésekre való méretezését viszonylag egyszerűbb előírások szabályozzák, a 60 méternél magasabb építmények esetén már jóval bonyolultabb ellenőrzési folyamatok és számítógépes szimulációk alkalmazása szükséges, ami lehetővé teszi a több száz méter magasságú és extrém formájú felhőkarcolók földrengés állósági modellezését is. Az építmények méretezésénél egyaránt figyelembe kell venni a gyakoribb vízszintes és kevésbé gyakori függőleges szeizmikus hullámok általi terhelést is.

Földrengésálló tartószerkezetek magasépítésnél

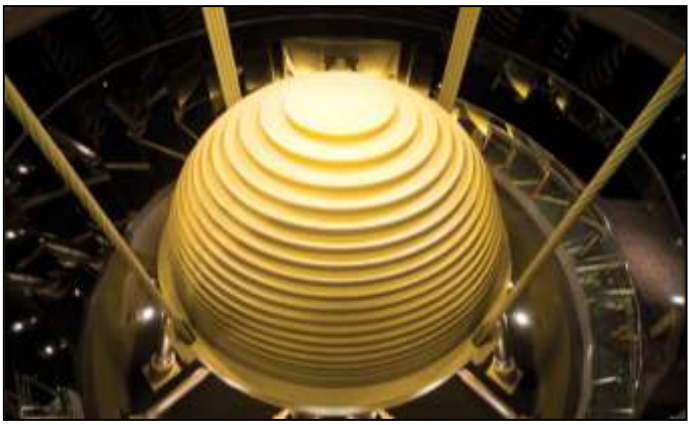
A kis elmozdulást lehetővé tevő merev vasbeton szerkezetekkel szemben a korszerű magasházak a már tárgyalt könnyű acélszerkezetes technológiával, szeizmikus csillapítóelemek beépítésével épülnek nem csak Japánban, hanem szerte a világban. A csillapító elemeknek hála, a rezgések elnyelődnek a szerkezeti elemek nagyobb elmozdulása mellett. Ezzel magyarázható az a jelenség, amikor egy intenzívebb földmozgás eredményeképpen a magas épület akár több méter kilengés mellett is biztosan ellenáll a rengéseknek, valamint az épületben jóval kisebb rezgés érzékelhető az elnyelődésnek köszönhetően.

A rengés-csillapítás elérése érdekében bevált technológiai eljárás a csillapító-falak beépítése az egyes szintek közé. Erre például szolgál a Tokióban található Roppongi Hills felhőkarcoló.

A csillapító elemeknél hatékonyabb, ugyanakkor költségesebb megoldás a szeizmikus szigetelők használata, ami nem befolyásolja az alaprajzi és homlokzati tervezést. Az alaptól a falszerkezeteket elválasztják, vagy az épület magasságát megosztják legalább egy köztes szinttel, ami lehetővé teszi, hogy földrengés esetén az épület egyes részei egymástól

függetlenül mozogjanak. Ezen eljárás a toronyházak mellett kiemelten fontos rendeltetésű épületeknél is alkalmazzák a biztonság fokozása érdekében. Ilyen szeizmikus szigetelők kerültek alkalmazásra például a Shiodome Sumitomo bankház épületénél, ugyancsak Japánban.

A földrengésvédelemre felsorolt főbb technológiák mellett léteznek alternatív, azonban költséghatékonynak nem nevezhető megoldások is. Példának okáért a Taiwanon található Taipei 101 nevezetű, 106 szintes felhőkarcoló stabilitását egy csaknem 730 tonnás inga (7. ábra) biztosítja, ami kiegyenlíti és csillapítja a földrengések okozta kilengéseket és rezgéseket. Az épület tetejébe beépített hatalmas „acélgolyó” mindig a kilengéssel ellentétes oldalra mozdulva minimalizálja az elmozdulást. [6]



7. ábra. A Taipei 101 toronyház kilengés csillapító ingája Forrás: http://mathspig.wordpress.com/category/popular-posts/cool-formula-for-calculating-skyskraper-sway/ Letöltés ideje: 2012.08.14.

A földrengések elleni építészeti megoldások tisztázásnál említésre került az alapozás jelentősége, ami a magas építésű épületekre is elmondható. Az acélszerkezetes toronyházak, középmagas épületek és hídszerkezetek építésénél világszerte alkalmazott ún. „földrengés-szigetelő pogácsák”, azaz lengéscsillapítók feltalálása Tarics Sándor (olimpiai bajnok vízilabdázó, építészmérnök professzor) nevéhez fűződik, aki nem mellesleg a világ jelenleg élő legidősebb olimpiai bajnokának mondhatja magát. A tarics-féle pogácsák energia-elnyelő hatása jóval hatékonyabbnak bizonyult, mint az ugyancsak az alapzatban épített bármelyik másik rugós, vagy gumis megoldás. Többek között ez a konstrukció biztosítja a San Franciscóban található Golden Gate-re felvezető autópályákat és felüljárókat, valamint hazánkban Paksi Atomerőmű kiemelten veszélyeztetett építményeit is. [7]

A továbbiakban nézzük, hogy milyen egységes szabványrendszer szabályozza az Európában, így hazánkban is épülő építmények földrengés állósági méretezési és tervezési szempontjait.

A Eurocode 8

A Eurocode 8 (MSZ EN 1998) egy olyan Európai Uniós szabványcsomag, melynek alapelve, hogy az adott épület típust olyan földrengésre kell tervezni, ami 50 év leforgása alatt 10%-os valószínűséggel fordulhat elő. A teherbírási követelmények alapján az építmény nem dőlhet össze a rengéstől, egyes épületeknek pedig a károsodási mértéke is meg van határozva. Ez esetben az épületszerkezet nem amortizálódhat jelentősen egy olyan földmozgás esetében, amelynek előfordulási lehetősége 10 év leforgása alatt 10%. A szabványcsomag három fő célja a következő: [8]

- az emberi életek megóvása,
- a károk mértékének csökkentése,
- és a kiemelt fontossággal rendelkező építmények funkciójának védelme.

Az Eurocode 8 hazánkban 2009. január 1. óta van érvényben, felépítését tekintve az alábbi szabványokból épül fel: [9]

- EN 1998-1 - magasépítési szerkezetek
- EN 1998-2 - hídszerkezetek
- EN 1998-3 - kárfelmérés és helyreállítás
- EN 1998-4 - silók, tartályok és csővezetékek
- EN 1998-5 - alapok, támaszszerkezetek
- EN 1998-6 - tornyok, kémények

Épületszerkezetek földrengésekre való méretezése

Az eddigiek alapján megállapítható, hogy az egyes épületek földrengésbiztos építése a helyes anyag és módszer megválasztásán, valamint a szerkezet megfelelő méretezésén múlik. Utóbbi részletes ismertetésére a következő pontokban kerül sor.

A tervezési válaszspektrum

A Eurocode 8 alapján a földrengésálló szerkezetek tervezésének alapja a tervezési válaszspektrum, amely egy adott frekvencián várható szeizmikus aktivitás hatását a frekvencia függvényében adja meg. A válaszspektrum meghatározása 4 lépésből tevődik össze: [9]

1. az építési terület szeizmikus zóna besorolásának meghatározása (pl. a szeizmikus zónatérképről) *(1. melléklet)*
2. a talaj típusának és talajmechanikai jellemzőinek meghatározása (A,B,C,D,E, S1,S2) *(2. melléklet)*
3. szeizmikus együtthatók meghatározása
4. válaszspektrum kiértékelése és grafikonos ábrázolása

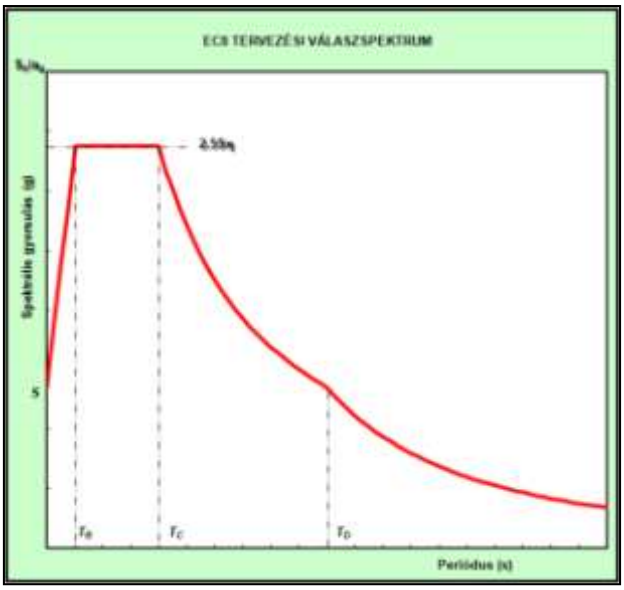
A tervezési válaszspektrum az épületszerkezet valós válaszait, illetve gyorsulásait megadó diagram, amely alapján az alábbi képlet segítségével meghatározható a földrengési teher nagyságának felső értéke a szerkezet tömegének és a válaszspektrum megfelelő értékének szorzatából:

$$Fb=mxSd(T1)$$ (tömeg x gyorsulás=erő)

ahol:

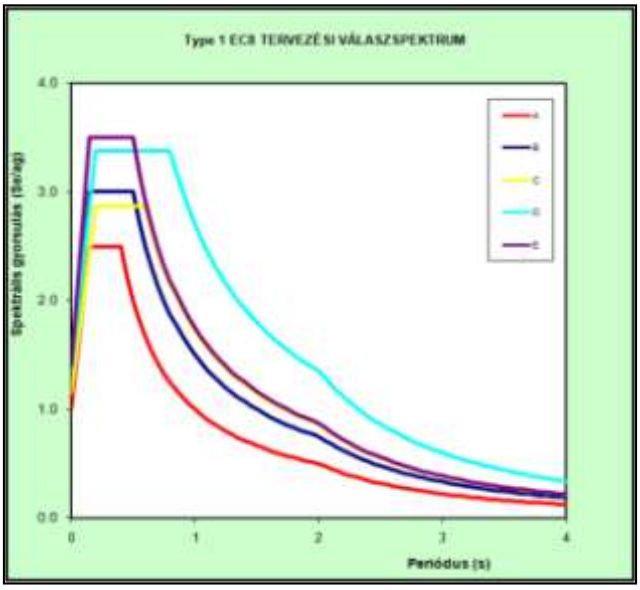
m: tömeg
Sd: válaszspektrum
T1- alaprezgési periódusidő (vízszintes mozgás esetén)

A kiértékelésnél a válaszspektrum függőleges és vízszintes összetevőjét is meg kell határozni, mivel földrengéskor a gyorsulásnak vertikális és horizontális (általában ez a pusztítóbb) komponense is van. Ez alapján az MSZ EN-1998-1 (Eurocode 8) vízszintes tervezési válaszspektrumát az alábbi diagramból *(1. diagram)* lehet kiszámítani a spektrális gyorsulás és periódus függvényében. [1]



1. diagram. Az Eurocode 8 vízszintes tervezési válaszspektruma Forrás: http://www.foldrenges.hu/index.php?option=com_content&view=article&id=94:magyarorszag-foeldrenges-veszelyeztetettsege&catid=5:geofizika&Itemid=7 Letöltés ideje: 2012.08.14.

A fenti diagramnak megfelelően az A, B, C, D, E talajtípusok esetén a tervezési válaszspektrum a következő ábra *(2. diagram)* szerint alakul.



2. diagram. Az Eurocode 8 vízszintes tervezési válaszspektruma Forrás: http://www.foldrenges.hu/index.php?option=com_content&view=article&id=94:magyarorszag-foeldrenges-veszelyeztetettsege&catid=5:geofizika&Itemid=7 Letöltés ideje: 2012.08.14.

A válaszspektrum függőleges komponensét a diagram alapján a következő lépésekben, az értékek behelyettesítésével lehet meghatározni:

$$0 \le T \le T_B : S_{ve}(T) = a_{vg}.\left[1 + \frac{T}{T_B}(\eta.3{,}0 - 1)\right]$$

$$T_B \le T \le T_C : S_{ve}(T) = a_{vg}.\eta.3{,}0$$

$$T_C \le T \le T_D : S_{(ve)}(T) = a_{vg}.\eta.3{,}0.\left[\frac{T_C}{T}\right]$$

$$T_D \le T \le 4s : S_{ve}(T) = a_{vg}.\eta.3{,}0.\left[\frac{T_C.T_D}{T^2}\right]$$

Ahol az MSZ EN-1998-1-ben meghatározott 1. típusú spektrum esetén:

$a_{vg}/a_g = 0{,}9$

T_B (s) = *0,05*

T_C (s) = *0,15*

T_D (s) = *1,0*

MAGYAR VONATKOZÁSOK

Hazánk földrajzi elhelyezkedése a természeti katasztrófák szempontjából szerencsésnek mondható, mivel a jelentős törésvonalak nagy távolsága miatt nem kell számolni gyakori, nagy intenzitású földrengéssel. Azonban, az elmúlt évtizedek során, az országban néhány esetben akár 5-6 magnitúdójú rengés is tapasztalható volt. Ezen földmozgások előfordulása teljesen rendszertelen területi eloszlásban következik be, egyes régiókban folyamatosan erősebb szeizmikus intenzitás mérhető. Ilyen például Komárom, Dunaharaszti, Mór és Eger térsége, amit a mellékelt szeizmikus zónatérkép *(1. melléklet)* jelöl. Az alacsony gyakoriságú előfordulással szemben a várható pusztítás mértéke miatt a kockázat azonban így is jelentős mértékű. Ezt tovább fokozza, hogy az ország területét nagyrészt laza üledékes kőzetek borítják, amelyek könnyedén átengedik, illetve felerősítik az - épületkárokért legnagyobb mértékben felelős - alacsony frekvenciájú rezgés hullámokat. Az üledékes talaj mellett, az országban jelentős mennyiségben épített merev épületszerkezetek (tégla- és betonépítésű lakóházak, egyéb építmények) azok, amik a földrengéskockázatot tovább fokozzák. A tapasztalatok alapján a vasbeton szerkezet, illetve a doboz szerű forma miatt egyes épületek ugyan jobban ellenállnak a rengéseknek, mint a téglából készült épületek, azonban a biztonságos szint eléréséhez nem elégséges módon, amit alátámaszt az 1977-es romániai, Richter-skála[1] szerinti 7,2-es erősségű földrengés, aminek következtében rengeteg panelépítésű vasbetonház omlott össze. A Eurocode 8-nak köszönhetően az elmúlt néhány évben már jelentős mértékben előtérbe kerültek a földrengés biztonsági szempontok az épületek tervezése során, azonban főként az ország nagyvárosaiban nagy számban található, régi, akár 100-150 éves életkort is meghaladó polgári épületek veszélyeztetettsége kritikus. Az MTA Geodéziai és Geofizikai Kutató Intézet kutatóinak álláspontja szerint, amennyiben Budapestet egy Richter-skála szerinti 7-e erősségű földrengés érné, a zsúfolt, sűrűn beépített belső kerületek esetén a károk felbecsülhetetlen mértékűnek prognosztizálhatóak. A többségében a 100 éves életkort is meghaladó bérházak nagy része minden bizonnyal a földdel válna egyenlővé egyrészt az elavult, merev építési technológia, másrészt az évtizedek során a válaszfalak sokszori átrendezése miatt, ami az épület statikai teherbíró képességét csökkenti. Sok régi templom is várhatóan összeomlana, viszont köszönhetően annak, hogy a parlament kupoláit könnyű acélszerkezet tartja, képes az intenzívebb földrengéseknek is

[1] Richter-skála: A földrengések energiájának a pontos megállapítására bevezetett skála, mértékegysége a magnitúdó (M) *[10]*

ellenállni. A kutatók véleménye alapján emellett jelentős károkat szenvedne a főváros közműhálózata is, mivel az öntöttvas víznyomócsövek és elöregedett gázcsövek rövid ideig tudnának csak ellenállni a földrengéshullámok okozta terhelésnek. [11]

Saját véleményem szerint az óriási károk bekövetkezéséhez nem szükséges 7-es magnitúdójú rengés, egy intenzívebb, 5-6-os erősségű csapás - aminek előfordulása reális veszély lehet az elkövetkezendő évtizedekben, vagy akár évek ben is - hatására is rengeteg épület szenvedne jelentős pusztítást, és minden bizonnyal a halálesetek száma is kirívóan magas lenne. Az ország jelenlegi gazdasági helyzetét és a költségvetési korlátait is figyelembe véve egyre aktuálisabb lenne egy olyan átfogó terv, illetve koncepció elkészítése, amelyben amellett, hogy megfogalmazódik az, hogy hogyan lehetne költséghatékony módon Budapest belvárosának földrengésbiztonságát növelni az előfordulás várható kockázatán alapulva, olyan építészeti tendenciát irányozna elő, ami a jövőre való tekintettel országos szinten. jelentősen hozzájárulna a földrengéskockázatok csökkentéséhez. A koncepció alapjául szolgálhat az EUROCODE 8 szabványcsomag, a könnyű acélszerkezetes építészeti megoldások, valamint a nemzetközi tapasztalatok.

ÖSSZEGZÉS

Az eddigi földrengés katasztrófák tapasztalati alapján bebizonyosodott, hogy a védekezés leghatékonyabb módja az építészeti technológiában rejlik, amelyre vonatkozóan fő szempontként említhető az építőanyag megfelelő megválasztása és a szerkezeti felépítés. A biztonsági szempontok mellett, a különböző fejlettségű országok lehetőségeit is figyelembe véve szem előtt kell tartani a költséghatékonyságot is, ezért az Európai Uniós szabályozás irányelvei alapján is a földrengésálló építkezésnek és tervezésnek célszerűen összhangban kell lennie a veszélyeztetettség mértékével, amit földtani és statisztikai mérésekkel és adatokkal lehet meghatározni. Mivel bizonyítást nyert, hogy a tégla- és betonépítésű lakóházak vesztik el teherbírásukat leghamarabb és dőlnek össze földrengés esetén, célszerű az építkezéseknél a rugalmasabb anyagok, mint az acél vagy akár a fa használata. Japánban is - amely etalonnak számít a földrengések elleni építészeti fejlesztések terén - a lakóházak többsége acél könnyűszerkezetes megoldással épült.

Magyarország földrengés veszélyeztetettsége nem indokolja a jelenlegi építészeti irányzatok gyökeres megváltoztatását, azonban a pusztítás várhatóan nagy mértéke miatt jelentős kockázattal kell így is számolni, ami egyértelműen szükségessé teszi a régi épületeink földrengésbiztonsági szempontból való felülvizsgálatát, illetve korszerűsítését a kritikus infrastruktúrákkal egyetemben.

Felhasznált Irodalom

[1] Földrengés hatása épületekre, HUN-Reng Magyarország Földrengés Információs Rendszere
http://www.foldrenges.hu/index.php?option=com_content&view=article&id=20:foeldrengesek-hatasa-epueletekre&catid=1:altalanos-fogalmak&Itemid=23
Letöltés: 2012.08.12.

[2] Augosto F. Villalon: Are heritage buildings earthquake-proof? Philippine Daily Inquirer, 2011.03.28.
http://lifestyle.inquirer.net/artsandbooks/artsandbooks/view/20110328-327971/Are-heritage--buildings--earthquake-proof *Letöltés: 2012.08.12.*

[3] Miből építkeznek a Japánok? Mitől földrengésbiztos egy ház? Készház portál, 2011.03.13. http://kp.hu/mibol-epitkeznek-a-japanok-mitol-foldrengesbiztos-egy-haz/
Letöltés: 2012.08.12.

[4] Acélszerkezetes készházak, Samarasbau építéstechnológia
http://samarasbau.hu/acelszerkezetes-keszhazak/ *Letöltés: 2012.08.12.*

[5] Earthquake Resistant steel structures, ArcelorMittal
http://www.arcelormittal.com/sections/fileadmin/redaction/4-Library/1-Sales_programme_Brochures/Earthquake/Earthquake_EN.pdf *Letöltés: 2012.08.12.*

[6] Várhelyi Judit: Tokióban a helyzet - Építészet és természeti katasztrófák, Építészfórum, 2011.08.19. http://epiteszforum.hu/node/19412 *Letöltés: 2012.08.12.*

[7] Magyar találmány óvta meg a nagyobb tragédiától Japánt, hirado.hu, 2011.03.20.
http://www.hirado.hu/Hirek/2011/03/20/19/Magyar_talalmany_ovta_meg_a_nagyobb_tragediatol_Japant.aspx *Letöltés: 2012.08.12.*

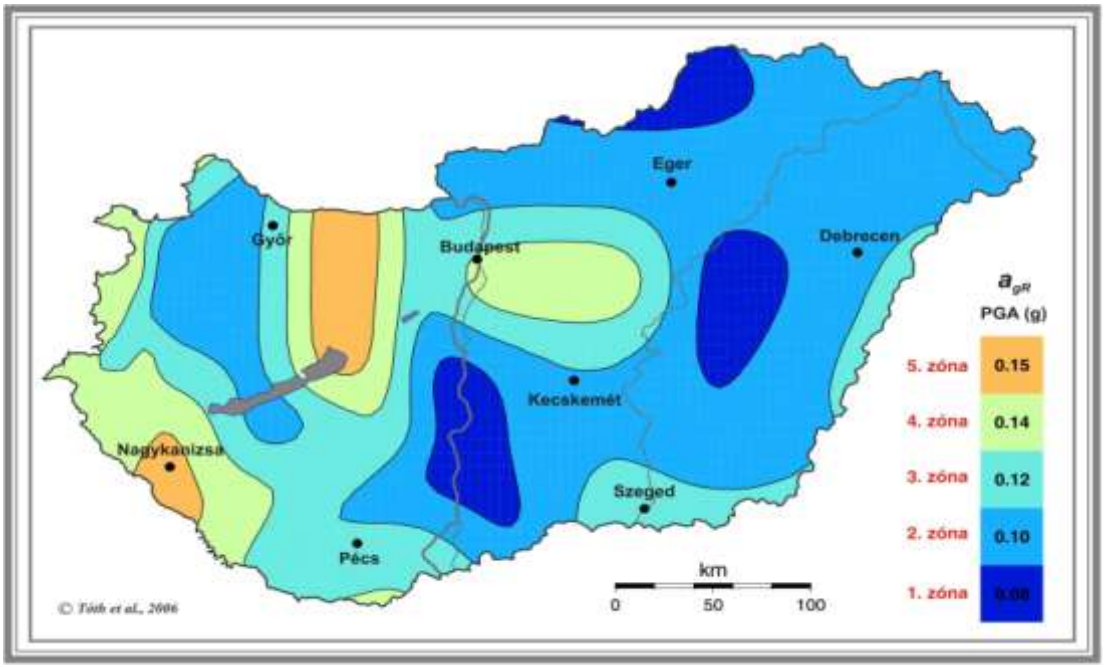
[8] Eurocode 8 - Földrengés, Eurocodes Expert
http://www.eurocodes.co.uk/EurocodeDetail.aspx?Eurocode=8 *Letöltés: 2012.08.12.*

[9] Tornai László (KÉSZ Zrt) előadása: A földrengésről mérnök szemmel, méretezés földrengésre, Budapest, 2011.12.16.
http://www.csmi-mernoki-kamara.hu/files/2011.12.16.%20-%20M%C3%A9retez%C3%A9s%20f%C3%B6ldreng%C3%A9sre.pdf
Letöltés: 2012.08.12.

[10] Magyar Larousse Enciklopédia III. kötet, Akadémiai Kiadó, Budapest, 1994 ISBN: 963-05-6748-2, a Richter-skála kifejezésre (478. o.)

[11] Földrengések Magyarországon és az épületek földrengés-biztonsága, Készház portál, 2011.01.29.
http://kp.hu/foldrengesek-magyarorszagon-es-az-epuletek-fodrengesbiztonsaga/
Letöltés: 2012.08.12.

Mellékletek



***1*. melléklet.** Magyarország szeizmikus zónatérképe Forrás: http://www.foldrenges.hu/images/stories/cikkek/images/TLfoldrengeskockazat4.jpg

Talaj típus	A rétegsor leírása	Jellemző paraméterek		
		$v_{s,30}$ (m/s)	N_{SPT} (ütés/30cm)	c_u (kPa)
A	kőzet vagy kőzetszerű geológiai formáció, beleértve legfeljebb 5 m gyengébb anyagot a felszínen	> 800	-	-
B	konszolidált, nagyon szilárd homok, kavics vagy agyag rétegek legalább több tíz méter vastagságban; a szilárdsági tulajdonságok a mélységgel fokozatosan javulnak	360 – 800	> 50	> 250
C	szilárd és közepesen szilárd homokos, kavicsos, agyagos rétegek, melyek vastagsága tíz métertől több száz méterig terjed	180 – 360	15 – 50	70 – 250
D	laza, közepes tartóképességű talaj rétegek	< 180	< 15	< 70
E	Olyan talaj profil, ahol a felső 5-20 méteren a v_s sebesség a C vagy a D talaj típusnak megfelelő, alatta pedig szilárdabb (v_s> 800 m/s) anyag található			
S_1	A felső rétegek között egy legalább 10 m vastag puha, képlékeny (PI>40), nagy víztartalmú agyag réteg található	< 100	-	10 – 20
S_2	Talajfolyósodásra hajlamos réteg(ek) fordulnak elő; minden olyan profil, mely nem sorolható az A-E vagy S_1 kategóriák valamelyikébe			

2. melléklet. A talajviszonyok osztályozása
Forrás: az MSZ EN 1998-1/ EUROCODE 8 szabvány 3.1. táblázata

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Dobák Imre
dobak.imre.@uni-nke.hu

BETEKINTÉS AZ ÁLLAMBIZTONSÁG 1960-70-ES ÉVEI NEMZETKÖZI TECHNIKAI KUTATÁS-FEJLESZTÉSI FOLYAMATAINAK SZERKEZETÉBE

Absztrakt

A szerző tanulmányában a szocialista állambiztonság időszakának egyes nemzetközi technikai kutatási kérdéseit veszi vizsgálat alá. Az áttekintett folyamatok hosszabb távon fontos szerepet játszottak a különböző operatív képességek megteremtésében. Az állandóan változó technikai környezet és kihívások mentén a nemzetközi együttműködési kapcsolatok meghatározták azokat a kutatási folyamatokat, amelyek a háború utáni technikai bázis színvonalának növelésére irányultak. A tanulmány célja a tudományos folyamatok bemutatásával hozzájárulni a szocialista állambiztonság sajátos eszközei és eszközrendszerei fejlődésének megértéséhez.

In this short essay the author examines some international technical research issues of the socialist state security period. The reviewed processes played important role in the creation of different operational capabilities in long term. Along the permanently changing technical environment and challenges, the relations of international cooperation have determined those research and development processes that helped to increase the quality of technical basis after the Second World War. The aim of this study is to contribute to understand the development of specialized equipments by presenting the scientific process in the state security era.

Kulcsszavak: *technikai fejlesztés, kutatás, állambiztonság, együttműködés ~ technical development, research, state security, cooperation*

BEVEZETŐ

A szocialista állambiztonság időszakában az egyes szakfeladatok végrehajtását támogató technikai kutatási és fejlesztési folyamatok fontos szerepet kaptak, amelyek jelentősége a külső technikai környezet fejlődésével párhuzamosan, az 1960-as évektől még nagyobb hangsúllyal kerültek előtérbe. A nemzeti szinteken rendelkezésre álló kutatási - fejlesztési képességek és kapacitások kihasználása, a folyamatosan bővülő, egyre mélyebb szakmai ismeretekkel rendelkező szakemberek részvétele mellett, azonban a többi szocialista országgal nemzetközi szinten megvalósított együttműködések is sajátos, jól szervezett felületet biztosítottak a technikai környezettel való lépéstartásra. Jelen tanulmány célja, hogy bepillantást engedjen az 1960-70-es évek célorientált mérnöki gondolkodását visszatükröző, nemzetközi kutatási és fejlesztési folyamatok belső szerkezetébe, amely emellett értékes ismeretekkel szolgálhat a téma nemzetközi viszonyainak megértéséhez is.

A korszak a hidegháború időszaka, amelyet (hadi)technikai értelemben is a szembenállás és rendkívüli verseny jellemzett. A külső biztonságpolitikai környezetben lezajlott események azonban a titkosszolgálati – állambiztonsági gondolkodás technikai aspektusainak fejlődését is felgyorsították. Ötven-hatvan évre visszatekintve a hazai állambiztonsági szervezetrendszer technikai-kutatási területeinek fontos feladatai között is megjelent a technikai eszközöket alkalmazó különböző szakterületek technikai feltételrendszereinek a megteremtése. A második világháborút követő években megörökölt, elhasználódott technikai eszközöket is alkalmazó titkosszolgálati – állambiztonsági szféra fejlesztési kérdései az 1950-es évektől kaptak igazi lendületet, amelynek legfőbb előmozdítói az európai szocialista országokkal kialakított állambiztonsági témájú bilaterális és multilaterális együttműködések voltak. „Lényegében a Varsói Szerződés létrejöttétől datálható a kommunista titkosszolgálatok közötti (bilaterális) kapcsolattartás rendszeressé tétele. Ezek jószerivel csak a hatvanas évek első harmadától lényegültek át – a szovjetek által koordináltan – tényleges multilaterális csapatmunkává”[1]. A vonatkozó együttműködések, illetve azok módosított megállapodásai egészen a rendszerváltás időszakáig végigkísérték az állambiztonság különböző technikai eszközöket alkalmazó szakterületeinek fejlődési irányait.

AZ EGYÜTTMŰKÖDÉS KERETRENDSZERE

Az operatív-technikai együttműködések jelentős állomásaként az 1960-as évek elejét kell megemlíteni, amikor is a magyar szervek munkatársai egy szakmai látogatás alkalmával betekintést kaphattak[2] az érintett szovjet állambiztonsági szervek munkájába. Az ez követő időszakban kialakult együttműködés, valamint az 1973-ban kötött általánosabb keret-megállapodás[3] (a Magyar Népköztársaság Belügyminisztériuma és a Szovjetunió Minisztertanácsa mellett működő Állambiztonsági Bizottság közötti 1973-ban kötött együttműködési egyezmény 1. cikkely 5 pontja, amely szerint a felek „együttműködtek operatív-technikai eszközök mintapéldányainak elkészítésében, az érvényben levő operatív-technikai együttműködési egyezményekben foglaltaknak megfelelően) megfelelő keretet biztosítottak többek között az egyes kutatási, fejlesztési tevékenységek összehangolására, a párhuzamosságok elkerülésére, valamint a szakterületek korszerű eszközökkel történő

[1]Gyarmati Gy. - A magyar humán hírszerzés átnyergelése a (mostoha)testvéri technikára Betekintő 2012/1. szám. http://www.betekinto.hu/ (Az Állambiztonsági Szolgálatok Történeti Levéltárának internetes folyóirata), letöltve: 2013.02.20.

[2] ÁBTL 1.11.8. 60-2035/60

[3] Lásd Krahulcsán Zsolt - KGB és III. Főcsoportfőnökség: egy kapcsolat vége…(?) (A szovjet–magyar állambiztonsági együttműködés szabályozása 1989-ben) Betekintő, 2007/4. száma, http://www.betekinto.hu, letöltve: 2013.02.20.

ellátását segítő tapasztalatcserére. Az operatív-technikai kérdésekben főként a kétoldalú kapcsolatok jelentették a technikai színvonal és módszerbeli, valamint alkalmazásbeli fejlődés lehetőségét, így a célok, tervek definiálására is a nemzeti szakmai igények mentén alapvetően a kétoldalú kapcsolatokban került sor[4].

A másik jelentős, sajátos technikai fejlesztéseket igénylő szakterület a rádióelhárítás[5] volt. A második világháborút követően lassan kibontakozó rádióelhárító tevékenység eredményességének fokozása kapcsán, az első nemzetközi szintű lépések az egyes szocialista országokkal való kapcsolatokra vezethetőek vissza, amelyek során pl. „1951 és 1954 között Csehszlovákiával, Lengyelországgal és Bulgáriával”[6] kötöttek a magyar szervek megállapodásokat. A multilaterális együttműködési kapcsolatok 1955-től jelennek meg az európai szocialista országok közös rádióelhárító szervezetének létrehozásával[7], amely központosított koordináló szerveként az ún. Koordinációs Központ[8] jelent meg. (Habár a belügyi rádióelhárítás és a katonai rádiófelderítés eltérő szervezeti keretek között fejlődött[9] az 1940-es évek végétől, a Varsói Szerződés időszakához köthető szakmai együttműködés mindkét területre erőteljes hatást gyakorolt.)

Anélkül, hogy részleteiben kitérnék az érintett belügyi nemzetközi együttműködés részleteire, annak fő feladatát képezte a rövidhullámú sávtartományban, a szocialista országok területén működő rádiósügynökök adásainak felderítése és iránymérése, amely tevékenységek csak korszerű és hatékony munkavégzést biztosító technikai eszközrendszerekkel és együttműködésben voltak biztosíthatóak. Ennek a tevékenységnek a szakmai irányítása, összehangolt technikai fejlesztési kérdései és folyamatai alkották azokat a kulcsterületeket, amelyek a szocialista országok rádióelhárító szolgálatainak együttműködésével alapjaiban biztosíthatták a közös szakmai feladatok teljesítését. A technikai – műszaki kérdések kiemelt szerepét és szakmai sajátosságait jelzi, hogy az együttműködésen belül – már a megalakuláskor - külön műszaki bizottság kerül kialakításra[10].

A nemzetközi technikai együttműködések keretében felmerülő kutatási – fejlesztési témaköröket ún. „témák” alá csoportosították, amelyek alapját képezték a számtalan különböző szakirányt felölelő fejlesztendő kérdéseknek. A „témák” alá csoportosított fejlesztések eredményei fokozatosan jelentkeztek, így a későbbiekben sor került a kutató és kísérleti – konstrukciós munkák során elkészült speciális technikai eszközök szállítási kérdéseinek rendezésére is.

Rendszeres találkozókon tekintették át a korábbi évek együttműködésének terveit és határozták meg a következő évek feladatait. Az érintett feladatok nagyságát és összetettségét jelzi, hogy az egyik ilyen 1970-es évekbeli szovjet-magyar találkozón például a szovjet fél részéről 50, a magyar fél részéről 19 téma és közös területként pedig 5 téma jelent meg az

[4] ÁBTL 46-2681/50/63 Jegyzőkönyv, valamint ÁBTL 46-4416/1963 Feljegyzés

[5] A rádióelhárítás és rádiófelderítés fogalmak közötti korabeli értelmezési különbség: 1. Rádióelhárítás - a felderített rádiós- ügynök vagy ügynökgyanús személy rádióállomása földrajzi helyzetének megállapítása. 2. Rádiófelderítés - állambiztonsági funkció. Feladata: a rövidhullámú frekvenciasávban felderíteni az ellenséges hírszerző szervek rádióközpontjait, rádiósügynökeit, ellenállomásait, valamint az ügynökgyanús és ismeretlen rádióállomásokat. ÁBTL 4.1 A-3036

[6] Borvendég Zsuzsanna - A BM II/16. Osztályának (Rádió-elhárítás) története és szervezeti felépítése 1945–1962 között - Betekintő – 2012/4. szám, http://www.betekinto.hu, letöltve: 2013.02.20.

[7] Az „európai népi demokratikus országok” rádióelhárító szolgálatai által 1955-ben kialakított, kezdetben varsói székhellyel működő nemzetközi együttműködés. ÁBTL, 1.11.8. 0024-20/9-55 (Jegyzőkönyv)

[8] Varsói Koordinációs Apparátus: a szocialista országok állambiztonsági szerveinek szerződésben vállalt kötelezettsége saját rádióelhárítási szerveik feladataira vonatkozóan. Forrás: Állambiztonsági Értelmező Szótár, http://hu.scribd.com/doc/47552737/Korabeli-allambiztonsagi-ertelmez%C5%91keziszotar (letöltve: 2013.02.10.)

[9] lásd: Imre Lajos – A hadászati rádiófelderítés a hidegháború éveiben 1946-1990, in: Felderítő Szemle, 2008. nov. VII. Évfolyam, 96 o., valamint Dr. Várhegyi István – A magyar rádiófelderítés működése a hidegháború éveiben 1945-1990, In: Felderítő Szemle, 2004. jún. III/2. szám, 133 o.

[10] ÁBTL, 1.11.8. 0024-20/9-55, Jegyzőkönyv

együttműködésben. Az 1970-es évek közepén zajlott másik megbeszélésen- amelyen Magyarországról két csoportfőnökség is képviseltette magát - az együttműködésbe a magyar Műszaki Fejlesztési Csoportfőnökség részéről 12, szovjet részről 13 téma, a magyar Operatív Technikai Csoportfőnökség részéről 10, szovjet részről 14, közös témaként pedig további 5 téma került bevonásra[11]. Az érintett témák a televízió, rádió és optika, valamint okmány, írás és szakértő témaköröket érintették.

Az együttműködések és ezen belül a kutatási-fejlesztési témák alatt megfogalmazott feladatok céljaként - relációtól függetlenül - többek között az alábbiakat láthatjuk:

- technikai eszközök, berendezések mintapéldányainak kifejlesztése;
- beszámoló elkészítése és másik félnek történő átadása az adott téma fejlesztéséről;
- technikai leírások adott témához kapcsolódó átadása a másik félnek;
- operatív technikai és elméleti kísérleti problémák megoldása;
- speciális technikai mintakészülékek cseréje;
- középtavú munkamegosztás;
- valamint tudományos és tapasztalatcsere.

Az operatív technikai irányú megállapodások keretében kitértek a felek közötti speciális technikai eszközök és anyagok szállításának lebonyolítására, valamint elszámolására is. Ennek lényege, hogy a megállapodások alapján a felek közvetlenül, a külkereskedelmi szervek közvetítése nélkül szállítottak egymásnak olyan speciális-operatív eszközöket és anyagokat, amelyeket a másik fél készített, a másik fél belső piacán vásároltak, vagy a másik fél a kapitalista külföldön vásárol.

Az egyes fejlesztési folyamatok szempontjából érdemes a rádiótechnikai fejlesztések azon folyamatát áttekinteni, amelyek a rádióelhárítás nemzetközi együttműködési feladatrendszeréhez kapcsolódtak. A szakterületet szélesebb nemzetközi formában koordinált fejlesztések jellemezték, amelyek sajátosságaiként jelentek meg, hogy az egyes témaköröket a nemzetközi szinten magvalósított rádióelhárítási feladatrendszer technikai rekonstrukciós munkáihoz igazodva határozták meg. A tagországokban kialakított, rendszerelemként értelmezhető eszközökkel kölcsönösen egészítették ki a rádióelhárítás nemzetközi rendszerének elemeit. Az adott témakör kutatásával foglalkozó adott ország fejlesztési területe a többi tagországai igényei alapján végezte az eszközök sorozatgyártását. Ezek gyakran azonban nem kizárólag belső fejlesztésekkel, hanem „külső” kutatóintézetek bevonásával zajlottak. Példaként említhető, hogy magyar rögzítő eszközöket biztosítottak a többi európai szocialista ország rádióelhárító szolgálatának.

A RÁDIÓELHÁRÍTÁS FEJLESZTÉSI FOLYAMATAINAK KERETRENDSZERE

A hazai rádióelhárítás történetében megjelenő főbb szakaszok közül a második világháborút követő években megjelenő, főként a fennmaradt haditechnikai eszközökre épülő első szakaszt[12] követő periódust (1955-től) tartjuk a szocialista együttműködés keretében megvalósított rádióelhárítás időszakának. Ezen a területen a vonatkozó kapcsolatokat a már említett széleskörű multilaterális együttműködés jellemezte, így a kutatási – fejlesztési kérdések és célok megfogalmazására is alapvetően a közösen működetett rendszerekhez illesztetten, központosítottan, koordinált módon került sor. A koordinálás szakmai okait az együttműködésben résztvevő állambiztonsági szolgálatok nemzeti szintű rádióelhárítási

[11] ÁBTL, 89-26-14/75 Jegyzőkönyv tanácskozásról

[12] az 1949-1955 közötti időszak (ÁBTL, 4.1 A-3168/1-5 (13-68/240/84) Állambiztonsági (Szolgálati) Ismeretek, 1984.)

területeinek egységes eszközellátása, a végrehajtandó feladatok és rendszerben való értelmezhetősége indokolta.

A vonatkozó tevékenységeket a speciális berendezések fejlesztésével és kidolgozásával kapcsolatos tudományos-kutató munkák, és kísérleti-konstrukciós munkák végrehajtási rendje[13] keretében szabályozták, amely részleteibe történő alábbi betekintés jól szemlélteti az egyes folyamatokat.

A szabályzat célja az volt, hogy meghatározza a rádióelhárító szolgálatok céljait szolgáló speciális készülékekkel kapcsolatos tudományos-kutató munkák és konstrukciós munkák rendjét az egyeztetett tervek és feladatok függvényében. A szabályozás (nem megjelenített) célja lehetett egyfelől a nemzetközi színterén jelentkező kutatási párhuzamosságok elkerülése, másfelől a rendelkezésre álló technikai – tudományos kapacitások hatékonyabb kihasználása is. A szabályzat - amely betartása kötelező érvényű volt minden együttműködésben érintett szolgálat számára - kimondta, hogy a tudományos kutató és kísérleti-konstrukciós munkát a felek önállóan, vagy egyesített erővel folytathatnak.

Az egyes szaktevékenységeket érintően két nagyobb elkülöníthető részt különböztettek meg, így az ún. tudományos-kutató munkát (TKM), valamint az ún. kísérleti-konstrukciós munkát (KKM).

Tudományos-kutató munka (TKM)

Ennek folyamatai alatt olyan tevékenységet értettek, amely rendszerint „tudományos beszámolóval és a kiválasztott megoldás helyességét alátámasztó készülék működő makettjének, vagy egyes elemeinek elkészítésével, valamint a kísérleti-konstrukciós munkákhoz szükséges taktikai-technikai követelmények elkészítésével ér véget".

Kísérleti-konstrukciós munka (KKM)

A kísérleti-konstrukciós munka megfogalmazása alatt olyan tevékenységet határoztak meg, amely az új technikai eszköz „kísérleti mintapéldányának létrehozásával kapcsolatos munkakomplexum elvégzését irányozta elő, a tudományos-kutató munka vagy korábban folytatott fejlesztések alapján. A kísérleti-konstrukciós munka a berendezés kísérleti mintapéldányának elkészítésével ért véget, amelyek a berendezések sorozatgyártásához szükségesek."

Az egyes fejlesztési munkák (tudományos-kutató és kísérleti-konstrukciós) megrendelőjeként mindig azon ország állambiztonsági szervének rádióelhárító szolgálata jelent meg, amely országban az adott munkát végezte. Ebben az esetben a munkákat „megrendelő" fél volt felelős az adott fejlesztések végrehajtásáért és annak különböző részterületeiért. Abban az esetben, ha a tudományos-kutató vagy kísérleti-konstrukciós feladatokban több tagország is részt vett, a rádióelhárító szolgálatok nemzetközi együttműködését koordináló központi szerv hatáskörébe került annak meghatározása, hogy melyik szolgálat került felelősként kijelölésre az adott feladat végrehajtásáért.

A szabályzat kitért arra is, hogy a tudományos-kutató vagy kísérleti-konstrukciós tevékenység kapcsán kik vehetnek részt a kivitelezési feladatokban. Ezek egyrészről az adott tagország szolgálatainak szakterületei, másrészről különböző tudományos-kutatóintézetek lehettek. Az adott fejlesztést megrendelő és azért felelős szolgálat döntése alapján egyéb, nem az állambiztonsági szférához kapcsolódó katonai, polgári intézetek, vagy vállalatok is bekapcsolódhattak a fejlesztési feladatokba „a titkosság szükséges mértékű betartásával". Az átfogó szabályzat keretén belül a megrendelő szerv kötelességeinél kerültek megjelenítésre az együttműködést koordináló központi szerv irányába jelentkező feladatok, így például az időszakos tájékoztatási kötelezettség („nem ritkábban mint 1-2 alkalom évenként"), a

[13] ÁBTL, 1.11.8. 00202/3K-72, Kivonat a KA XIII. Kibővített Tanácskozásának jegyzőkönyvéből

fejlesztések eredményeinek közös megtekintése, a kísérleti mintapéldányok „kipróbálási programjának és metodikájának” egyeztetése.

Mindezek mellett a szocialista országok nemzetközi szintű rádióelhárító együttműködésének központosítottságát mutatja, hogy a koordinációs szervezet fenntartotta magának a jogot, hogy ”évente legalább egyszer [….] megismerkedjen a fejlesztés állapotával”. További lehetőségei közé tartozott, hogy a fejlesztést végző szolgálattal összehangolva, bevonja más együttműködő szolgálatok szakembereit a fejlesztés bármely szakaszában az eredmények megtekintésébe és a technikai konzultációk folytatásába. A hivatkozott dokumentum jól mutatja, hogy az ún. Koordináció joga széles körben kiterjedt az egyes nemzeti szolgálatoknál folyó fejlesztési munkákban való betekintésre, és egyfajta ráhatással lehettek a fejlesztési folyamatokra is. A megállapítást támasztja alá a szabályzatnak azon része is, amely leírja, hogy abban az esetben, ha az adott nemzeti szintű rádióelhárító szolgálat által folytatott fejlesztési feladat nem megfelelő műszaki szinten folyt, „nem a szolgálatok közös érdekeinek megfelelő irányba halad” vagy akár „nem fejeződik be a tervbe vett határidőre” közvetetten beavatkozhattak és közös értekezlet keretében vitathatták meg a munka „sikeres befejezéséhez szükséges” intézkedéseket.

A fejlesztés napjainkban is, de a hidegháború időszakának állambiztonsági szférájában is rendkívül költség és tudásigényes területet képviselt. Az egyes tudományos-kutató vagy kísérleti-konstrukciós munkák finanszírozása éppen ezért szabályozott kérdésként jelent meg a nemzetközi színtéren is. A korszak kialakított megoldása szerint a fejlesztési munkák költsége minden esetben a megrendelő szolgálatokra hárult, azok költségvonzatainak a többi együttműködő szervvel történő megosztása nélkül. A felmerülő költségek viselésénél a fejlesztés adott szakaszaiban mindemellett nem kerülhettek figyelembevételre a későbbi sorozatgyártás szempontjai, valamint a fejlesztés folyamatok során felmerülő költségek utólag sem voltak megjeleníthetőek (például egy másik szocialista ország szolgálatának kikínált sorozatgyártott eszköz árában).

Az alábbi, a rádióelhárító terület nemzetközi együttműködési felületében megjelenő - a vonatkozó dokumentumok[14] alapján összeállított eszközfejlesztési folyamat - lépései jól jelzik a tevékenység rendkívüli összetettségét és vezetettségét.

1. A készülékek, technikai eszközök fejlesztése az adott szerv évekre előremutató rekonstrukciós tervének megfelelően kerültek meghatározásra. A különböző fejlesztési témákat, mint javaslatokat az érintett szolgálatok megküldték a nemzetközi szintű koordinációs szervnek, akik ezeket véleményezték és összesítették.
2. A különböző fejlesztési témákat (TKM, KKM) alapvetően az egyes szolgálatok nemzeti szinteken dolgozó munkatársai állították össze.
3. A fejlesztési témák többi szolgálattal való egyeztetésének feladata azonban már a nemzeti szinteken túlmutatva a koordinációs szervezetre hárult, amely az egyeztetések eredményéről visszatájékoztatta a témát megrendelő szolgálatot.
4. Az adott téma kidolgozása és határidejének meghatározása csak az összes szolgálattal való egyeztetés után kezdődhetett meg. Érdekes elemként jelent meg, hogy azon fejlesztési témákban, amelyekben nem volt egyetértés, a koordinációs szerv szerepe értekezletek, konzultációk megszervezésére irányult, a végső döntést az adott téma „célszerűségéről” azonban a kidolgozó ország biztonsági szerve vezetői hoztak.
5. Az adott fejlesztési feladat beindításához kapcsolódó egyes adminisztratív feladatok (pl. a fejlesztéshez kapcsolódó anyagok szövegezése, konzultációk és találkozók

[14] forrás: ÁBTL, 1.11.8. 00202/3K-72, Kivonat a KA XIII. Kibővített Tanácskozásának jegyzőkönyvéből

szervezése) a központi szervre hárultak és a megvalósítás munkafázisa a vonatkozó jegyzőkönyv aláírásával kezdődhetett meg.

6. A különböző fejlesztési témákat és kapcsolódó műszaki feladatokat a megrendelő rádióelhárító szolgálatok és a nemzetközi koordinációs szerv jogosult munkatársai írták alá. Több tagországot érintő fejlesztési feladatok során természetesen az aláírók köre is bővült.
7. A fejlesztési szakasz az egyes részes szolgálatok feladataként megjelenve, számos sajátossággal összetetten (pl. belső fejlesztési kapacitások, szakembergárda, illetve külső szervek – intézetek esetleges igénybevétele) kerültek végrehajtásra.
8. Az eszközök kifejlesztését követően az átvételi eljárás, hasonlóan az egyes koordinált fejlesztések megkezdéséhez, szabályozott és nemzetközi színtéren összetett tevékenységként jelent meg. Az egyes technikai fejlesztések elvégzését követőn azok átvételét az összes együttműködő ország szakembereiből álló bizottság végezte.
9. Számos adminisztratív elem nehezítette a folyamatot. Ilyenek voltak például az adott műszaki és tudományos dokumentációk teljes körű elkészítése. Ezek alapesetben a kivitelező ország nyelvén készültek el, majd adott részeiket az együttműködés hivatalos nyelvére, oroszra fordították és megküldték a többi együttműködő szolgálatnak. Ezek formai megjelenése, terjedelme, példányszáma mind nemzetközi egyeztetési feladatként jelent meg.
10. Az átvételi eljárás során első körben az érintett tagország saját szakembereiből álló bizottság vette át a fejlesztés eredményét, majd ezt követte a nemzetközi szakemberekből álló bizottság átvételi eljárása. Anélkül hogy részleteiben ismertetném az átvétel összetettségét és folyamatait, számos egyeztetés, jóváhagyás előzte meg a későbbi esetleges sorozatgyártás megkezdését.
11. Az eszközök sorozatgyártása rendszerint abban az országban történt, ahol az eszközrendszer mintapéldányának előállítása megtörtént. Azokban az esetekben, amikor azonban nem állt rendelkezésre megfelelő technikai háttér és gyártókapacitás, másik tagországban is megszervezhető volt a sorozatgyártás az adott felelős megrendelő szolgálat biztonsági szervének egyetértése esetén.

Nem tekinthető elhanyagolható területnek különösen a sorozatgyártott eszközökhöz, és rendszerekhez kapcsolódó képzés feladata sem, amely - figyelembe véve az eszközt felhasználó egyéb tagországokhoz kapcsolódó nemzetközi vonzatokat is - a kivitelező, kidolgozó szolgálatra hárult. A kifejlesztett eszközrendszerek megrendelését az érintett rádióelhárító szolgálatok a koordinációs szervezeten keresztül bonyolíthatták, amely tájékoztatást adott a sorozatgyártást szervező félnek a szükséges mennyiségről. Az eszközök valós beszerzése azonban már az adott ország saját külkereskedelmi szervén segítségével történt.

ÖSSZEGZÉS

A szocialista állambiztonság 1960-70-es éveiben az állambiztonság operatív technikai hátterét biztosító nemzetközi fejlesztéseket mérnöki szemmel a célorientáltság, a tervszerűség és a szervezettség jellemezte. Mindezek mellett azonban az állambiztonsági tevékenység sajátosságaiból adódóan a titkosság és a konspiráltság is végigkísérte a kutatási fejlesztési kérdéseket. A kutatási és fejlesztési, valamint az ezekhez kapcsolódó kísérleti feladatok összetételét vizsgálva azok főként egy-egy új önálló eszköz fejlesztéséhez, vagy egy rendszer részelemét képező eszköz kialakításához kapcsolódtak. A nemzetközi kutatási – fejlesztési együttműködések alapját a vonatkozó együttműködési megállapodások képezték, amelyekben

foglaltak teljesítését az érintett állambiztonsági szervek vezetői rendszeres időközönként vezetői találkozókon tekintették át. Ezeken a találkozókon került sor a végrehajtott feladatok és az elkövetkező évek fejlesztési-kutatási témáinak meghatározására és azok eredményei kölcsönös hasznosíthatóságához kapcsolódó folyamatok gyakorlati kérdéseinek tisztázására is. Az említett fejlesztési – kutatási felületeket megalapozó állambiztonsági szakterületek vonatkozásában lényeges különbség a már említett bi- és multilaterális megvalósítási formáktól eltérően abban mutatkozott meg, hogy a rádiótechnikai kérdéseket jóval szélesebb körű nemzetközi kooperáció, külső kutató intézetek bevonásával járó fejlesztési lehetőségek, valamint a képzések szélesebb körben történő megvalósításának gyakorlata is jellemzett.

Felhasznált irodalmak

[1] Borvendég Zsuzsanna - A BM II/16. Osztályának (Rádió-elhárítás) története és szervezeti felépítése 1945–1962 között - Betekintő 2012/4. szám, http://www.betekinto.hu/ letöltve: 2013.02.20.

[2] Fisher Ferenc – A kétpólusú világ 1945-1989, Dialóg Campus Kiadó, Budapest-Pécs, 2005

[3] Gyarmati György - A magyar humán hírszerzés átnyergelése a (mostoha)testvéri technikára Betekintő 2012/1. szám. http://www.betekinto.hu/ letöltve: 2013.02.20.

[4] Imre Lajos – A hadászati rádiófelderítés a hidegháború éveiben 1946-1990, In: Felderítő Szemle, 2008. nov. VII. Évfolyam, MK KFH, Budapest, pp. 94-99

[5] Krahulcsán Zsolt - KGB és III. Főcsoportfőnökség: egy kapcsolat vége…(?) (A szovjet–magyar állambiztonsági együttműködés szabályozása 1989-ben), Betekintő, 2007/4. szám, http://www.betekinto.hu/ letöltve: 2013.02.10.

[6] Müller Rolf - Az operatív technika alkalmazása és szervezeti keretei a politikai rendőrségen (1945–1962). In.: Szakszolgálat Magyarországon, avagy tanulmányok a hírszerzés és titkos adatgyűjtés világából (1785–2011). Csóka F. (főszerk.). Budapest, Nemzetbiztonsági Szakszolgálat, 2012

[7] Opauszki P. - Vörös J. - Rádióforgalom ellenőrzés. In.: Szakszolgálat Magyarországon, avagy tanulmányok a hírszerzés és titkos adatgyűjtés világából (1785–2011). Csóka F. (főszerk.). Budapest, Nemzetbiztonsági Szakszolgálat, 2012

[8] Pászka Tibor - Szükség van-e a rádióelektronikai felderítésre? Felderítő Szemle, 2004. jún. III/2. szám, MK KFH, Budapest, pp. 84-90

[9] Várhegyi István - A magyar rádiófelderítés működése a hidegháború éveiben 1945-1990, Felderítő Szemle, 2004. jún. III/2. szám, MK KFH, Budapest, pp. 126-153

Levéltári Források:

[10] ÁBTL, 1.11.8. 98-13-4/1974. BM III/5. Osztály, Jelentés a KA XIV. értekezletéről

[11] ÁBTL, 1.11.8. 98-13-5/1975. A KA vezetőjének tájékoztatása, a XV. Kibővített Tanácskozás előzetes napirendjéről, valamint a Tanácskozás munkarendjével kapcsolatos javaslatokról

[12] ÁBTL, 1.11.8. 98-13-4/75. A KA vezetője által a MNK Belügyminiszter-helyettes részére megküldött időszaki beszámoló

[13] ÁBTL, 1.11.8. 98-291/85 BM III/5. Osztály által a BM III. Főcsoportfőnök első helyettesének készített felterjesztés. Felterjesztett anyag: 98-291/1985 BM III/5. Osztály (Rádióelhárítás) ideiglenes ügyrendje

[14] ÁBTL, 1.11.8. 00202/3K-72, Kivonat a KA XIII. Kibővített Tanácskozásának jegyzőkönyvéből

[15] ÁBTL 1.11.8. 98-13-7/76. (Fejlesztési terv)

[16] ÁBTL 89-26-14/75 (Jegyzőkönyv)

[17] ÁBTL 60-156/61 (Egyezmény tervezet)

[18] ÁBTL 46-126/64 (Megállapodás)

[19] ÁBTL, 10-1837/1967. BM III/V. Főcsoportfőnökség ügyrendje,

[20] http://www.abtl.hu/sites/default/files/pdf/forrasok/iii_ugyrend_1967.pdf (letöltve: 2013.02.10.)

[21] ÁBTL, 98-37/1972. BM III/5. Osztály ügyrendje,

[22] http://www.abtl.hu/sites/default/files/pdf/forrasok/ugyrend_10.pdf (letöltve: 2013.02.10.)

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Antal Örs
antal.ors@gmail.com

A FÖLDRENGÉSÁLLÓ ÉPÍTKEZÉS KORSZERŰ LEHETŐSÉGEI

Absztrakt

Haiti, Szecsuán, L'Aquila, Törökország; elég csak néhány esetet felsorolni az elmúlt évek súlyos földrengései közül, aminek következtében a felbecsülhetetlen anyagi károk mellett tízezrek vesztették életüket és százezrek váltak hajléktalanná. A földrengés megelőzésére és elkerülésére nincsen mód, azonban ismét bebizonyosodott, hogy a veszteségek a megfelelő építési technológia alkalmazásával minimalizálhatóak lehettek volna, a Japán mintát követve. Hazánk nem tartozik a magas földregés veszélyeztetettséggel bíró országok közé, azonban a régi, elavult technológiával épült épületek magas száma miatt egy kisebb erejű rengés is jelentős kockázatot jelenthet a jövőre való tekintettel. Jelen tanulmány bemutatja a földrengésálló építkezés főbb szempontjait, valamint a világszerte elterjedt és hatékonynak bizonyul technológiai megoldásokat. Emellett vizsgálja, hogy az uniós szabályozás tükrében milyen tendenciák mutatkoznak az európai, így a hazai földrengésbiztonsági építkezés tekintetében is.

Haiti, Sechuan, L'Aquila and Turkey are examples for devastating earthquakes from the recent years causing ten thousands of deaths and hundred thousands of homelesses besides the inestimable property damages. No applicable method exists to prevent or avoid the earthquakes, neverthelles it had been proved again that the losses could had been minimized with the suitable earthquake-resistant building technology, following the Japanese pattern.Our country does not belong to the significantly earthquake-endangered countries, however due to the high number of bulildings contstructed by old and traditional technology a smaller earthquake could cause high risk in the future, too. This study represents the most important aspects of earthquake-resistant building methods and the world-wide technologies that proved to be efficient. Furthermore it investigates the future european tendencies in point of the domestic and international earthquake-resistant building technologies.

Kulcsszavak: *horizontális erő, rengéshullámok, Japán, rugalmasság, méretezés ~ horizontal force, seismic waves, Japan, flexibility, sizing*

BEVEZETÉS

A legpusztítóbb, évente százezres nagyságrendben mérhető haláleseteket okozó természeti katasztrófák a földrengések, amelyek ellen - a magas technológiai fejlettség ellenére - a mai napig nem létezik hatékony előrejelzési módszer, emellett a rengések megelőzésére nincs mód, csak a pusztító hatás csökkentésére. Ennek kulcsa a földrengésálló építészeti technológia, ami szerves részét képezi a védelmi képességek növelésére, valamint a megelőzésre irányuló tevékenységeknek. Az építészeti eljárások jelentőségét jól alátámasztja Japán, amely földünk szeizmikusan legaktívabb zónájában helyezkedik el, mégis az elmúlt évek jelentős földrengései alig tettek kárt a szigetország építményeinek szerkezeteiben. A tanulmány során részletesen bemutatásra kerülnek ezen építészeti technológiák, kiemelten foglalkozva a könnyű acélszerkezetes megoldás jelentőségével. A technológia háttér tisztázása mellett vizsgálom ennek szabályozási hátterét, ami alapvetően meghatározza az európai földrengésbiztonsági építkezési tendenciákat is a jövőre való tekintettel. Fontos továbbá tisztázni, hogy melyek azok a legfontosabb szempontok és eljárások, amelyeket a tervezésnél figyelembe kell venni. Az olykor merésznek tűnő, ugyanakkor hatékony technológiai eljárásoknak köszönhetően az elmúlt évtizedekhez képest áttörés történt a földrengésálló építkezés terén, amit a növekvő urbanizáció kiemelten szükségessé tett.

A FÖLDRENGÉSEK KÖZVETLEN HATÁSAI AZ ÉPÍTMÉNYEKRE

Az épületek tervezésénél általában fő szempont a vertikális terhek elleni ellenálló képesség, így az előírásoknak megfelelően megépített építmények saját súlyuk mellett a beltéri és a csapadékból adódó esetleges külső terheknek is biztosan ellenállnak. A földrengések esetén a problémát azonban a rengéshullámokból eredő és épületszerkezetekre ható oldalirányú talajmozgás okozza. A hirtelen fellépő horizontális terhelés következménye legtöbb esetben az épület összeomlása, totális pusztítást okozva. A földrengéshullámok gyakori jellemzője - főként a puhább talajrétegek esetén - hogy több hullámban érkeznek, ami a masszívabb, ellenállóbb épületszerkezetek tartószerkezetinek teherbíró képességét is még intenzívebben redukálja.

Az elsődleges veszélyt tehát a földrengéshullámok vízszintes irányú gyorsulása okozza, mivel a teherhordó szerkezetekben nyírófeszültségeket hoznak létre, ami sok esetben az épületszerkezeteket nem lehet megfelelően méretezni. A másik, közvetlen károsodást kiváltó fizikai tényező a rezgés frekvenciája, amelyek általában 0 és 15 Hz közé tehetőek. Az épület akkor van kitéve a legnagyobb terhelésnek, ha a maximális rengés frekvencia megegyezik az épületek sajátfrekvenciájával, mivel ilyenkor rezonancia generálódik, ami nagy rezgés amplitúdót eredményez. [1]

Számos esetben fordult már elő, hogy az épület összeomlását a földrengéshullámok mellett az épületre ható túlterheltség okozta, (utólag beépített emelettel, elválasztó falakkal, körbe épített teraszokkal, belső raktározással stb.). Ez a probléma sokszor a földrengésálló épületek összedőléséhez is közvetlenül hozzájárul, mivel a plusz terhek meghaladták az épületszerkezet méretezéséből adott határokat. Bizonyított tény, hogy a túlterhelt épületszerkezetek jelentő mértékben sebezhetőbbek földrengésekkor, sok esetben az épület összedőlését egy kisebb, ugyanakkor az előzőekhez képest más irányból érkező utórengés, vagy a rezgések frekvenciájának változása okozza.

Az eddigi bekövetkezett földrengéskárok tapasztalati alapján az épületek gyors, „kártyavárszerű” összeomlásának további oka lehet, hogy az alsóbb szinteket magasabb belmagassággal és kevesebb teherhordó fallal, vagy oszloppal tervezték, amelyek a földrengéshullámok érkezésekor elsőként vesztik el teherhordó funkciójukat az egész épület teljes pusztulását következményezve. Emellett, rendkívül fontos a talaj keménység és az

alapozás helyes megválasztása is, mivel főként magasabb, több emeletes tömbházaknál jelentkezhet, hogy a puhább talaj futóhomokszerűen képes porladni a rezgések hatására.

Az épületek szerkezeti hiányosságai mellett a földrengéskárok általános oka az építőanyagok nem megfelelő megválasztása is. Hogy csak két releváns példát említsek, 2008-ban, a nyugat-kínai Szecsuan tartományban kipattanó, valamint a 2009-es észak-olaszországi L'Aquila városában pusztító földrengés által okozott jelentős épületkárok oka az előírásoknak nem megfelelő konstrukciók és anyagok használata volt. A mentésben résztvevő tűzoltók elmondásai szerint, olyan teherhordó szerkezetek zúzódtak porrá a földrengést követően, amelyek eltávolítására általában fűrészt vagy más speciális vágószerszámot kellett használjanak. Ebből arra lehetett következtetni, hogy sok építkezésnél - költségmegtakarítás céljából - a betonelemeket a cement magas ára miatt homokkal pótoltak ki, amik a rezgések hatására rövid időn belül szétporladtak.

A földrengésálló, rugalmas tulajdonságú építőanyagok használatának kulcsfontosságát már évszázadok óta ismerik a különösen veszélyeztetett térségekben élők, a következőben ezek részletes bemutatására is sor kerül.

A FÖLDRENGÉSÁLLÓ ÉPÍTKEZÉS MÚLTJA

Ahogyan az előbbiekben említettem, egyes területeken már évszázadok óta fontos szempontként kezelik a földrengés ellenálló képességet az építkezések során. Földünk szeizmikusan legaktívabb térségében, a Csendes-óceán partjainál szélesen, sávszerűen húzódó cirkumpacifikus övezetben található Fülöp-szigeteken már a XV. századtól tudatosan építkeztek a földrengésekre készülve. A helyiek által *„bahay-na-nipa"*-nak vagy *„bahay kubo"*-nak nevezett, többnyire egy légterű bambuszból épült és nádtetővel fedett kunyhók jelesre vizsgáztak az igen intenzív, 7-8-as magnitúdójú földrengések esetén is. A kunyhók tetejét egy fából épített dúcszerkezet a bambuszból készült könnyű falaktól függetlenül tartotta, ami ily módon megfelelő rugalmasságot és ingást tett lehetővé a földrengéseknek ellenállóvá téve az építményt. Később, a nagyobb településeken ugyanezt az elvet követve már masszívabb fagerendákból épített és cseréptetővel fedett házakat kezdtek a szigeteken élők építeni, ami kiszélesítette azok kihasználásának és funkcionális lehetőségeit.

A helyi építési kultúra fejlődésének, és az idegen telepeseknek is köszönhetően a városokban a nipa-kat fokozatosan felváltották a több szintes kőből és téglából épített „*bahay-na-batok"*, *(1. ábra)* amelyeknek - elődeik szerkezetén alapulva - masszívabb és merevebb szerkezetű kőfalai egy rugalmas faszerkezet beépítésével el voltak választva a tetőtől, így biztosítva azt, hogy a rezgéshullámok hatására ne omoljanak össze. A *„batok"* a mai napig biztonságos otthonként szolgálnak a Fülöp-szigeteken élők számára. [2]

1. ábra. „Bahay-na-bato" lakóház modern változata a Fülöp-szigeteken Forrás: http://www.bokkins3d.blogspot.hu/2008/03/bahay-na-bato.html Letöltés ideje: 2012.08.14.

KORSZERŰ FÖLDRENGÉSÁLLÓ ÉPÍTÉSI TECHNOLÓGIÁK

A földrengésálló építkezés alapja az építőanyagok megfelelő megválasztása. Az intenzív rezgéshullámoknak a rugalmas anyagok - mint a fa és az acél - ellenállnak, a tégla és a beton viszont egyáltalán nem biztosít megfelelő rugalmasságot, ami az esetek többségében épületszerkezet összeomlását eredményezi. Ismét felhozható példának az észak-olaszországi L'Aquilában pusztító, 6,3-as magnitúdójú - nem kivételesen nagymértékű energia felszabadulással járó - földrengés, amelynek következtében csaknem 70.000 ember vált hajléktalanná. A magas kár fő oka a sok merev építőanyagból készült lakóház és műemlék épület volt *(2. ábra)*, az újraépítés során már könnyűszerkezetes épületeket építettek. *[3]* A közép- és kelet-európai térségben, így hazánkban is jelentős a tégla és betonépítésű lakóházak aránya, míg a világ más tájain a könnyű acélszerkezetes építmények száma rohamosan terjed, szem előtt tartva a földrengések általi veszélyeztetettség mértékét, valamint az erre vonatkozó nemzetközi irányelveket és szabályozásokat.

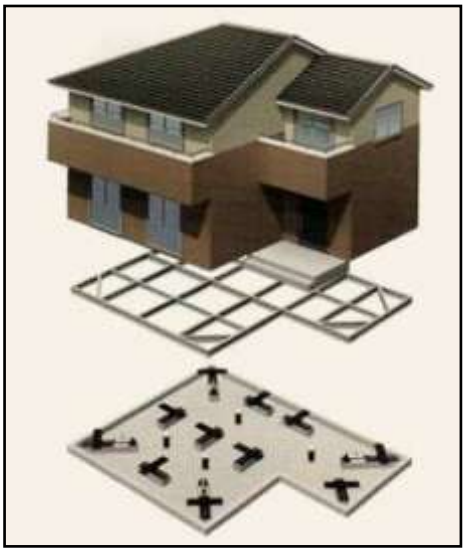
2. ábra. Santa Maria Suffragio templom romjai a 2009-es l'aquilai földrengést követően
Forrás: http://www.i-italy.org/bloggers/8564/invisible-victims-abruzzo-earthquake
Letöltés ideje: 2012.08.14. (Készítette: Samuele Pellecchia)

Hogy említsünk pozitív példát is, az építési technológia fontosságát kiválóan demonstrálja a 2011. március 11-i, 9-es magnitúdójú japán földrengés, ahol a megfelelő építési technológiának köszönhetően az épületek szerkezetében csak a legritkább esetben keletkezett komoly kár. Az, hogy ennek ellenére óriási pusztítást szenvedett el a „felkelő nap országa", a földrengés másodlagos hatásaként jelentkező szökőárnak volt köszönhető, ami ellen nem létezik technológiai eljárás.

A következő kép *(3. ábra)* egy klasszikus japán földrengésre tervezett lakóházat szemléltet. A biztonság és statikai tulajdonságok mellet a formatervezés is hangsúlyt kap az esetek többségében.

3. ábra. Földregésálló könnyűszerkezetes lakóház Japánban
Forrás: http://kp.hu/mibol-epitkeznek-a-japanok-mitol-foldrengesbiztos-egy-haz/
Letöltés ideje: 2012.08.12.

A védekezést tekintve két földrengésálló technológiai megoldás ismert, amely alapján létezik a rezgésálló megoldással épített ház, amikor az építménybe rugalmas teherbíró szerkezetek kerülnek beépítésre, valamint a földrengés szigetelés *(4. ábra),* mely esetben a talapzatba beépített acélszerkezet biztosítja a szeizmikus energia elnyelését. A különböző konstrukciós megoldásoknál fő szempont, hogy a talapzatot és az alapozást nem szabad egybeépíteni, mivel így megelőzhető, hogy a rezgések direkt átadódjanak a ház szerkezetére. A hatékonyság fokozása érdekében a két eljárás kombinálása is adott, mint lehetőség. A világon elterjedt védekezési építési megoldás, a könnyű acélszerkezetes technológia részletes bemutatására a következő fejezetben kerül sor. *[3]*

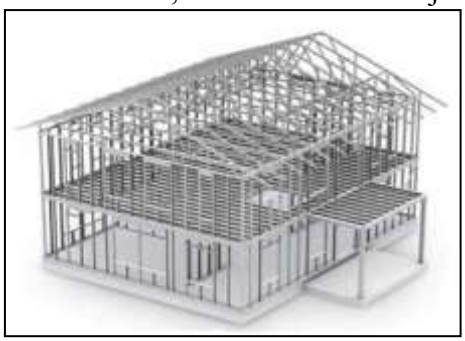


4. ábra. Földrengésálló szigetelés
Forrás: http://kp.hu/mibol-epitkeznek-a-japanok-mitol-foldrengesbiztos-egy-haz/
Letöltés ideje: 2012.08.14.

A könnyű acélszerkezetes technológia, mint a földrengéskárok elleni védekezés első számú lehetősége

Az eddigiekben tárgyaltak alapján megerősíthető, hogy az egetlen korszerű építőanyag a földrengésálló épületek létrehozására az acél. Az acélszerkezet jellemzője, hogy még a fánál is könnyűszerkezetesebb, ami annyit jelent, hogy egy azonos statikai mutatókkal rendelkező acélgerenda jóval kisebb súlyú (kb. 1/7), mintha fából készült volna.

Felépítésüket tekintve az acélszerkezetes épületek *(5. ábra)* falai vázszerkezetből állnak össze, amely közé hőszigetelő anyagok kerülnek beépítésre. Értelemszerűen a hőszigetelő anyagok szerepe a hőátbocsátás csökkentése, míg a hidegen hengerelt vékonyfalú acél U és C profilokból szerelt vázszerkezetnek statikai, teherhordó funkciója van. [4.]



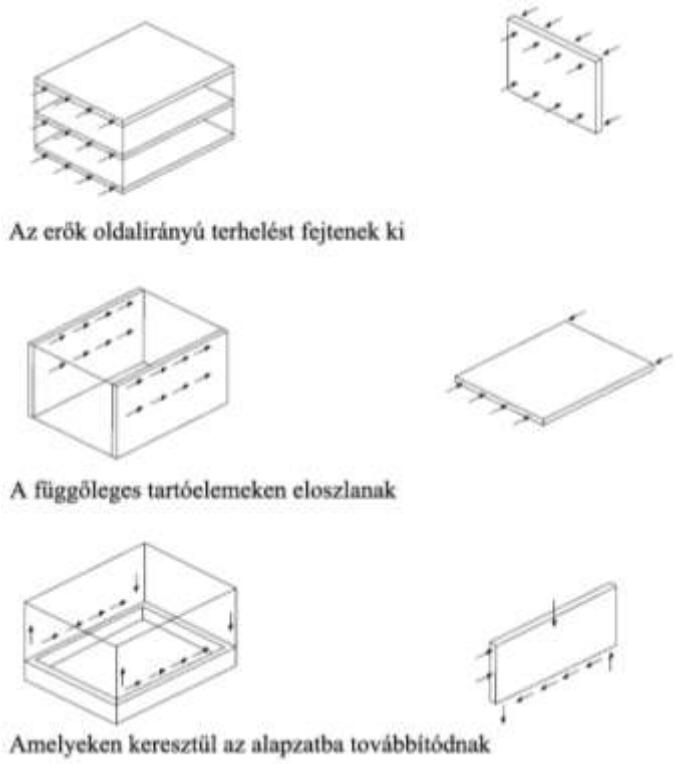
5. ábra. Acélszerkezetes épület szerkezeti rajza
Forrás: http://samarasbau.hu/wp-content/uploads/2012/01/acelszerkezetes-haz.jpg
Letöltés ideje: 2012.08.14. Készítette: nincs megnevezve

A könnyű acélszerkezetes házak száma ma már meghaladja a hagyományos építőanyagokból készül házakét a világon, mivel földrengés ellenállóságuk mellett számos más előnnyel rendelkeznek: [1]

- az acélszerkezet profiljainak gyártása során nem keletkezik hulladék,
- az egyes elemeket nem kell vegyszerrel kezelni (szemben a faszerkezettel),
- a szerkezet nem vetemedik a hőmérséklet és az öregedés hatására,
- az elemek nagy méretpontossággal gyárthatóak,
- környezetbarát megoldás, mivel nem kell fákat kivágni, alapanyaga újrahasznosítható,
- az acélszerkezet nem tűzveszélyes, valamint a bogarak és kártevők nem tudják károsítani.
- a szerkezetek könnyű súlya miatt egyszerűbb és olcsóbb a szállíthatóságuk.

A földrengésálló acélszerkezetes épületek jellemzői

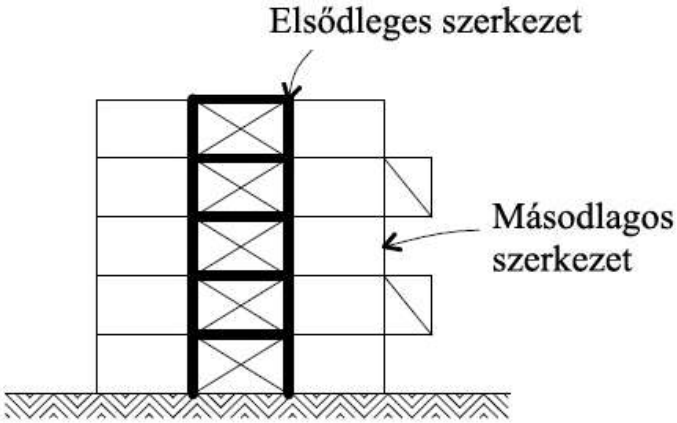
A könnyű acélszerkezetes építmények esetén a merev és ellenálló vízszintes épületelemek lehetővé teszik minden emeleten, hogy a horizontálisan ható erők szétszóródjanak a merőlegesen kapcsolódó függőleges szerkezeti elemeken, illetve válaszfalakon. A függőleges épületszerkezetek az így érkező erőhatásokat (pl. nagy erejű rezgéseket) az alapzatba továbbítják, a következő ábrán vázolt módon. [5]



Elsődleges-másodlagos szerkezetek

A védekezőképesség fokozása érdekében a függőleges acél tartóelemekbe beépítésre kerülhet egy ún. „elsődleges szerkezet”, melynek fő funkciója az összes földrengés terhelés elvezetése, és egy „másodlagos szerkezet”, amely csak a nehézségi erőkből származó terhek viselésére van tervezve. A másodlagos váz hosszanti ellenálló képessége és merevsége nem haladhatja meg az elsődleges szerkezet 15%-át, emellett a tervezésnél figyelmet kell fordítani a másodlagos szerkezet elsődlegeshez való csatlakozásainak illeszkedésére, a

földrengéshullámok okozta eltolódások esetén. Az említett szerkezeti felépítést az alábbi ábra *(6. ábra)* illusztrálja. [5]



6. ábra. Acélszerkezetes épület szerkezeti rajza
Forrás: http://www.arcelormittal.com/sections/fileadmin/redaction/4-Library/1-Sales_programme_Brochures/Earthquake/Earthquake_EN.pdf Letöltés ideje: 2012.08.14.

Az alapzatnak biztosítania kell, hogy földrengés esetén, a talajból érkező rezgéshullámok az épület egészén egyenletesen oszlódjanak el. Másik funkciójuk, hogy a talaj süllyedése esetén is megfelelő tartást biztosítson az épületnek, ami egyaránt elérhető sík- és mélyalapozással is. Cölöpök vagy lábazat beépítése esetén fontos, hogy a stabilitás érdekében a cölöpök kötőgerendákkal, vagy lemez alappal egymáshoz legyenek rögzítve.

Toronyházak földrengésvédelme

A lakóházak, felhőkarcolók, hidak és vasúti pályák földrengésálló építészeti megoldásainak alkalmazásában Japán világelsőnek számít, ami szoros összefüggésben van a szigetország magas veszélyeztetettségével és technológiai fejlettségével. Az egyszerű lakóházak földrengésekre való méretezését viszonylag egyszerűbb előírások szabályozzák, a 60 méternél magasabb építmények esetén már jóval bonyolultabb ellenőrzési folyamatok és számítógépes szimulációk alkalmazása szükséges, ami lehetővé teszi a több száz méter magasságú és extrém formájú felhőkarcolók földrengés állósági modellezését is. Az építmények méretezésénél egyaránt figyelembe kell venni a gyakoribb vízszintes és kevésbé gyakori függőleges szeizmikus hullámok általi terhelést is.

Földrengésálló tartószerkezetek magasépítésnél

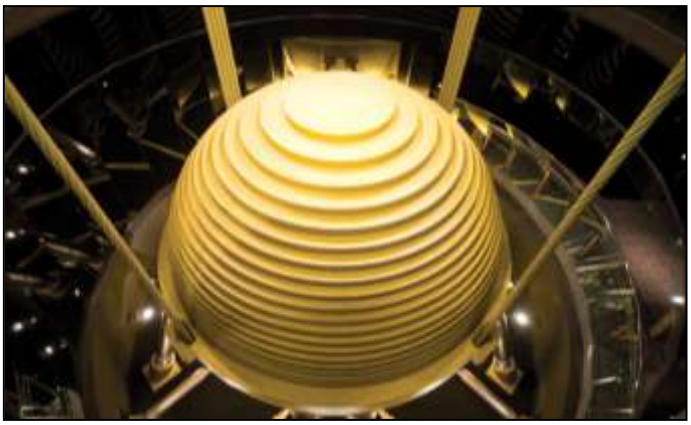
A kis elmozdulást lehetővé tevő merev vasbeton szerkezetekkel szemben a korszerű magasházak a már tárgyalt könnyű acélszerkezetes technológiával, szeizmikus csillapítóelemek beépítésével épülnek nem csak Japánban, hanem szerte a világban. A csillapító elemeknek hála, a rezgések elnyelődnek a szerkezeti elemek nagyobb elmozdulása mellett. Ezzel magyarázható az a jelenség, amikor egy intenzívebb földmozgás eredményeképpen a magas épület akár több méter kilengés mellett is biztosan ellenáll a rengéseknek, valamint az épületben jóval kisebb rezgés érzékelhető az elnyelődésnek köszönhetően.

A rengés-csillapítás elérése érdekében bevált technológiai eljárás a csillapító-falak beépítése az egyes szintek közé. Erre például szolgál a Tokióban található Roppongi Hills felhőkarcoló.

A csillapító elemeknél hatékonyabb, ugyanakkor költségesebb megoldás a szeizmikus szigetelők használata, ami nem befolyásolja az alaprajzi és homlokzati tervezést. Az alaptól a falszerkezeteket elválasztják, vagy az épület magasságát megosztják legalább egy köztes szinttel, ami lehetővé teszi, hogy földrengés esetén az épület egyes részei egymástól

függetlenül mozogjanak. Ezen eljárás a toronyházak mellett kiemelten fontos rendeltetésű épületeknél is alkalmazzák a biztonság fokozása érdekében. Ilyen szeizmikus szigetelők kerültek alkalmazásra például a Shiodome Sumitomo bankház épületénél, ugyancsak Japánban.

A földrengésvédelemre felsorolt főbb technológiák mellett léteznek alternatív, azonban költséghatékonynak nem nevezhető megoldások is. Példának okáért a Taiwanon található Taipei 101 nevezetű, 106 szintes felhőkarcoló stabilitását egy csaknem 730 tonnás inga (7. ábra) biztosítja, ami kiegyenlíti és csillapítja a földrengések okozta kilengéseket és rezgéseket. Az épület tetejébe beépített hatalmas „acélgolyó” mindig a kilengéssel ellentétes oldalra mozdulva minimalizálja az elmozdulást. [6]



7. ábra. A Taipei 101 toronyház kilengés csillapító ingája Forrás: http://mathspig.wordpress.com/category/popular-posts/cool-formula-for-calculating-skyskraper-sway/ Letöltés ideje: 2012.08.14.

A földrengések elleni építészeti megoldások tisztázásnál említésre került az alapozás jelentősége, ami a magas építésű épületekre is elmondható. Az acélszerkezetes toronyházak, középmagas épületek és hídszerkezetek építésénél világszerte alkalmazott ún. „földrengés-szigetelő pogácsák”, azaz lengéscsillapítók feltalálása Tarics Sándor (olimpiai bajnok vízilabdázó, építészmérnök professzor) nevéhez fűződik, aki nem mellesleg a világ jelenleg élő legidősebb olimpiai bajnokának mondhatja magát. A tarics-féle pogácsák energia-elnyelő hatása jóval hatékonyabbnak bizonyult, mint az ugyancsak az alapzatban épített bármelyik másik rugós, vagy gumis megoldás. Többek között ez a konstrukció biztosítja a San Franciscóban található Golden Gate-re felvezető autópályákat és felüljárókat, valamint hazánkban Paksi Atomerőmű kiemelten veszélyeztetett építményeit is. [7]

A továbbiakban nézzük, hogy milyen egységes szabványrendszer szabályozza az Európában, így hazánkban is épülő építmények földrengés állósági méretezési és tervezési szempontjait.

A Eurocode 8

A Eurocode 8 (MSZ EN 1998) egy olyan Európai Uniós szabványcsomag, melynek alapelve, hogy az adott épület típust olyan földrengésre kell tervezni, ami 50 év leforgása alatt 10%-os valószínűséggel fordulhat elő. A teherbírási követelmények alapján az építmény nem dőlhet össze a rengéstől, egyes épületeknek pedig a károsodási mértéke is meg van határozva. Ez esetben az épületszerkezet nem amortizálódhat jelentősen egy olyan földmozgás esetében, amelynek előfordulási lehetősége 10 év leforgása alatt 10%. A szabványcsomag három fő célja a következő: [8]

- az emberi életek megóvása,
- a károk mértékének csökkentése,
- és a kiemelt fontossággal rendelkező építmények funkciójának védelme.

Az Eurocode 8 hazánkban 2009. január 1. óta van érvényben, felépítését tekintve az alábbi szabványokból épül fel: [9]

- EN 1998-1 - magasépítési szerkezetek
- EN 1998-2 - hídszerkezetek
- EN 1998-3 - kárfelmérés és helyreállítás
- EN 1998-4 - silók, tartályok és csővezetékek
- EN 1998-5 - alapok, támaszszerkezetek
- EN 1998-6 - tornyok, kémények

Épületszerkezetek földrengésekre való méretezése

Az eddigiek alapján megállapítható, hogy az egyes épületek földrengésbiztos építése a helyes anyag és módszer megválasztásán, valamint a szerkezet megfelelő méretezésén múlik. Utóbbi részletes ismertetésére a következő pontokban kerül sor.

A tervezési válaszspektrum

A Eurocode 8 alapján a földrengésálló szerkezetek tervezésének alapja a tervezési válaszspektrum, amely egy adott frekvencián várható szeizmikus aktivitás hatását a frekvencia függvényében adja meg. A válaszspektrum meghatározása 4 lépésből tevődik össze: [9]

1. az építési terület szeizmikus zóna besorolásának meghatározása (pl. a szeizmikus zónatérképről) *(1. melléklet)*
2. a talaj típusának és talajmechanikai jellemzőinek meghatározása (A,B,C,D,E, S1,S2) *(2. melléklet)*
3. szeizmikus együtthatók meghatározása
4. válaszspektrum kiértékelése és grafikonos ábrázolása

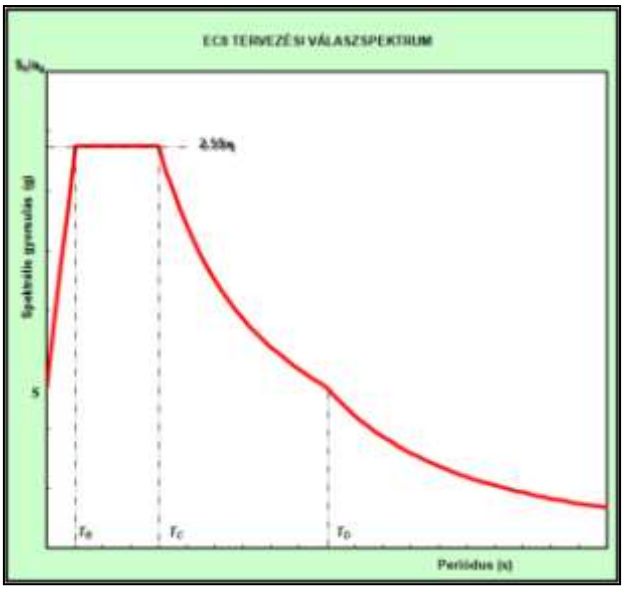
A tervezési válaszspektrum az épületszerkezet valós válaszait, illetve gyorsulásait megadó diagram, amely alapján az alábbi képlet segítségével meghatározható a földrengési teher nagyságának felső értéke a szerkezet tömegének és a válaszspektrum megfelelő értékének szorzatából:

$$Fb=mxSd(T1)$$ (tömeg x gyorsulás=erő)

ahol:

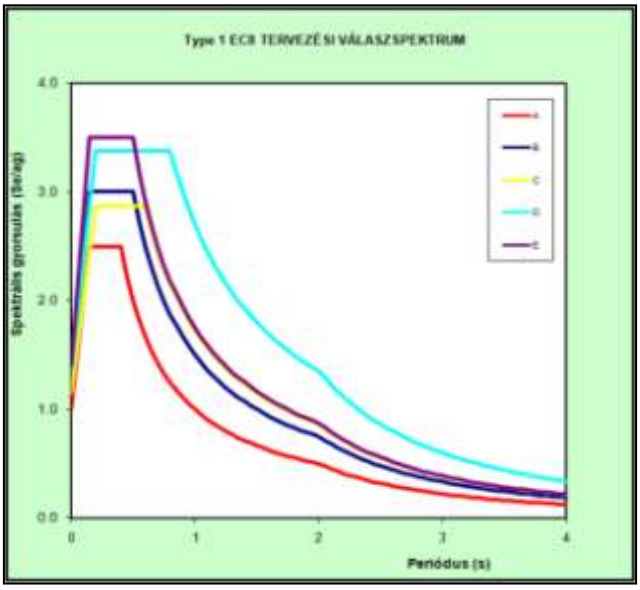
m: tömeg
Sd: válaszspektrum
T1- alaprezgési periódusidő (vízszintes mozgás esetén)

A kiértékelésnél a válaszspektrum függőleges és vízszintes összetevőjét is meg kell határozni, mivel földrengéskor a gyorsulásnak vertikális és horizontális (általában ez a pusztítóbb) komponense is van. Ez alapján az MSZ EN-1998-1 (Eurocode 8) vízszintes tervezési válaszspektrumát az alábbi diagramból *(1. diagram)* lehet kiszámítani a spektrális gyorsulás és periódus függvényében. [1]



1. diagram. Az Eurocode 8 vízszintes tervezési válaszspektruma Forrás: http://www.foldrenges.hu/index.php?option=com_content&view=article&id=94:magyarorszag-foeldrenges-veszelyeztetettsege&catid=5:geofizika&Itemid=7 Letöltés ideje: 2012.08.14.

A fenti diagramnak megfelelően az A, B, C, D, E talajtípusok esetén a tervezési válaszspektrum a következő ábra *(2. diagram)* szerint alakul.



2. diagram. Az Eurocode 8 vízszintes tervezési válaszspektruma Forrás: http://www.foldrenges.hu/index.php?option=com_content&view=article&id=94:magyarorszag-foeldrenges-veszelyeztetettsege&catid=5:geofizika&Itemid=7 Letöltés ideje: 2012.08.14.

A válaszspektrum függőleges komponensét a diagram alapján a következő lépésekben, az értékek behelyettesítésével lehet meghatározni:

$$0 \le T \le T_B : S_{ve}(T) = a_{vg}.\left[1 + \frac{T}{T_B}(\eta.3{,}0 - 1)\right]$$

$$T_B \le T \le T_C : S_{ve}(T) = a_{vg}.\eta.3{,}0$$

$$T_C \le T \le T_D : S_{(ve)}(T) = a_{vg}.\eta.3{,}0.\left[\frac{T_C}{T}\right]$$

$$T_D \le T \le 4s : S_{ve}(T) = a_{vg}.\eta.3{,}0.\left[\frac{T_C.T_D}{T^2}\right]$$

Ahol az MSZ EN-1998-1-ben meghatározott 1. típusú spektrum esetén:

$a_{vg}/a_g = 0{,}9$

T_B (s) = *0,05*

T_C (s) = *0,15*

T_D (s) = *1,0*

MAGYAR VONATKOZÁSOK

Hazánk földrajzi elhelyezkedése a természeti katasztrófák szempontjából szerencsésnek mondható, mivel a jelentős törésvonalak nagy távolsága miatt nem kell számolni gyakori, nagy intenzitású földrengéssel. Azonban, az elmúlt évtizedek során, az országban néhány esetben akár 5-6 magnitúdójú rengés is tapasztalható volt. Ezen földmozgások előfordulása teljesen rendszertelen területi eloszlásban következik be, egyes régiókban folyamatosan erősebb szeizmikus intenzitás mérhető. Ilyen például Komárom, Dunaharaszti, Mór és Eger térsége, amit a mellékelt szeizmikus zónatérkép *(1. melléklet)* jelöl. Az alacsony gyakoriságú előfordulással szemben a várható pusztítás mértéke miatt a kockázat azonban így is jelentős mértékű. Ezt tovább fokozza, hogy az ország területét nagyrészt laza üledékes kőzetek borítják, amelyek könnyedén átengedik, illetve felerősítik az - épületkárokért legnagyobb mértékben felelős - alacsony frekvenciájú rezgés hullámokat. Az üledékes talaj mellett, az országban jelentős mennyiségben épített merev épületszerkezetek (tégla- és betonépítésű lakóházak, egyéb építmények) azok, amik a földrengéskockázatot tovább fokozzák. A tapasztalatok alapján a vasbeton szerkezet, illetve a doboz szerű forma miatt egyes épületek ugyan jobban ellenállnak a rengéseknek, mint a téglából készült épületek, azonban a biztonságos szint eléréséhez nem elégséges módon, amit alátámaszt az 1977-es romániai, Richter-skála[1] szerinti 7,2-es erősségű földrengés, aminek következtében rengeteg panelépítésű vasbetonház omlott össze. A Eurocode 8-nak köszönhetően az elmúlt néhány évben már jelentős mértékben előtérbe kerültek a földrengés biztonsági szempontok az épületek tervezése során, azonban főként az ország nagyvárosaiban nagy számban található, régi, akár 100-150 éves életkort is meghaladó polgári épületek veszélyeztetettsége kritikus. Az MTA Geodéziai és Geofizikai Kutató Intézet kutatóinak álláspontja szerint, amennyiben Budapestet egy Richter-skála szerinti 7-e erősségű földrengés érné, a zsúfolt, sűrűn beépített belső kerületek esetén a károk felbecsülhetetlen mértékűnek prognosztizálhatóak. A többségében a 100 éves életkort is meghaladó bérházak nagy része minden bizonnyal a földdel válna egyenlővé egyrészt az elavult, merev építési technológia, másrészt az évtizedek során a válaszfalak sokszori átrendezése miatt, ami az épület statikai teherbíró képességét csökkenti. Sok régi templom is várhatóan összeomlana, viszont köszönhetően annak, hogy a parlament kupoláit könnyű acélszerkezet tartja, képes az intenzívebb földrengéseknek is

[1] Richter-skála: A földrengések energiájának a pontos megállapítására bevezetett skála, mértékegysége a magnitúdó (M) *[10]*

ellenállni. A kutatók véleménye alapján emellett jelentős károkat szenvedne a főváros közműhálózata is, mivel az öntöttvas víznyomócsövek és elöregedett gázcsövek rövid ideig tudnának csak ellenállni a földrengéshullámok okozta terhelésnek. [11]

Saját véleményem szerint az óriási károk bekövetkezéséhez nem szükséges 7-es magnitúdójú rengés, egy intenzívebb, 5-6-os erősségű csapás - aminek előfordulása reális veszély lehet az elkövetkezendő évtizedekben, vagy akár évek ben is - hatására is rengeteg épület szenvedne jelentős pusztítást, és minden bizonnyal a halálesetek száma is kirívóan magas lenne. Az ország jelenlegi gazdasági helyzetét és a költségvetési korlátait is figyelembe véve egyre aktuálisabb lenne egy olyan átfogó terv, illetve koncepció elkészítése, amelyben amellett, hogy megfogalmazódik az, hogy hogyan lehetne költséghatékony módon Budapest belvárosának földrengésbiztonságát növelni az előfordulás várható kockázatán alapulva, olyan építészeti tendenciát irányozna elő, ami a jövőre való tekintettel országos szinten. jelentősen hozzájárulna a földrengéskockázatok csökkentéséhez. A koncepció alapjául szolgálhat az EUROCODE 8 szabványcsomag, a könnyű acélszerkezetes építészeti megoldások, valamint a nemzetközi tapasztalatok.

ÖSSZEGZÉS

Az eddigi földrengés katasztrófák tapasztalati alapján bebizonyosodott, hogy a védekezés leghatékonyabb módja az építészeti technológiában rejlik, amelyre vonatkozóan fő szempontként említhető az építőanyag megfelelő megválasztása és a szerkezeti felépítés. A biztonsági szempontok mellett, a különböző fejlettségű országok lehetőségeit is figyelembe véve szem előtt kell tartani a költséghatékonyságot is, ezért az Európai Uniós szabályozás irányelvei alapján is a földrengésálló építkezésnek és tervezésnek célszerűen összhangban kell lennie a veszélyeztetettség mértékével, amit földtani és statisztikai mérésekkel és adatokkal lehet meghatározni. Mivel bizonyítást nyert, hogy a tégla- és betonépítésű lakóházak vesztik el teherbírásukat leghamarabb és dőlnek össze földrengés esetén, célszerű az építkezéseknél a rugalmasabb anyagok, mint az acél vagy akár a fa használata. Japánban is - amely etalonnak számít a földrengések elleni építészeti fejlesztések terén - a lakóházak többsége acél könnyűszerkezetes megoldással épült.

Magyarország földrengés veszélyeztetettsége nem indokolja a jelenlegi építészeti irányzatok gyökeres megváltoztatását, azonban a pusztítás várhatóan nagy mértéke miatt jelentős kockázattal kell így is számolni, ami egyértelműen szükségessé teszi a régi épületeink földrengésbiztonsági szempontból való felülvizsgálatát, illetve korszerűsítését a kritikus infrastruktúrákkal egyetemben.

Felhasznált Irodalom

[1] Földrengés hatása épületekre, HUN-Reng Magyarország Földrengés Információs Rendszere
http://www.foldrenges.hu/index.php?option=com_content&view=article&id=20:foeldrengesek-hatasa-epueletekre&catid=1:altalanos-fogalmak&Itemid=23
Letöltés: 2012.08.12.

[2] Augosto F. Villalon: Are heritage buildings earthquake-proof? Philippine Daily Inquirer, 2011.03.28.
http://lifestyle.inquirer.net/artsandbooks/artsandbooks/view/20110328-327971/Are-heritage--buildings--earthquake-proof *Letöltés: 2012.08.12.*

[3] Miből építkeznek a Japánok? Mitől földrengésbiztos egy ház? Készház portál, 2011.03.13. http://kp.hu/mibol-epitkeznek-a-japanok-mitol-foldrengesbiztos-egy-haz/
Letöltés: 2012.08.12.

[4] Acélszerkezetes készházak, Samarasbau építéstechnológia
http://samarasbau.hu/acelszerkezetes-keszhazak/ *Letöltés: 2012.08.12.*

[5] Earthquake Resistant steel structures, ArcelorMittal
http://www.arcelormittal.com/sections/fileadmin/redaction/4-Library/1-Sales_programme_Brochures/Earthquake/Earthquake_EN.pdf *Letöltés: 2012.08.12.*

[6] Várhelyi Judit: Tokióban a helyzet - Építészet és természeti katasztrófák, Építészfórum, 2011.08.19. http://epiteszforum.hu/node/19412 *Letöltés: 2012.08.12.*

[7] Magyar találmány óvta meg a nagyobb tragédiától Japánt, hirado.hu, 2011.03.20.
http://www.hirado.hu/Hirek/2011/03/20/19/Magyar_talalmany_ovta_meg_a_nagyobb_tragediatol_Japant.aspx *Letöltés: 2012.08.12.*

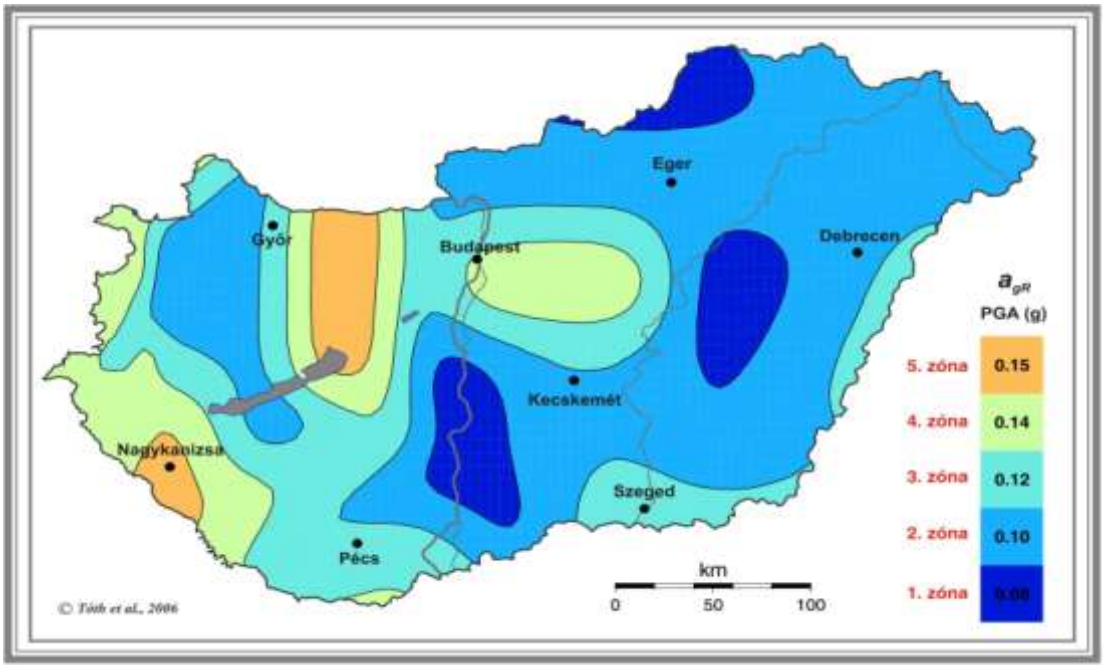
[8] Eurocode 8 - Földrengés, Eurocodes Expert
http://www.eurocodes.co.uk/EurocodeDetail.aspx?Eurocode=8 *Letöltés: 2012.08.12.*

[9] Tornai László (KÉSZ Zrt) előadása: A földrengésről mérnök szemmel, méretezés földrengésre, Budapest, 2011.12.16.
http://www.csmi-mernoki-kamara.hu/files/2011.12.16.%20-%20M%C3%A9retez%C3%A9s%20f%C3%B6ldreng%C3%A9sre.pdf
Letöltés: 2012.08.12.

[10] Magyar Larousse Enciklopédia III. kötet, Akadémiai Kiadó, Budapest, 1994 ISBN: 963-05-6748-2, a Richter-skála kifejezésre (478. o.)

[11] Földrengések Magyarországon és az épületek földrengés-biztonsága, Készház portál, 2011.01.29.
http://kp.hu/foldrengesek-magyarorszagon-es-az-epuletek-fodrengesbiztonsaga/
Letöltés: 2012.08.12.

Mellékletek



***1*. melléklet.** Magyarország szeizmikus zónatérképe Forrás: http://www.foldrenges.hu/images/stories/cikkek/images/TLfoldrengeskockazat4.jpg

Talaj típus	A rétegsor leírása	Jellemző paraméterek		
		$v_{s,30}$ (m/s)	N_{SPT} (ütés/30cm)	c_u (kPa)
A	kőzet vagy kőzetszerű geológiai formáció, beleértve legfeljebb 5 m gyengébb anyagot a felszínen	> 800	-	-
B	konszolidált, nagyon szilárd homok, kavics vagy agyag rétegek legalább több tíz méter vastagságban; a szilárdsági tulajdonságok a mélységgel fokozatosan javulnak	360 – 800	> 50	> 250
C	szilárd és közepesen szilárd homokos, kavicsos, agyagos rétegek, melyek vastagsága tíz métertől több száz méterig terjed	180 – 360	15 – 50	70 – 250
D	laza, közepes tartóképességű talaj rétegek	< 180	< 15	< 70
E	Olyan talaj profil, ahol a felső 5-20 méteren a v_s sebesség a C vagy a D talaj típusnak megfelelő, alatta pedig szilárdabb (v_s> 800 m/s) anyag található			
S_1	A felső rétegek között egy legalább 10 m vastag puha, képlékeny (PI>40), nagy víztartalmú agyag réteg található	< 100	-	10 – 20
S_2	Talajfolyósodásra hajlamos réteg(ek) fordulnak elő; minden olyan profil, mely nem sorolható az A-E vagy S_1 kategóriák valamelyikébe			

2. melléklet. A talajviszonyok osztályozása
Forrás: az MSZ EN 1998-1/ EUROCODE 8 szabvány 3.1. táblázata

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Dobák Imre
dobak.imre.@uni-nke.hu

BETEKINTÉS AZ ÁLLAMBIZTONSÁG 1960-70-ES ÉVEI NEMZETKÖZI TECHNIKAI KUTATÁS-FEJLESZTÉSI FOLYAMATAINAK SZERKEZETÉBE

Absztrakt

A szerző tanulmányában a szocialista állambiztonság időszakának egyes nemzetközi technikai kutatási kérdéseit veszi vizsgálat alá. Az áttekintett folyamatok hosszabb távon fontos szerepet játszottak a különböző operatív képességek megteremtésében. Az állandóan változó technikai környezet és kihívások mentén a nemzetközi együttműködési kapcsolatok meghatározták azokat a kutatási folyamatokat, amelyek a háború utáni technikai bázis színvonalának növelésére irányultak. A tanulmány célja a tudományos folyamatok bemutatásával hozzájárulni a szocialista állambiztonság sajátos eszközei és eszközrendszerei fejlődésének megértéséhez.

In this short essay the author examines some international technical research issues of the socialist state security period. The reviewed processes played important role in the creation of different operational capabilities in long term. Along the permanently changing technical environment and challenges, the relations of international cooperation have determined those research and development processes that helped to increase the quality of technical basis after the Second World War. The aim of this study is to contribute to understand the development of specialized equipments by presenting the scientific process in the state security era.

Kulcsszavak: *technikai fejlesztés, kutatás, állambiztonság, együttműködés ~ technical development, research, state security, cooperation*

BEVEZETŐ

A szocialista állambiztonság időszakában az egyes szakfeladatok végrehajtását támogató technikai kutatási és fejlesztési folyamatok fontos szerepet kaptak, amelyek jelentősége a külső technikai környezet fejlődésével párhuzamosan, az 1960-as évektől még nagyobb hangsúllyal kerültek előtérbe. A nemzeti szinteken rendelkezésre álló kutatási - fejlesztési képességek és kapacitások kihasználása, a folyamatosan bővülő, egyre mélyebb szakmai ismeretekkel rendelkező szakemberek részvétele mellett, azonban a többi szocialista országgal nemzetközi szinten megvalósított együttműködések is sajátos, jól szervezett felületet biztosítottak a technikai környezettel való lépéstartásra. Jelen tanulmány célja, hogy bepillantást engedjen az 1960-70-es évek célorientált mérnöki gondolkodását visszatükröző, nemzetközi kutatási és fejlesztési folyamatok belső szerkezetébe, amely emellett értékes ismeretekkel szolgálhat a téma nemzetközi viszonyainak megértéséhez is.

A korszak a hidegháború időszaka, amelyet (hadi)technikai értelemben is a szembenállás és rendkívüli verseny jellemzett. A külső biztonságpolitikai környezetben lezajlott események azonban a titkosszolgálati – állambiztonsági gondolkodás technikai aspektusainak fejlődését is felgyorsították. Ötven-hatvan évre visszatekintve a hazai állambiztonsági szervezetrendszer technikai-kutatási területeinek fontos feladatai között is megjelent a technikai eszközöket alkalmazó különböző szakterületek technikai feltételrendszereinek a megteremtése. A második világháborút követő években megörökölt, elhasználódott technikai eszközöket is alkalmazó titkosszolgálati – állambiztonsági szféra fejlesztési kérdései az 1950-es évektől kaptak igazi lendületet, amelynek legfőbb előmozdítói az európai szocialista országokkal kialakított állambiztonsági témájú bilaterális és multilaterális együttműködések voltak. „Lényegében a Varsói Szerződés létrejöttétől datálható a kommunista titkosszolgálatok közötti (bilaterális) kapcsolattartás rendszeressé tétele. Ezek jószerivel csak a hatvanas évek első harmadától lényegültek át – a szovjetek által koordináltan – tényleges multilaterális csapatmunkává”[1]. A vonatkozó együttműködések, illetve azok módosított megállapodásai egészen a rendszerváltás időszakáig végigkísérték az állambiztonság különböző technikai eszközöket alkalmazó szakterületeinek fejlődési irányait.

AZ EGYÜTTMŰKÖDÉS KERETRENDSZERE

Az operatív-technikai együttműködések jelentős állomásaként az 1960-as évek elejét kell megemlíteni, amikor is a magyar szervek munkatársai egy szakmai látogatás alkalmával betekintést kaphattak[2] az érintett szovjet állambiztonsági szervek munkájába. Az ez követő időszakban kialakult együttműködés, valamint az 1973-ban kötött általánosabb keret-megállapodás[3] (a Magyar Népköztársaság Belügyminisztériuma és a Szovjetunió Minisztertanácsa mellett működő Állambiztonsági Bizottság közötti 1973-ban kötött együttműködési egyezmény 1. cikkely 5 pontja, amely szerint a felek „együttműködtek operatív-technikai eszközök mintapéldányainak elkészítésében, az érvényben levő operatív-technikai együttműködési egyezményekben foglaltaknak megfelelően) megfelelő keretet biztosítottak többek között az egyes kutatási, fejlesztési tevékenységek összehangolására, a párhuzamosságok elkerülésére, valamint a szakterületek korszerű eszközökkel történő

[1]Gyarmati Gy. - A magyar humán hírszerzés átnyergelése a (mostoha)testvéri technikára Betekintő 2012/1. szám. http://www.betekinto.hu/ (Az Állambiztonsági Szolgálatok Történeti Levéltárának internetes folyóirata), letöltve: 2013.02.20.

[2] ÁBTL 1.11.8. 60-2035/60

[3] Lásd Krahulcsán Zsolt - KGB és III. Főcsoportfőnökség: egy kapcsolat vége…(?) (A szovjet–magyar állambiztonsági együttműködés szabályozása 1989-ben) Betekintő, 2007/4. száma, http://www.betekinto.hu, letöltve: 2013.02.20.

ellátását segítő tapasztalatcserére. Az operatív-technikai kérdésekben főként a kétoldalú kapcsolatok jelentették a technikai színvonal és módszerbeli, valamint alkalmazásbeli fejlődés lehetőségét, így a célok, tervek definiálására is a nemzeti szakmai igények mentén alapvetően a kétoldalú kapcsolatokban került sor[4].

A másik jelentős, sajátos technikai fejlesztéseket igénylő szakterület a rádióelhárítás[5] volt. A második világháborút követően lassan kibontakozó rádióelhárító tevékenység eredményességének fokozása kapcsán, az első nemzetközi szintű lépések az egyes szocialista országokkal való kapcsolatokra vezethetőek vissza, amelyek során pl. „1951 és 1954 között Csehszlovákiával, Lengyelországgal és Bulgáriával”[6] kötöttek a magyar szervek megállapodásokat. A multilaterális együttműködési kapcsolatok 1955-től jelennek meg az európai szocialista országok közös rádióelhárító szervezetének létrehozásával[7], amely központosított koordináló szerveként az ún. Koordinációs Központ[8] jelent meg. (Habár a belügyi rádióelhárítás és a katonai rádiófelderítés eltérő szervezeti keretek között fejlődött[9] az 1940-es évek végétől, a Varsói Szerződés időszakához köthető szakmai együttműködés mindkét területre erőteljes hatást gyakorolt.)

Anélkül, hogy részleteiben kitérnék az érintett belügyi nemzetközi együttműködés részleteire, annak fő feladatát képezte a rövidhullámú sávtartományban, a szocialista országok területén működő rádiósügynökök adásainak felderítése és iránymérése, amely tevékenységek csak korszerű és hatékony munkavégzést biztosító technikai eszközrendszerekkel és együttműködésben voltak biztosíthatóak. Ennek a tevékenységnek a szakmai irányítása, összehangolt technikai fejlesztési kérdései és folyamatai alkották azokat a kulcsterületeket, amelyek a szocialista országok rádióelhárító szolgálatainak együttműködésével alapjaiban biztosíthatták a közös szakmai feladatok teljesítését. A technikai – műszaki kérdések kiemelt szerepét és szakmai sajátosságait jelzi, hogy az együttműködésen belül – már a megalakuláskor - külön műszaki bizottság kerül kialakításra[10].

A nemzetközi technikai együttműködések keretében felmerülő kutatási – fejlesztési témaköröket ún. „témák” alá csoportosították, amelyek alapját képezték a számtalan különböző szakirányt felölelő fejlesztendő kérdéseknek. A „témák” alá csoportosított fejlesztések eredményei fokozatosan jelentkeztek, így a későbbiekben sor került a kutató és kísérleti – konstrukciós munkák során elkészült speciális technikai eszközök szállítási kérdéseinek rendezésére is.

Rendszeres találkozókon tekintették át a korábbi évek együttműködésének terveit és határozták meg a következő évek feladatait. Az érintett feladatok nagyságát és összetettségét jelzi, hogy az egyik ilyen 1970-es évekbeli szovjet-magyar találkozón például a szovjet fél részéről 50, a magyar fél részéről 19 téma és közös területként pedig 5 téma jelent meg az

[4] ÁBTL 46-2681/50/63 Jegyzőkönyv, valamint ÁBTL 46-4416/1963 Feljegyzés

[5] A rádióelhárítás és rádiófelderítés fogalmak közötti korabeli értelmezési különbség: 1. Rádióelhárítás - a felderített rádiós- ügynök vagy ügynökgyanús személy rádióállomása földrajzi helyzetének megállapítása. 2. Rádiófelderítés - állambiztonsági funkció. Feladata: a rövidhullámú frekvenciasávban felderíteni az ellenséges hírszerző szervek rádióközpontjait, rádiósügynökeit, ellenállomásait, valamint az ügynökgyanús és ismeretlen rádióállomásokat. ÁBTL 4.1 A-3036

[6] Borvendég Zsuzsanna - A BM II/16. Osztályának (Rádió-elhárítás) története és szervezeti felépítése 1945–1962 között - Betekintő – 2012/4. szám, http://www.betekinto.hu, letöltve: 2013.02.20.

[7] Az „európai népi demokratikus országok” rádióelhárító szolgálatai által 1955-ben kialakított, kezdetben varsói székhellyel működő nemzetközi együttműködés. ÁBTL, 1.11.8. 0024-20/9-55 (Jegyzőkönyv)

[8] Varsói Koordinációs Apparátus: a szocialista országok állambiztonsági szerveinek szerződésben vállalt kötelezettsége saját rádióelhárítási szerveik feladataira vonatkozóan. Forrás: Állambiztonsági Értelmező Szótár, http://hu.scribd.com/doc/47552737/Korabeli-allambiztonsagi-ertelmez%C5%91keziszotar (letöltve: 2013.02.10.)

[9] lásd: Imre Lajos – A hadászati rádiófelderítés a hidegháború éveiben 1946-1990, in: Felderítő Szemle, 2008. nov. VII. Évfolyam, 96 o., valamint Dr. Várhegyi István – A magyar rádiófelderítés működése a hidegháború éveiben 1945-1990, In: Felderítő Szemle, 2004. jún. III/2. szám, 133 o.

[10] ÁBTL, 1.11.8. 0024-20/9-55, Jegyzőkönyv

együttműködésben. Az 1970-es évek közepén zajlott másik megbeszélésen- amelyen Magyarországról két csoportfőnökség is képviseltette magát - az együttműködésbe a magyar Műszaki Fejlesztési Csoportfőnökség részéről 12, szovjet részről 13 téma, a magyar Operatív Technikai Csoportfőnökség részéről 10, szovjet részről 14, közös témaként pedig további 5 téma került bevonásra[11]. Az érintett témák a televízió, rádió és optika, valamint okmány, írás és szakértő témaköröket érintették.

Az együttműködések és ezen belül a kutatási-fejlesztési témák alatt megfogalmazott feladatok céljaként - relációtól függetlenül - többek között az alábbiakat láthatjuk:

- technikai eszközök, berendezések mintapéldányainak kifejlesztése;
- beszámoló elkészítése és másik félnek történő átadása az adott téma fejlesztéséről;
- technikai leírások adott témához kapcsolódó átadása a másik félnek;
- operatív technikai és elméleti kísérleti problémák megoldása;
- speciális technikai mintakészülékek cseréje;
- középtavú munkamegosztás;
- valamint tudományos és tapasztalatcsere.

Az operatív technikai irányú megállapodások keretében kitértek a felek közötti speciális technikai eszközök és anyagok szállításának lebonyolítására, valamint elszámolására is. Ennek lényege, hogy a megállapodások alapján a felek közvetlenül, a külkereskedelmi szervek közvetítése nélkül szállítottak egymásnak olyan speciális-operatív eszközöket és anyagokat, amelyeket a másik fél készített, a másik fél belső piacán vásároltak, vagy a másik fél a kapitalista külföldön vásárol.

Az egyes fejlesztési folyamatok szempontjából érdemes a rádiótechnikai fejlesztések azon folyamatát áttekinteni, amelyek a rádióelhárítás nemzetközi együttműködési feladatrendszeréhez kapcsolódtak. A szakterületet szélesebb nemzetközi formában koordinált fejlesztések jellemezték, amelyek sajátosságaiként jelentek meg, hogy az egyes témaköröket a nemzetközi szinten magvalósított rádióelhárítási feladatrendszer technikai rekonstrukciós munkáihoz igazodva határozták meg. A tagországokban kialakított, rendszerelemként értelmezhető eszközökkel kölcsönösen egészítették ki a rádióelhárítás nemzetközi rendszerének elemeit. Az adott témakör kutatásával foglalkozó adott ország fejlesztési területe a többi tagországai igényei alapján végezte az eszközök sorozatgyártását. Ezek gyakran azonban nem kizárólag belső fejlesztésekkel, hanem „külső” kutatóintézetek bevonásával zajlottak. Példaként említhető, hogy magyar rögzítő eszközöket biztosítottak a többi európai szocialista ország rádióelhárító szolgálatának.

A RÁDIÓELHÁRÍTÁS FEJLESZTÉSI FOLYAMATAINAK KERETRENDSZERE

A hazai rádióelhárítás történetében megjelenő főbb szakaszok közül a második világháborút követő években megjelenő, főként a fennmaradt haditechnikai eszközökre épülő első szakaszt[12] követő periódust (1955-től) tartjuk a szocialista együttműködés keretében megvalósított rádióelhárítás időszakának. Ezen a területen a vonatkozó kapcsolatokat a már említett széleskörű multilaterális együttműködés jellemezte, így a kutatási – fejlesztési kérdések és célok megfogalmazására is alapvetően a közösen működetett rendszerekhez illesztetten, központosítottan, koordinált módon került sor. A koordinálás szakmai okait az együttműködésben résztvevő állambiztonsági szolgálatok nemzeti szintű rádióelhárítási

[11] ÁBTL, 89-26-14/75 Jegyzőkönyv tanácskozásról

[12] az 1949-1955 közötti időszak (ÁBTL, 4.1 A-3168/1-5 (13-68/240/84) Állambiztonsági (Szolgálati) Ismeretek, 1984.)

területeinek egységes eszközellátása, a végrehajtandó feladatok és rendszerben való értelmezhetősége indokolta.

A vonatkozó tevékenységeket a speciális berendezések fejlesztésével és kidolgozásával kapcsolatos tudományos-kutató munkák, és kísérleti-konstrukciós munkák végrehajtási rendje[13] keretében szabályozták, amely részleteibe történő alábbi betekintés jól szemlélteti az egyes folyamatokat.

A szabályzat célja az volt, hogy meghatározza a rádióelhárító szolgálatok céljait szolgáló speciális készülékekkel kapcsolatos tudományos-kutató munkák és konstrukciós munkák rendjét az egyeztetett tervek és feladatok függvényében. A szabályozás (nem megjelenített) célja lehetett egyfelől a nemzetközi színterén jelentkező kutatási párhuzamosságok elkerülése, másfelől a rendelkezésre álló technikai – tudományos kapacitások hatékonyabb kihasználása is. A szabályzat - amely betartása kötelező érvényű volt minden együttműködésben érintett szolgálat számára - kimondta, hogy a tudományos kutató és kísérleti-konstrukciós munkát a felek önállóan, vagy egyesített erővel folytathatnak.

Az egyes szaktevékenységeket érintően két nagyobb elkülöníthető részt különböztettek meg, így az ún. tudományos-kutató munkát (TKM), valamint az ún. kísérleti-konstrukciós munkát (KKM).

Tudományos-kutató munka (TKM)

Ennek folyamatai alatt olyan tevékenységet értettek, amely rendszerint „tudományos beszámolóval és a kiválasztott megoldás helyességét alátámasztó készülék működő makettjének, vagy egyes elemeinek elkészítésével, valamint a kísérleti-konstrukciós munkákhoz szükséges taktikai-technikai követelmények elkészítésével ér véget".

Kísérleti-konstrukciós munka (KKM)

A kísérleti-konstrukciós munka megfogalmazása alatt olyan tevékenységet határoztak meg, amely az új technikai eszköz „kísérleti mintapéldányának létrehozásával kapcsolatos munkakomplexum elvégzését irányozta elő, a tudományos-kutató munka vagy korábban folytatott fejlesztések alapján. A kísérleti-konstrukciós munka a berendezés kísérleti mintapéldányának elkészítésével ért véget, amelyek a berendezések sorozatgyártásához szükségesek."

Az egyes fejlesztési munkák (tudományos-kutató és kísérleti-konstrukciós) megrendelőjeként mindig azon ország állambiztonsági szervének rádióelhárító szolgálata jelent meg, amely országban az adott munkát végezte. Ebben az esetben a munkákat „megrendelő" fél volt felelős az adott fejlesztések végrehajtásáért és annak különböző részterületeiért. Abban az esetben, ha a tudományos-kutató vagy kísérleti-konstrukciós feladatokban több tagország is részt vett, a rádióelhárító szolgálatok nemzetközi együttműködését koordináló központi szerv hatáskörébe került annak meghatározása, hogy melyik szolgálat került felelősként kijelölésre az adott feladat végrehajtásáért.

A szabályzat kitért arra is, hogy a tudományos-kutató vagy kísérleti-konstrukciós tevékenység kapcsán kik vehetnek részt a kivitelezési feladatokban. Ezek egyrészről az adott tagország szolgálatainak szakterületei, másrészről különböző tudományos-kutatóintézetek lehettek. Az adott fejlesztést megrendelő és azért felelős szolgálat döntése alapján egyéb, nem az állambiztonsági szférához kapcsolódó katonai, polgári intézetek, vagy vállalatok is bekapcsolódhattak a fejlesztési feladatokba „a titkosság szükséges mértékű betartásával". Az átfogó szabályzat keretén belül a megrendelő szerv kötelességeinél kerültek megjelenítésre az együttműködést koordináló központi szerv irányába jelentkező feladatok, így például az időszakos tájékoztatási kötelezettség („nem ritkábban mint 1-2 alkalom évenként"), a

[13] ÁBTL, 1.11.8. 00202/3K-72, Kivonat a KA XIII. Kibővített Tanácskozásának jegyzőkönyvéből

fejlesztések eredményeinek közös megtekintése, a kísérleti mintapéldányok „kipróbálási programjának és metodikájának” egyeztetése.

Mindezek mellett a szocialista országok nemzetközi szintű rádióelhárító együttműködésének központosítottságát mutatja, hogy a koordinációs szervezet fenntartotta magának a jogot, hogy ”évente legalább egyszer [….] megismerkedjen a fejlesztés állapotával”. További lehetőségei közé tartozott, hogy a fejlesztést végző szolgálattal összehangolva, bevonja más együttműködő szolgálatok szakembereit a fejlesztés bármely szakaszában az eredmények megtekintésébe és a technikai konzultációk folytatásába. A hivatkozott dokumentum jól mutatja, hogy az ún. Koordináció joga széles körben kiterjedt az egyes nemzeti szolgálatoknál folyó fejlesztési munkákban való betekintésre, és egyfajta ráhatással lehettek a fejlesztési folyamatokra is. A megállapítást támasztja alá a szabályzatnak azon része is, amely leírja, hogy abban az esetben, ha az adott nemzeti szintű rádióelhárító szolgálat által folytatott fejlesztési feladat nem megfelelő műszaki szinten folyt, „nem a szolgálatok közös érdekeinek megfelelő irányba halad” vagy akár „nem fejeződik be a tervbe vett határidőre” közvetetten beavatkozhattak és közös értekezlet keretében vitathatták meg a munka „sikeres befejezéséhez szükséges” intézkedéseket.

A fejlesztés napjainkban is, de a hidegháború időszakának állambiztonsági szférájában is rendkívül költség és tudásigényes területet képviselt. Az egyes tudományos-kutató vagy kísérleti-konstrukciós munkák finanszírozása éppen ezért szabályozott kérdésként jelent meg a nemzetközi színtéren is. A korszak kialakított megoldása szerint a fejlesztési munkák költsége minden esetben a megrendelő szolgálatokra hárult, azok költségvonzatainak a többi együttműködő szervvel történő megosztása nélkül. A felmerülő költségek viselésénél a fejlesztés adott szakaszaiban mindemellett nem kerülhettek figyelembevételre a későbbi sorozatgyártás szempontjai, valamint a fejlesztés folyamatok során felmerülő költségek utólag sem voltak megjeleníthetőek (például egy másik szocialista ország szolgálatának kikínált sorozatgyártott eszköz árában).

Az alábbi, a rádióelhárító terület nemzetközi együttműködési felületében megjelenő - a vonatkozó dokumentumok[14] alapján összeállított eszközfejlesztési folyamat - lépései jól jelzik a tevékenység rendkívüli összetettségét és vezetettségét.

1. A készülékek, technikai eszközök fejlesztése az adott szerv évekre előremutató rekonstrukciós tervének megfelelően kerültek meghatározásra. A különböző fejlesztési témákat, mint javaslatokat az érintett szolgálatok megküldték a nemzetközi szintű koordinációs szervnek, akik ezeket véleményezték és összesítették.
2. A különböző fejlesztési témákat (TKM, KKM) alapvetően az egyes szolgálatok nemzeti szinteken dolgozó munkatársai állították össze.
3. A fejlesztési témák többi szolgálattal való egyeztetésének feladata azonban már a nemzeti szinteken túlmutatva a koordinációs szervezetre hárult, amely az egyeztetések eredményéről visszatájékoztatta a témát megrendelő szolgálatot.
4. Az adott téma kidolgozása és határidejének meghatározása csak az összes szolgálattal való egyeztetés után kezdődhetett meg. Érdekes elemként jelent meg, hogy azon fejlesztési témákban, amelyekben nem volt egyetértés, a koordinációs szerv szerepe értekezletek, konzultációk megszervezésére irányult, a végső döntést az adott téma „célszerűségéről” azonban a kidolgozó ország biztonsági szerve vezetői hoztak.
5. Az adott fejlesztési feladat beindításához kapcsolódó egyes adminisztratív feladatok (pl. a fejlesztéshez kapcsolódó anyagok szövegezése, konzultációk és találkozók

[14] forrás: ÁBTL, 1.11.8. 00202/3K-72, Kivonat a KA XIII. Kibővített Tanácskozásának jegyzőkönyvéből

szervezése) a központi szervre hárultak és a megvalósítás munkafázisa a vonatkozó jegyzőkönyv aláírásával kezdődhetett meg.

6. A különböző fejlesztési témákat és kapcsolódó műszaki feladatokat a megrendelő rádióelhárító szolgálatok és a nemzetközi koordinációs szerv jogosult munkatársai írták alá. Több tagországot érintő fejlesztési feladatok során természetesen az aláírók köre is bővült.
7. A fejlesztési szakasz az egyes részes szolgálatok feladataként megjelenve, számos sajátossággal összetetten (pl. belső fejlesztési kapacitások, szakembergárda, illetve külső szervek – intézetek esetleges igénybevétele) kerültek végrehajtásra.
8. Az eszközök kifejlesztését követően az átvételi eljárás, hasonlóan az egyes koordinált fejlesztések megkezdéséhez, szabályozott és nemzetközi színtéren összetett tevékenységként jelent meg. Az egyes technikai fejlesztések elvégzését követőn azok átvételét az összes együttműködő ország szakembereiből álló bizottság végezte.
9. Számos adminisztratív elem nehezítette a folyamatot. Ilyenek voltak például az adott műszaki és tudományos dokumentációk teljes körű elkészítése. Ezek alapesetben a kivitelező ország nyelvén készültek el, majd adott részeiket az együttműködés hivatalos nyelvére, oroszra fordították és megküldték a többi együttműködő szolgálatnak. Ezek formai megjelenése, terjedelme, példányszáma mind nemzetközi egyeztetési feladatként jelent meg.
10. Az átvételi eljárás során első körben az érintett tagország saját szakembereiből álló bizottság vette át a fejlesztés eredményét, majd ezt követte a nemzetközi szakemberekből álló bizottság átvételi eljárása. Anélkül hogy részleteiben ismertetném az átvétel összetettségét és folyamatait, számos egyeztetés, jóváhagyás előzte meg a későbbi esetleges sorozatgyártás megkezdését.
11. Az eszközök sorozatgyártása rendszerint abban az országban történt, ahol az eszközrendszer mintapéldányának előállítása megtörtént. Azokban az esetekben, amikor azonban nem állt rendelkezésre megfelelő technikai háttér és gyártókapacitás, másik tagországban is megszervezhető volt a sorozatgyártás az adott felelős megrendelő szolgálat biztonsági szervének egyetértése esetén.

Nem tekinthető elhanyagolható területnek különösen a sorozatgyártott eszközökhöz, és rendszerekhez kapcsolódó képzés feladata sem, amely - figyelembe véve az eszközt felhasználó egyéb tagországokhoz kapcsolódó nemzetközi vonzatokat is - a kivitelező, kidolgozó szolgálatra hárult. A kifejlesztett eszközrendszerek megrendelését az érintett rádióelhárító szolgálatok a koordinációs szervezeten keresztül bonyolíthatták, amely tájékoztatást adott a sorozatgyártást szervező félnek a szükséges mennyiségről. Az eszközök valós beszerzése azonban már az adott ország saját külkereskedelmi szervén segítségével történt.

ÖSSZEGZÉS

A szocialista állambiztonság 1960-70-es éveiben az állambiztonság operatív technikai hátterét biztosító nemzetközi fejlesztéseket mérnöki szemmel a célorientáltság, a tervszerűség és a szervezettség jellemezte. Mindezek mellett azonban az állambiztonsági tevékenység sajátosságaiból adódóan a titkosság és a konspiráltság is végigkísérte a kutatási fejlesztési kérdéseket. A kutatási és fejlesztési, valamint az ezekhez kapcsolódó kísérleti feladatok összetételét vizsgálva azok főként egy-egy új önálló eszköz fejlesztéséhez, vagy egy rendszer részelemét képező eszköz kialakításához kapcsolódtak. A nemzetközi kutatási – fejlesztési együttműködések alapját a vonatkozó együttműködési megállapodások képezték, amelyekben

foglaltak teljesítését az érintett állambiztonsági szervek vezetői rendszeres időközönként vezetői találkozókon tekintették át. Ezeken a találkozókon került sor a végrehajtott feladatok és az elkövetkező évek fejlesztési-kutatási témáinak meghatározására és azok eredményei kölcsönös hasznosíthatóságához kapcsolódó folyamatok gyakorlati kérdéseinek tisztázására is. Az említett fejlesztési – kutatási felületeket megalapozó állambiztonsági szakterületek vonatkozásában lényeges különbség a már említett bi- és multilaterális megvalósítási formáktól eltérően abban mutatkozott meg, hogy a rádiótechnikai kérdéseket jóval szélesebb körű nemzetközi kooperáció, külső kutató intézetek bevonásával járó fejlesztési lehetőségek, valamint a képzések szélesebb körben történő megvalósításának gyakorlata is jellemzett.

Felhasznált irodalmak

[1] Borvendég Zsuzsanna - A BM II/16. Osztályának (Rádió-elhárítás) története és szervezeti felépítése 1945–1962 között - Betekintő 2012/4. szám, http://www.betekinto.hu/ letöltve: 2013.02.20.

[2] Fisher Ferenc – A kétpólusú világ 1945-1989, Dialóg Campus Kiadó, Budapest-Pécs, 2005

[3] Gyarmati György - A magyar humán hírszerzés átnyergelése a (mostoha)testvéri technikára Betekintő 2012/1. szám. http://www.betekinto.hu/ letöltve: 2013.02.20.

[4] Imre Lajos – A hadászati rádiófelderítés a hidegháború éveiben 1946-1990, In: Felderítő Szemle, 2008. nov. VII. Évfolyam, MK KFH, Budapest, pp. 94-99

[5] Krahulcsán Zsolt - KGB és III. Főcsoportfőnökség: egy kapcsolat vége…(?) (A szovjet–magyar állambiztonsági együttműködés szabályozása 1989-ben), Betekintő, 2007/4. szám, http://www.betekinto.hu/ letöltve: 2013.02.10.

[6] Müller Rolf - Az operatív technika alkalmazása és szervezeti keretei a politikai rendőrségen (1945–1962). In.: Szakszolgálat Magyarországon, avagy tanulmányok a hírszerzés és titkos adatgyűjtés világából (1785–2011). Csóka F. (főszerk.). Budapest, Nemzetbiztonsági Szakszolgálat, 2012

[7] Opauszki P. - Vörös J. - Rádióforgalom ellenőrzés. In.: Szakszolgálat Magyarországon, avagy tanulmányok a hírszerzés és titkos adatgyűjtés világából (1785–2011). Csóka F. (főszerk.). Budapest, Nemzetbiztonsági Szakszolgálat, 2012

[8] Pászka Tibor - Szükség van-e a rádióelektronikai felderítésre? Felderítő Szemle, 2004. jún. III/2. szám, MK KFH, Budapest, pp. 84-90

[9] Várhegyi István - A magyar rádiófelderítés működése a hidegháború éveiben 1945-1990, Felderítő Szemle, 2004. jún. III/2. szám, MK KFH, Budapest, pp. 126-153

Levéltári Források:

[10] ÁBTL, 1.11.8. 98-13-4/1974. BM III/5. Osztály, Jelentés a KA XIV. értekezletéről

[11] ÁBTL, 1.11.8. 98-13-5/1975. A KA vezetőjének tájékoztatása, a XV. Kibővített Tanácskozás előzetes napirendjéről, valamint a Tanácskozás munkarendjével kapcsolatos javaslatokról

[12] ÁBTL, 1.11.8. 98-13-4/75. A KA vezetője által a MNK Belügyminiszter-helyettes részére megküldött időszaki beszámoló

[13] ÁBTL, 1.11.8. 98-291/85 BM III/5. Osztály által a BM III. Főcsoportfőnök első helyettesének készített felterjesztés. Felterjesztett anyag: 98-291/1985 BM III/5. Osztály (Rádióelhárítás) ideiglenes ügyrendje

[14] ÁBTL, 1.11.8. 00202/3K-72, Kivonat a KA XIII. Kibővített Tanácskozásának jegyzőkönyvéből

[15] ÁBTL 1.11.8. 98-13-7/76. (Fejlesztési terv)

[16] ÁBTL 89-26-14/75 (Jegyzőkönyv)

[17] ÁBTL 60-156/61 (Egyezmény tervezet)

[18] ÁBTL 46-126/64 (Megállapodás)

[19] ÁBTL, 10-1837/1967. BM III/V. Főcsoportfőnökség ügyrendje,

[20] http://www.abtl.hu/sites/default/files/pdf/forrasok/iii_ugyrend_1967.pdf (letöltve: 2013.02.10.)

[21] ÁBTL, 98-37/1972. BM III/5. Osztály ügyrendje,

[22] http://www.abtl.hu/sites/default/files/pdf/forrasok/ugyrend_10.pdf (letöltve: 2013.02.10.)

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Háber Péter
haber.peter@chello.hu

AZ ASSZIMMETRIKUS HADVISELÉS NÖVEKVŐ JELENTŐSÉGE

Absztrakt

A szerző a katonai konfliktusok egyik közeli példáját, az orosz – grúz konfliktust mutatja be. Tanulmányában a konfliktus történetével, a katonai események bemutatásával, elemzésével és következtetések levonásával, a válság aszimmetrikus jellegének kidomborításával foglalkozik. A katonai erőszak alkalmazását, az erőszak mértékét, jellegét és a konfliktusok újszerű jellemzőit is feldolgozza. Az aszimmetria kérdésében nem csak a „Dávid- Góliát" effektust, hanem az ettől eltérő módszereket eljárásokat is vizsgálja. A cikk végén a konfliktusból levonható katonai tapasztalatokat foglalja össze.

The author presents a nearby example of military conflicts, the Russia-Georgia War. He describes the history of the conflict, analysis and conclusions of the military events, by emphasizing the asymmetric nature of the crisis in his study. He also processes the use of force, the extent and nature of violence and the new characteristics of conflicts. In terms of asymmetry, he investigates other methods and procedures as well as the "David-Goliath" effect. The article concludes by a summary of the military experiences drawn from the conflict.

Kulcsszavak: *katonai konfliktus, aszimmetria, erőszak, túlzott erőssza ~ military conflict, asymmetry, violence, extremly force*

BEVEZETÉS

Napjainkban mind a nemzetközi, mind a hazai katonai szakmai gondolkodásban egyre nagyobb teret nyer az aszimmetrikus hadviselés témaköre. Ugyanakkor általában ez a fogalom elsősorban a terrorizmus elleni harccal kapcsolatban jelenik meg. Azonban a reguláris haderők és a legkülönfélébb célok érdekében tevékenykedő irreguláris (de nem terrorista) erők is évszázadok óta alkalmazzák az aszimmetrikus hadviselést. Az aszimmetrikus műveletek általános meghatározását egy amerikai szerzőpáros foglalta össze a következők szerint: *„A katonai és a nemzetbiztonsági területeken értelmezve, az aszimmetria gyakorlatilag, a szembenálló féltől eltérő cselekvési változatokat (műveleteket), szervezeteket, és gondolkodási módot képvisel, abból a célból, hogy maximalizálja a saját előnyeit, és kiaknázza az ellenség gyengeségeit, valamint megragadja a kezdeményezést, vagy nagyobb cselekvési szabadságot nyerjen. Az aszimmetria lehet politikai-stratégiai, vagy katonai-stratégiai, illetve ezek kombinációja is."*[1] Természetesen az aszimmetrikus tevékenység nem csak a stratégiai, hanem alacsonyabb szinteken is érvényesülhet és a szembenálló felek közötti küzdelem szinte bármilyen aspektusában megjelenhet.

A hazai és külföldi biztonságpolitikai és katonai szakértő egy része már a negyedik generációs hadviselés témakörével foglakozik, amelyben egymást kiegészítve jelennek meg a hagyományos (reguláris erők közötti) és az aszimmetrikus hadviselés elemei, vagy azok egy része. *„A hadviselés korábbi generációiban a szembenálló felek egymás hadviselő képességének, fegyveres erőinek, infrastruktúrájának megsemmisítése útján igyekeztek megtörni egymás akaraterejét. Ennek érdekében a harci tevékenységet információs és propagandamunka egészítette ki. A negyedik generációs hadviselésben az erőpróba és az akaraterők összemérése közötti viszony visszájára fordul. Negyedik generációs erők — a döntéshozók és közvélemény manipulálása útján — közvetlenül az ellenség valamint szövetségesei akaraterejét támadják. A harctevékenység továbbra is nagyon fontos elem, de célja az ellenség pusztítása helyett a fegyveres propaganda: fegyveres akciók támogatják, kiegészítik, erősítik a propaganda és az információs kampányok üzeneteit. A műveletek egy időben folynak a megtámadott társadalom teljes mélységében, a katonai mellett a gazdasági, politikai, társadalmi dimenziókban és a nemzetközi életben is"* [2]

A szakemberek véleménye szerint a grúz-orosz fegyveres konfliktusnak azonban volt egy új, katona-technikai jellemzője is. Ez a konfliktus volt az első, amelynek során a hagyományos fegyverek mellett, azokkal együtt az információs hadviselés eszközeit is bevetették. Felvetődik a kérdés: vajon a kibertérre (a számítógépes és információ, kommunikációs rendszerekre) is vonatkoznak-e a fegyveres küzdelem szabályai és törvényszerűségei? [3]

Ezt szeretném bemutatni a 2008-ban lezajlott grúz – dél-oszét – orosz fegyveres konfliktust használva példaként.

A GRÚZ – DÉL-OSZÉT – OROSZ FEGYVERES KONFLIKTUST ÖSSZEFOGLALÓJA

Előzmények

A grúz–dél-oszét konfliktust kiváltó közvetlen előzményeknek a 2008 tavaszán bekövetkezett események tekinthetők. Ezek időrenden az alábbiak szerint történtek. Először az abház-grúz tűzszüneti zónában következtek be incidensek, amelyek közül a legsúlyosabb az április 20-i eset volt, amikor az orosz légierő Grúzia légterében lelőtt egy grúz pilóta nélküli felderítő repülőgépet. Ezt követően az orosz légierő bombázó és felderítő repülőgépeket telepített a Grúziához közeli repülőterekre, amelyekkel demonstratív repüléseket, valamint légi felderítést hajtott végre. Ezek a határ menti repülések áprilisban és májusban voltak a legintenzívebbek, de csökkenő intenzitással ugyan, a következő hónapokban is folytatódtak.

Az orosz fegyveres erőknek a Kaukázusban állomásozó alakulatai júliusban lényegében folyamatosan gyakorlatoztak. A gyakorlatokon résztvevő erők létszám, és a nehézfegyverzet mennyisége folyamatosan nőtt. A végrehajtásba bevont állomány nem települtek vissza állandó elhelyezési körleteikbe és a határ közelében maradtak. A legnagyobb orosz gyakorlat „Kaukázus 2008" fedőnéven augusztus 2-án ért véget. Ezen körülbelül 8000 fő vett részt.

Ezzel egy időben Grúziában békepartnerségi (PfP) -gyakorlat zajlott, amelyen a grúz haderőn kívül amerikai, örmény, ukrán és azeri katonák is részt vettek.

Eközben a dél-oszét–grúz adminisztratív határ mentén sorozatos fegyveres összecsapások történtek. A legjelentősebb incidensre július 3-án került sor, amikor valószínűleg helyi szakadár fegyveresek sikertelen merényletet hajtottak végre a dél-oszétiai grúz enklávék vezetője, Dmitrij Szanakojev ellen. Augusztus elején Dél-Oszétia azzal vádolta Grúziát, hogy a grúz haderő több alkalommal is tüzérségi eszközökkel lőtt Dél-Oszétia területén elhelyezkedő célpontokat, valamint harckocsi- és tüzéralegységeket vezényelt a grúz–dél-oszét konfliktusövezet határához.

Augusztus 7-én napközben újabb, összecsapások voltak a grúz és dél-oszét fegyveresek között, amelyeket követően Szaakasvili grúz elnök tűzszünetet ajánlott és tárgyalásokra szólította fel a Dél-Oszétiát. Az orosz békefenntartó erők parancsnoka bejelentette, hogy Grúzia és Dél-Oszétia tűzszünetben állapodott meg. A napközben történt események ellenére 7-én éjszaka – arra hivatkozva, hogy a dél-oszétok tovább folytatják a támadásokat – a grúz tüzérség csapást mért Chinvalira, Dél-Oszétia fővárosára, és a grúz haderő támadó hadműveletet[1] indított a szakadár köztársaság ellen. A grúz tüzérség a tűzcsapásai során célpontként lőtte az orosz békefenntartó erők bázisát is.

A fegyveres harcot tehát Grúzia kezdte, súlyosan megsértve a nemzetközi jogot, mert a békefenntartók ellen is figyelmeztetés nélkül erőt alkalmazott. Abházia és az Oroszországi Föderáció azonnal jelezte, hogy katonai segítséget nyújt Dél-Oszétiának.

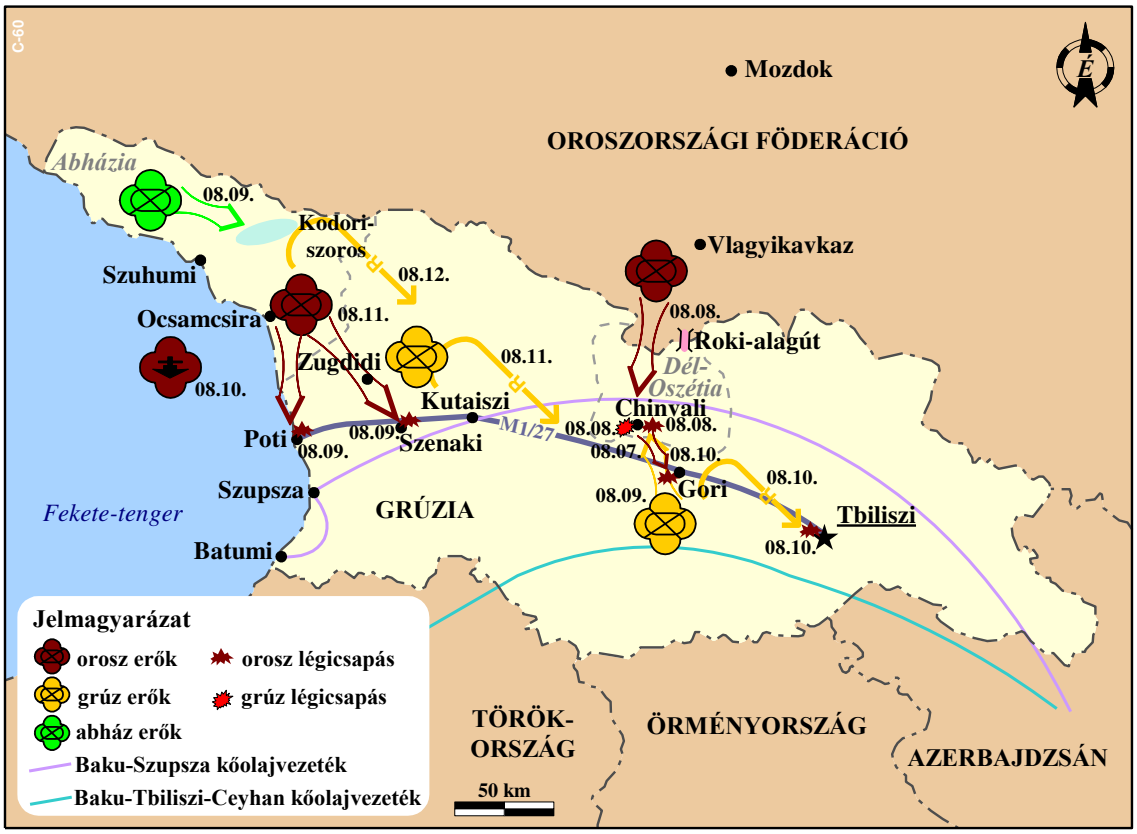
A harctevékenységek időszaka

	Grúzia	**Dél-Oszétia**	**Abházia**	**A „békekikényszerítésbe" bevont orosz erők**
Békelétszám	**30 000**	**2500**	**8000**	**25 000**
Tartalékos létszám	**100 000**	**16 000**	**10 000**	na.
Harckocsi	**165 db** T-72, **40 db** T-55	**15 db** T-55/T-72	**40 db** T-55	**200 db** T-72/62
Páncélozott harcjármű	**180 db** BMP-1/BMP-2, BTR-80	**22 db** BMP-1, **24 db** BTR-70/80	**57 db** BTR-70/80, **49 db** BMP-1	**160 db** BMD-1/2, **120 db** BMP-1/2, **120 db** BTR-70/80
Ágyú/tarack	**120 db** 122 és 152 mm-es	**24 db** 122 és 152 mm-es	**40 db** 122 mm-es	**144 db** 122 és 152 mm-es
Sorozatvető	**40 db** BM-21, RM-70	**6 db** BM-21	**15 db** BM-21	**36 db** BM-21, **18 db** Szmercs
Aknavető	**80 db** M120, M75, 2S12	**30 db**	na.	**40 db** 120 mm-es öj. aut. av., **54 db** 2S12
Harci repülőgép	**4-5 db** harcképes Szu-25	na.	**2 db** Szu-25, **3 db** L-39	**120 db** különböző harci repülőgép
Helikopter	**30 db**, ebből 9 db Mi-24	**4 db** Mi-8	**3 db** Mi-24, **12 db** Mi-8	**54 db** Mi-24

1. ábra. A szembenálló felek haderőinek fontosabb mutatói [4] (Szerkesztette: Háber Péter)

[1] A támadásban résztvevő erők létszáma nem éri el a „hadművelet" megnevezéshez szükséges szintet, de abból kiindulva, hogy egy ország politikai céljainak elérése érdekében folytat műveleteket indokolt a hadművelet kifejezés alkalmazása.

A fegyveres konfliktus kirobbanását követően a harctevékenységek augusztus 07-12. között zajlottak Grúzia – Dél-Oszétia – Abházia és az úgynevezett „békekikényszerítésbe” bevont orosz 58. Hadsereg erői között.



2. ábra. Harctevékenységek 2008.08.07 – 08.12 között [5] (Szerkesztette: Háber Péter)

Dél-Oszétia

A grúz támadás augusztus 8-án folytatódott Chinvali ellen. Medvegyev elnök vezetésével az Oroszországi Föderáció Biztonsági Tanácsa a kialakult helyzet elemzése után az orosz csapatok Dél-Oszétiába vezényléséről döntött. Ezt követően megindult az orosz haderő kijelölt alakulatainak átcsoportosítása a térségbe, és az orosz légierő csapásokat mért a grúz csapatokra Dél-Oszétiában. Szaakasvili grúz elnök bejelentette, hogy Oroszország támadó hadműveletet kezdett Grúzia ellen és elrendelte a grúz haderő teljes harckészültségbe helyezését, valamint 100 ezer fő tartalékos mozgósítását.

Másnap az orosz 58. Hadsereg csapatai már megkezdték a grúz erők kiszorítását Dél-Oszétiából, és Dmitrij Medvegyev orosz elnök bejelentette, hogy a Dél-Oszétiába vezényelt orosz erők béke kikényszerítő műveletet folytatnak. Szaakasvili grúz elnök azonnali tűzszünetre, a csapatok szétválasztására és a harcok által érintett területek fegyvermentesítésére szólított fel. A grúz parlament jóváhagyta az államfő korábbi rendeletét a hadiállapot bevezetéséről. A hadiállapot 15 napos határidővel Grúzia egész területére kiterjedt. Az orosz csapatok 10-ére befejeztek a Dél-Oszétiában harcoló grúz erők ellenállásának felszámolást és kiszorítását a szakadár köztársaság területéről. Az orosz erők helyenként átlépték a grúz–dél-oszét határt is. Augusztus 11-én a dél-oszét és a grúz határ menti területekről visszavont grúz erők védelmi állásokat foglaltak Tbiliszitől nyugatra, azonban továbbra is tüzérségi csapásokat mértek Chinvalira, és az 58. Hadsereg csapataira.

	Mennyiségi erőviszony	
	Grúz	**Dél-Oszét**
Békelétszám	12	1
Tartalékos létszám	6,2	1
Harckocsi	11	1
Páncélozott harcjármű	3,9	1
Ágyú/tarack (100 mm felett)	5	1
Sorozatvető	6,7	1
Aknavető	2,7	1
Helikopter	7,5	1

3. ábra. Az erőviszony a grúz – dél-oszét erők között (Szerkesztette: Háber Péter)

Abházia

Augusztus 8-án fokozott harckészültségbe helyezték a grúz-abház határ térségében elhelyezkedő abház erőket, amelyek szétbontakoztak a békefenntartó erők által ellenőrzött övezet határán. Augusztus 9-én az abház erők megkezdték a Kodori-szorosban levő grúz erők kiszorítását. Másnap az orosz Fekete-tengeri Flotta erőinek egy részét Grúzia partjaihoz, az abház partszakasz közelébe vezényelték, de Poti és Batumi kikötőjét nem vették blokád alá. Augusztus 11-én az abház és orosz erők összehangolt támadást indítottak a grúz–abház biztonsági zónában levő grúz erők ellen. 12-ére a grúz erőket kiszorították a Kodori-szorosból és az orosz/abház erők elfoglalták Potit, Szenakit és Zugdidit. A grúz belügyminisztérium szóvivője bejelentette, hogy a grúz csapatok kivonultak Abházia területéről.

	Mennyiségi erőviszony	
	Grúz	**Abház**
Békelétszám	3,7	1
Tartalékos létszám	10	1
Harckocsi	4,1	1
Páncélozott harcjármű	1,7	1
Ágyú/tarack (100 mm felett)	3	1
Sorozatvető	2,7	1
Harci repülőgép	2,5	1
Helikopter	2	1

4. ábra. Az erőviszony a grúz – abház erők között (Szerkesztette: Háber Péter)

A harcokban résztvevő orosz erőkkel az erőviszony számvetés során egységesen számoltam, mert nem rendelkezem pontos információkkal ezek megoszlásáról Abházia és Dél-Oszétia területén.

	Mennyiségi erőviszony	
	Grúz	A „békekikényszerítésbe” bevont orosz erők
Békelétszám	1.2	1
Harckocsi	1	1
Páncélozott harcjármű	1	2,,3
Ágyú/tarack	1	1,2
Sorozatvető	1	14
Aknavető	1	1,2
Harci repülőgép	1	24
Helikopter	1	1,8

5. ábra. Az erőviszony a grúz – „békekikényszerítésbe” bevont orosz erők között (Szerkesztette: Háber Péter)

Augusztus 12-én délre az orosz erők elérték a kitűzött hadműveleti célokat, vagyis az orosz békefenntartók és a szakadár területek lakosságának védelmét, vlamint a 2008. augusztus 7-e előtti állapot helyreállítását, ezért Medvegyev orosz elnök elrendelte a hadművelet leállítását és ideiglenes tűszünet jött létre a harcoló felek között.

Veszteségek

Veszteség	Grúzia	Oroszország
személyi	143 fő halott 1964 fő sebesült	74 fő halott 171 fő sebesült 19 fő eltűnt
haditechnikai	1 db Szu-25, 1 db Mi-8, 1 db Mi-24, - kb. 70-40 db harckocsi és harcjármű 7 db hadihajó	3 db Szu-25, 2db Szu-24M 1 db Tu-22M3 repülőgép, - nincs információ az harckocsi és harcjármű veszteség nagyságáról.

6. ábra. A szemben álló felek vesztesége [6]; [7]; [8] (Szerkesztette: Háber Péter)

A polgári áldozatok számáról ellentmondásos adatok kerültek nyilvánosságra. Az összesítések szerint Dél-Oszétiában 300 fő vesztette életét, a grúziai halálos áldozatok száma 228 fő. [9]

A harctevékenységek leállítását követő katonai események

A harctevékenységek leállítását követően azonnal az orosz erők egy része megkezdte a visszatelepülést a békeelhelyezési-körletekbe, ezzel párhuzamosan az orosz erők biztonsági zóna kiépítését kezdték meg Grúzia területén. Ennek során ellenőrző-áteresztő és megfigyelő pontokat létesítettek, valamint ellenőrzésük alatt tartották Potit, Szenakit, Gorit. Az orosz erők megkezdték a grúz katonai objektumok rombolását, a zsákmányolt fegyverzet, lőszer és felszerelés megsemmisítését vagy elszállítását.

Augusztus 23-án megkezdték és be is fejezték a nehézfegyverzettel rendelkező orosz erők többségének visszavonását Grúziából Dél-Oszétiába és Abháziába, valamint a visszavont alakulatok zömének útba indítását Oroszországba.

Augusztus 23-a után az orosz katonai vezetés egyoldalúan új tűzszüneti zónákat jelölt ki a grúz – dél-oszét, valamint a grúz – abház határ körzetében. A Dél-Oszétia körüli zóna nagyjából egybeesett az 1992. évi tűzszüneti szerződésben rögzített zónával, de az Abházia körüli zóna ugyanakkor lényegesen nagyobb volt, mint az 1994. évi tűzszüneti szerződésben rögzített, helyenként 20 km-rel is mélyebben benyúlt Grúzia területébe. A zónákon belül megfigyelő pontokat létesítettek, de azok személyi állománya csak az ellenőrző-áteresztő pontok védeleméhez szükséges fegyverzettel rendelkezett. Oroszország a Sarkozy-Medvegyev megállapodásban vállalta a grúz területen lévő ellenőrző pontjai felszámolását, amit október 10-ig be is fejezett.

A hadrafogható grúz erőket augusztus 10-én Tbiliszi körzetében vonták össze, majd az orosz csapatok kivonulását követően fokozatosan visszatértek korábbi laktanyáikba, s megkezdték a háborús sérüléseket szenvedett infrastruktúra helyreállítását.

A grúz tevékenység értékelése:

A grúz politikai vezetés feltételezhetően az alábbi okok miatt döntött a támadó hadművelet megkezdése mellett:

- a NATO bukaresti csúcstalálkozóját követően a grúz vezetés már nem bízott a NATO-tagság gyors elnyerésében;
- attól tartott, hogy a szakadár köztársaságok számára Koszovó függetlenségének kikiáltása és nemzetközi elismerése precedenst jelenthet;

- a NATO csúcstalálkozót követően Abházia és Dél-Oszétia egyaránt magabiztosabbá vált, és rendszeresen – kisebb összecsapásokkal – provokálták Grúziát;
- az erőviszonyok és a katonaföldrajzi tényezők ismeretében Grúzia feltehetően már lemondott az Abházia feletti ellenőrzés visszaszerzéséről, de Dél-Oszétia visszafoglalására még látott esélyt;
- a grúz fegyveres erőknél a háborút megelőző években végrehajtott fegyverzeti és kiképzése korszerűsítés miatt a grúz politikai vezetés bízott a katonai erőfölényében és sikerben a szakadár köztársasággal szemben.

Az orosz fegyveres erők konfliktus előtti tevékenysége arra utalt, hogy – feltehetően megbízható hírszerzési adatok birtokában – felkészültek egy esetleges grúz támadás elhárítására, amiről a grúz hírszerzésnek is tudnia kellett. A grúz politikai vezetés valószínűleg azért döntött mégis Dél-Oszétia megtámadása mellett, mert abban bízott, hogy a nyári szabadságolás és az olimpia megnyitása jelentősen lassítja az eseményekre történő orosz és nemzetközi reagálást. Egy gyors támadó hadművelettel (mielőtt az orosz politikai vezetés reagálni tudna) elfoglalja Dél-Oszétia fővárosát, majd leállítja a harctevékenységet, és új status quo-t teremtve biztosítja a köztársaság visszacsatolását Grúziához. Az orosz politikai és katonai vezetés azonban gyorsan és határozottan reagált, mielőtt a grúz haderő elérte volna céljait.

A grúz harci morál összeomlásának okai

A grúz szárazföldi csapatok harci morálja – feltehetően a gyors orosz sikerek, a nem megfelelő kiképzettség és a vezetési rendszer súlyos hiányosságai következtében – rövid idő alatt összeomlott, ami a harcképesség gyors elvesztését eredményezte. Az előző években jelentős technikai fejlesztéseket hajtott végre a grúz haderő, de a csapatok, és főként a tiszti állomány kiképzettsége, gyakorlati tapasztalati nem voltak megfelelő szinten. Az alegységparancsnokok még nem készültek fel az önálló döntéshozatalra, az alárendeltek vezetésére. A harci morál gyors összeomlásában feltehetően közrejátszott az is, hogy a politikai vezetés a grúz erőket elsősorban nemzetközi keretek között végrehajtott békefenntartói feladatokra készítette fel. Ennek ellenére azonban egy olyan művelet végrehajtására alkalmazta, amelynek céljával (a nemzetközi jogot súlyosan megsértve, egy több mint 15 éve de facto független területnek a visszafoglalása katonai erővel) a személyi állomány jelentős része valószínűleg nem tudott teljesen azonosulni. A katonák pszichikai felkészületlenségét és alacsony morális állapotát jól jelzi, hogy a személyi állomány jelentős része harcba sem bocsátkozva, felszerelését és haditechnikai eszközeit elhagyva elmenekült. A grúz haditechnikai veszteség jelentős része ebből származott. A lélektani felkészültség és a feladattal történő azonosulás fontosságát és a katonai sikerre gyakorolt hatását jól példázza, hogy az ország légterét oltalmazó és mind gyakorlatilag, mind pszichológiailag erre felkészített grúz légvédelem az orosz légi fölény ellenére meglehetősen sikeresen hajtotta végre a feladatait.

Az orosz fegyveres erők tevékenységének értékelése

Az orosz haderő elsődlegesen a Dél-Oszétia elleni grúz támadó csoportosítás első, majd második lépcsőjére, az abház területeken állomásozó grúz erőkre, továbbá a haditengerészet Poti-i bázisára és a grúz légierő repülőtereire mért csapásokat. Ugyanakkor nem érte támadás a Tbiliszi védelmére összevont erőket, a Tbilisziben levő vezetési pontokat. Poti polgári kikötője is sértetlen maradt, holott a nemzetközi sajtó először arról tájékoztatott, hogy teljesen

lerombolták. A csecsenföldi harcokhoz képest lényegesen kevesebb polgári áldozatot követeltek a harcok, s a lakott települések nem szenvedtek jelentős károkat.

Az orosz fegyveres erők a hadművelet végrehajtása során nem támadtak szándékosan civil célpontokat, törekedtek a polgári lakosság és a nemzetközi erők megóvására. A támadásokat megelőzően felszólították az ENSZ-t és az EBESZ-t megfigyelőik kivonására, valamint az Egyesült Államokat, hogy távolítsa el szállító repülőgépeit a Tbiliszi közelében lévő repülőtérről.

Nem áll rendelkezésre megerősített adat arra vonatkozóan, hogy az orosz erők rendszeresen és kiterjedten fosztogattak volna. Ilyen cselekmények feltehetően előfordultak, de valószínűsíthetően elsősorban a beérkezett nem reguláris dél-oszét és abház erők egyes tagjainak részéről, és inkább elszigetelt jelenségnek lehet tekinteni, amit a grúz média hadjárat felerősített.

A szárazföldi csapatok tevékenysége

A Dél-Oszétiába és Abháziába vezényelt orosz szárazföldi csapatok létszámban és fegyverzetben a grúz szárazföldi csapatokhoz közel azonos erőt képviseltek. A beérkező orosz harccsoportok helyi erőfölény létrehozásával folyamatosan támadták a még harcképes grúz erőket. Az átszegdelt, erdős-hegyes, nehezen járható terepen harckocsi- és gépesített lövészalegységeket alkalmaztak. A légideszant-alegységek a gépesített lövész alegységekkel együtt, a támadás első lépcsőjében harcoltak.

Felszerelés

A műveletben részt vevő szárazföldi alegységek zöme régi típusú és gyártású, nem korszerű fegyverzettel rendelkezett. A nehézfegyverzet jelentős részét az 1960-as, 1970-es években gyártott fegyverek tették ki. Az egyetlen kivételt a légideszant-csapatok alegységei jelentették, amelyek már új egyéni fegyverzettel, védőeszközökkel és felszereléssel hajtották végre feladataikat.

Morális helyzet

Az orosz alakulatok személyi állományának morális helyzete jó volt, ugyanakkor a feladatokat nem minden esetben a harcszabályzatoknak megfelelően hajtották végre. Magabiztosságuk lezserséget, a felderítés és a menetbiztosítás elhanyagolását eredményezte.[2]

A légierő tevékenysége

Az orosz légierő – a szárazföldi csapatokkal ellentétben – döntő mennyiségi és minőségi fölénnyel rendelkezett a grúz légierővel szemben.

A grúz légierő minimális képességei miatt a légierő csata- és bombázó repülőgépei legtöbbször vadászkíséret nélkül hajtották végre feladataikat.

A döntő légi fölény ellenére az orosz légierőnek nem sikerült semlegesítenie a grúz légvédelmet, ezért hat repülőgép veszteséget szenvedett. [10] A szárazföldi csapatok légi támogatására csak elvétve alkalmaztak harci helikoptereket, ezt a feladatot is Szu–25 típusú csatarepülőgépekkel oldották meg. Az orosz repülőerők katonai célpontokat támadtak. A légierő repülőgépei szándékosan nem támadtak polgári célpontokat.

Az orosz légierő repülőgépei csak korlátozott mennyiségben alkalmaztak precíziós fegyvereket, ezért a csapások pontatlanok voltak. A bevetések során ledobott bombák jelentős része feltehetően lejárt szavatossága következtében nem robbant fel.

A konfliktus során az orosz erők nem alkalmaztak pilóta nélküli felderítő repülőgépeket, és csak néhány esetben hajtották végre a csapások eredményének megfigyelését.

[2] Augusztus 8-án az 58. hadsereg parancsnoka kis híján fogságba esett.

Az orosz légierő nem készült kutató-mentő feladatok végrehajtására, ezért kísérletet sem tettek a lezuhant repülőgépek személyzetének kimentésére.

A haditengerészet tevékenysége

Az orosz Fekete-tengeri Flotta az orosz erők hadműveletének támogatására augusztus 10-én vonult fel Grúzia partjaihoz, illetve kezdte meg tengerészgyalogos erők szállítását Abháziába. A flotta négy hadihajóval [11] hajtotta végre feladatát, amivel – figyelembe véve az orosz hadihajók összehasonlíthatatlanul nagyobb tűzerejét és harci alkalmazási képességeit – döntő fölénybe került a grúz haditengerészettel szemben.

Pszichológiai-információs és számítógépes hadviselés

Pszichológiai hadviselést orosz részről elsősorban harcászati szinten alkalmaztak. A leghatásosabb módszer a „csecsenek bevetésével" történő fenyegetés volt. Kiszivárogtatták, hogy a Csecsenföldön állomásozó 42. gépesített lövészhadosztály csecsen katonákból álló zászlóaljaiból néhány alegység Dél-Oszétiába érkezett.[3]

Az orosz információs hadviselés hadászati szinten nem volt hatékony. Az orosz katonai és polgári szervezetek nem használták ki lehetőségeiket annak bizonyítására, hogy – a grúz vádakkal ellentétben – Oroszország nem alkalmaz túlzott erőt, illetve hogy Grúzia szegte meg az érvényben levő tűzszünetet. Ennek következtében Oroszország a nemzetközi médiában egy ideig alulmaradt a grúz propagandával szemben.

Orosz részről hatékony megosztott szolgáltatásmegtagadással (DDoS)[4] járó támadásokat hajtottak végre a grúz internetes oldalak ellen. A túlterheléses támadásokkal sikerült jelentős mértékben bénítaniuk a grúz köztársasági elnök, a minisztériumok, az állami szervezetek, a hírcsatornák és a bankok internetes oldalainak a működését. A hírcsatornák bénításával azonban csak részben sikerült csökkenteni a grúz propaganda-hadjárat eredményességét.

A GRÚZ – DÉL-OSZÉT – OROSZ FEGYVERES KONFLIKTUS ÖSSZEFOGLALÁSA AZ ASZIMMETRIKUS MŰVELETEK SZEMPONTJÁBÓL

A fenti fegyveres konfliktus eseményei és adatai megítélésem szerint jól szemléltetik, hogy az aszimmetrikus műveletek egyszerre jelenhetnek meg a reguláris és a milícia jellegű erők közötti összecsapásokban is, illetve a fegyveres küzdelem különböző szintjein, valamint a nem fegyveres szembenállás területein is.

Stratégiai szintű aszimmetriának lehetne tekinteni, hogy a létszámban jelentősen kisebb grúz haderő egy atomfegyverrel rendelkező katonai nagyhatalom érdekszférájába tartozó terület ellen indított támadást. A gyakorlatban azonban ez mégis, csak a hadműveleti szintnek felelt meg, mert az orosz fél – amint ez az erőviszony számvetésekből is látszik – nem alkalmazott túlzott katonai erőt érdekei védelme érdekében.

A konfliktusban részt vevők tevékenysége véleményem szerint kellő mértékben illusztrálja, hogy az aszimmetria milyen változatos területeken alakulhat ki a különböző erejű, képességű és helyzetű ellenfelek között. Ezt szeretném az alábbi példákkal részletesen is alátámasztani:

- a grúz erők jelentős számbeli erőfölénye a dél-oszét csapatokkal szemben;
- az orosz szárazföldi erők képessége arra, hogy harcászati szintű helyi erőfölényt hozzanak létre az egyébként összlétszámban és fegyverzetben közel azonos grúz haderővel szemben;

[3] 1992-ben, az abház-grúz fegyveres konfliktus során a segítségül beérkezett csecsen szabadcsapatok jelentős részben hozzájárultak a grúz csapatokkal szembeni abház győzelemhez.

[4] Distributed Denial of Service (DDoS) – megosztott szolgáltatásmegtagadással járó támadás

- az abszolút orosz légi fölény, és az ennek ellenére meglehetősen sikeresen tevékenykedő grúz légvédelem;
- a gyors orosz haditengerészeti fölény kivívása;
- az abház csapatok sikeres tevékenysége a szinte minden területen mennyiségi fölénnyel rendelkező grúz erőkkel szemben;
- a konfliktust megelőző politikai helyzetértékelés, a hadműveleti tervezés és a kiképzés során jelentkező különbözőségek a grúz és orosz erők között, annak ellenére, hogy feltételezhetően mindkét fél rendelkezett a szükséges hírszerzési és felderítési információkkal;
- a katonák pszichológiai felkészítés és a csapatok morális állapota között meglévő jelentős különbségek, amelyek akkor sem csökkentek, amikor a grúz erőknek már a honi területeket kellett volna védeniük;
- a diplomáciában és a nemzetközi média irányába folytatott kommunikációban jelentkező, hónapokig tartó túlnyomó grúz fölény;
- és végül, de nem utolsó sorban a számítástechnikai hadviselés területén kialakult jelentős orosz túlsúly.

ÖSSZEGZÉS

Az aszimmetrikus hadviselés fogalma jelenleg erősen kapcsolódik a terrorizmushoz túlnyomó részt csak ebből a szempontból értékelik és elemzik ezt a műveleti formát. Ez a nézőpont azonban erősen kötődik a jelenlegi amerikai biztonságpolitikai helyzethez, kihívásokhoz, és stratégiai környezethez, vagyis nem eléggé általános (átfogó) jellegű. Ez a szemlélet csak az ún. „negatív aszimmetriát" tartalmazza, ami abból indul ki, hogy az USA mindenkivel szemben már eleve nagy technológiai, katonai, és gazdasági fölényből indul, így nem tárgyalja az olyan szituációkat, amelyekben egyenrangú, vagy közel egyenrangú felek alkalmazzák egymás ellen az aszimmetrikus eljárásokat, vagyis az aszimmetriára alapozzák a teljes stratégiájukat. [12]

Az orosz-grúz összecsapás arra figyelmeztet, hogy két állam közötti konfliktus esetén számolni kell azzal, hogy a szemben álló felek arra törekednek majd, hogy megbénítsák egymás, az Internettel összeköttetésben lévő infrastruktúráinak működését. Ezzel az iparilag és gazdaságilag fejlett országokban több stratégiai fontosságú területen is jelentős károkat okozhatnak. [13]

Úgy gondolom, hogy a korábbi ideológiai alapú globális katonai szemben állás megszűntével az aszimmetrikus hadviselés egyre inkább jellemző lesz korunk és a jövő fegyveres konfliktusaira, helyi, vagy regionális háborúira is. Ebből kiindulva véleményem szerint mind inkább szükségessé válik majd az aszimmetrikus műveletek területeinek, fajtáinak, módszereinek és más egyéb összetevőinek elméleti feldolgozása, rendszerezése és gyakorlati alkalmazási lehetőségeinek a meghatározása nem csak a nagyhatalmak, hanem a különböző szövetségi rendszerekben és békeműveletekben résztvevő országok haderői számára is.

Ugyanakkor a 2008-as orosz grúz háború megmutatta, hogy továbbra sem lehet kizárni egy magas intenzitású konfliktus kialakulásának esélyét a fejlett országok között sem. Az a tény, hogy összhaderőnemi hadviselés alkalmazásával az orosz fegyveres erők megközelítőleg egy hét alatt teljesítették feladatukat és ezzel több, hadműveleti szintű katonai és külpolitikai célt is megvalósítottak minden döntéshozót el kell, hogy gondolkoztasson. A fenti események tükrében nem lehet felelősséggel kijelenteni, hogy nem léphet színre bárhol egy szélsőséges politikus, aki kihasználva a nemzetközi diplomácia meglehetősen lassú reakció idejét, megkísérli, hogy erőszakot alkalmazva kész, új tények elé állítsa a világot? Éppen ezért egyetlen ország sem nélkülözhet, egy hiteles elrettentő képességgel rendelkező haderőt,

melyet szükség esetén egy aszimmetrikus hadviselésre kiképzett és felfegyverzett tartalékos erő egészít ki. [14]

Felhasznált irodalom

[1] Dr. habil. Krajnc Zoltán: Az aszimmetrikus hadviselés, fenyegetés alapkérdései; Repüléstudományi Közlemények, 2008. évi Különszám; (Repüléstudományi Konferencia 2008. április 11.) http://www.szrfk.hu/rtk/kulonszamok/2008_cikkek/Krajnc_Zoltan.pdf (Letöltés ideje: 2013.03.18.)

[2] Kiss Álmos Péter: Generációk a hadviselésben – negyedik generáció; Hadtudományi Szemle 2009./ 2. szám, pp.: 10-18. http://uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi_szemle/szamok/2009/2009_2/2009_2_hm_kiss_almos_10_18.pdf (Letöltés ideje: 2013.03.23.)

[3] http://portal.zmne.hu/portal/page?_pageid=34,17704,34_112973,34_112961&_dad=portal&_schema=PORTAL (Letöltés ideje: 2013.03.23.)

[4] Михаил Барабанов, Антон Лавров, Вячеслав Целуйко: Танки августа; Центр анализа стратегий и технологий; Москва, 2009 http://cast.ru/files/the_tanks_of_august_sm.pdf (Letöltés ideje: 2013.03.23.)

[5] http://hu.wikipedia.org/wiki/Orosz%E2%80%93gr%C3%BAz_h%C3%A1bor%C3%BA (Letöltés ideje: 2013.03.19.)

[6] http://hu.wikipedia.org/wiki/Orosz (Letöltés ideje: 2013.03.23.)

[7] http://ru.wikipedia.org/wiki/ Война_в_Южной_Осетии_(2008) (Letöltés ideje: 2013.03.23.)

[8] Михаил Барабанов, Антон Лавров, Вячеслав Целуйко: Танки августа; Центр анализа стратегий и технологий; Москва, 2009 http://cast.ru/files/the_tanks_of_august_sm.pdf (Letöltés ideje: 2013.03.23.)

[9] http://hu.wikipedia.org/wiki/Orosz%E2%80%93gr%C3%BAz_h%C3%A1bor%C3%BA (Letöltés ideje: 2013.03.22.)

[10] http://hu.wikipedia.org/wiki/Orosz%E2%80%93gr%C3%BAz_h%C3%A1bor%C3%BA (Letöltés ideje: 2013.03.22.)

[11] http://ru.wikipedia.org/wiki/Российско-грузинское_военно-морское_столкновение_(2008) (Letöltés ideje: 2013.03.22.)

[12] Dr. habil. Krajnc Zoltán: Az aszimmetrikus hadviselés, fenyegetés alapkérdései; Repüléstudományi Közlemények, 2008. évi Különszám; (Repüléstudományi Konferencia 2008. április 11.) http://www.szrfk.hu/rtk/kulonszamok/2008_cikkek/Krajnc_Zoltan.pdf (Letöltés ideje: 2013.03.18.)

[13] http://portal.zmne.hu/portal/page?_pageid=34,17704,34_112973,34_112961&_dad=portal&_schema=PORTAL (Letöltés ideje: 2013.03.23.)

[14] Somkuti Bálint: A negyedik generációs hadviselés - az érdekérvényesítés új lehetőségei; Doktori (PhD) értekezés, Nemzeti Közszolgálati Egyetem, 2012; p. 145.; http://www.uni-nke.hu/downloads/konyvtar/digitgy/phd/2012/somkuti_balint.pdf (Letöltés ideje:2013.03.23.)

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Kolonics Gábor – Kóródi Gyula
kolonicsg@yahoo.com – korodigy@freemail.hu

THE EXAMINATION OF THE ROLE OF NATURAL SUBSTANCES IN THE PROTECTION AGAINST UV RADIATION

Abstract

UV radiation is one of the serious risk factors among the extreme external factors for our soldiers serving in missions. In the military health care, the advanced sunscreen products play an important role as being integral part of the new UV radiation protection system and the training system the authors have planned. These substances must meet the following criteria: efficient, natural, easily available in large quantities, cheap, non-toxic, antioxidant. In our series of experiments, the authors were looking for substances complying with these principles. As a first step, fulvic acids were taken into account, and the authors examined if, on the basis of the UV absorption of these substances, it may be used as the component of the sun protection cream the authors have imagined.

Missziókban szolgáló bajtársainkat érő több extrém külső fizikai tényező közül az egyik nagyon komoly kockázati tényező az UV sugárzás. A katonai egészségvédelemben a szerzők tervezett új UV sugárvédelmi rendszer és kiképzési rendszer szerves részeként fontos szerepet játszanak a korszerű napvédő anyagok. Ezeknek az anyagoknak a következő szempontoknak kell megfelelniük: hatékony, természetes, nagy mennyiségben könnyen előállítható, olcsó, nem toxikus, antioxidáns tulajdonságú. Kísérlet sorozatukban ezen elveknek megfelelő anyagokat kerestek a szerzők, így első lépésként a fulvósavak kerültek látóterükbe és azt vizsgálták, hogy ezek az anyagok UV abszorbciója alapján alkalmas lehet-e az általuk elképzelt napvédő krém komponenseként alkalmazni.

Keywords: *UV radiation, personal UV protection,skin cancer, fulvic acid, absorbance of fulvic acid, mission, prevention. ~ UV sugárzás, személyes UV védelem, bőrrák, fulvosav, fulvosav abszorbancia, misszió, megelőzés*

INTRODUCTION

In the following, the authors will present that for personal UV protection, as being part of the complex UV protection planned in the Hungarian Army, the authors plan to examine an efficient, cost effective substance of natural origin.

UV radiation is one of the most predictable health-endangering agents among the extreme external factors affecting soldiers serving in missions far away from our country (e.g. Afghanistan, Iraq, Cyprus and Egypt).

In these duty stations, the number of hours spent in the direct sunlight is high in working ours or rest period, entailing short and long-term risks of irreversible effects. In Cyprus for example, the approximate number of the sunny days can be 300 per year, the UV index is almost always in the in the range of 8 to 10 in the summer, and even the extreme value of 11+ is not rare, based on personal experience. [1]

This subject needs to be a requirement as part of military culture for those on military service in Hungary on a regular basis, because even here this environmental factor is a danger of increasing significance. Because of its adverse effects, it may jeopardise the performance abilities of the military personnel both short term (e.g. immune suppression) and long term (e.g. melanoma).

PERSONAL UV PROTECTION

The complex UV protection is divided into three parts:

1. education
2. prevention - regulation, personal protection
3. screening tests (pre- and post-test)

Personal protection is one of the forms of prevention, it can be by the usage of personal protective equipment (e.g. sunglasses), appropriate clothing (sun cap hat, shell-jacket) and sunscreen (sun protection creams).

The currently available sun protection creams, ointments, solutions are mostly artificial, multicomponent and relatively expensive.

However, the protective material the authors have imagined contains 1 or 2 natural materials apart from the carrier that can be produced in large quantities very cheaply. The UV absorption is in the appropriate range and has significant antioxidant effects, which can slow down, prevent or reverse disease processes.

That is how the authors started the work with fulvic acid, which can be recovered from peat that occurs in the nature and is a cheap source in large quantities.

HARMFUL UV SPECTRUM

7% of the sunlight is in the ultraviolet range (Nicholson et al., 2005) [2], but only a fraction reaches the surface of the earth. According to the absorption in the atmosphere, further division of the high-energy optical radiation is possible on the basis of wavelength. UVC between 100-280 nm is fully absorbed and dispersed by nitrogen and oxygen molecules of the atmosphere. UVB, 315 – 280 nm, is absorbed by ozone, generated by UVC. UVA with longer wavelength reaches the surface without hindrance, similar to the visible light. [3]

UVA (315-400 nm)	Biological effect: It causes neither erythema nor pigmentation in low doses. At higher doses, together with UVB, it is followed by erythema or pigmentation. At high doses, erythema is caused without direct pigmentation.
UVB (280-315 nm)	Biological effect: Direct erythema, after 12-24 hours, indirect pigmentation, which regresses It irritates conjunctiva and cornea Synthesis of vitamin D3 synthesis Carcinogenesis!
UVC (180-280 nm)	It does not reach the surface.

Figure 1. Biological effects of UV radiation[4]

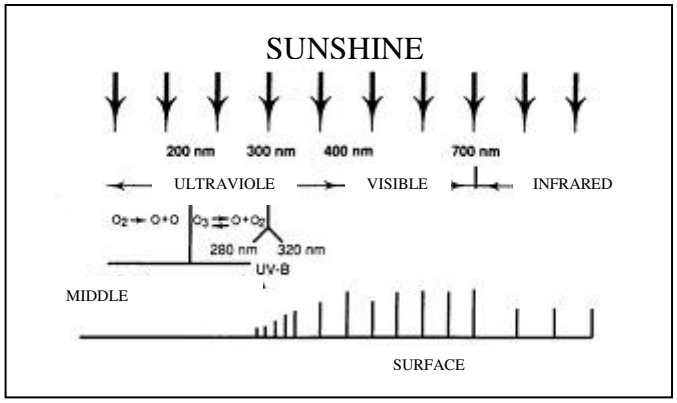


Figure 2. Ultraviolet Reflections[5]

Thus, the sunscreen substances sought must absorb in UVA and UVB range.

HISTORY OF SUNSCREEN

„The first effective sunscreen may have been developed by chemist Franz Greiter in 1946. The product, called Gletscher Crème (Glacier Cream), subsequently became the basis for the company *Piz Buin* (named in honor of the place Greiter allegedly obtained the sunburn that inspired his concoction), which is still today a marketer of sunscreen products. It has been estimated that Gletscher Crème had a sun protection factor of 2.

The first widely used sunscreen was produced by Benjamin Green, an airman and later a *pharmacist*, in 1944. The product, Red Vet Pet (for red veterinary petrolatum), had limited effectiveness, working as a physical blocker of ultraviolet radiation. It was a disagreeable red, sticky substance similar to petroleum jelly. This product was developed during the height of *World War II*, when it was likely that the hazards of sun overexposure were becoming apparent to soldiers in the Pacific and to their families at home. Sales of this product boomed when *Coppertone* acquired the patent and marketed the substance under the *Coppertone girl* and *Bain de Soleil* branding in the early 1950s.

Franz Greiter is credited with introducing the concept of sun protection factor (SPF) in 1962, which has become a worldwide standard for measuring the effectiveness of sunscreen when applied at an even rate of 2 milligrams per square centimeter (mg/cm^2). Some controversy exists over the usefulness of SPF measurements, especially whether the 2 mg/cm^2 application rate is an accurate reflection of people's actual use.

Newer sunscreens have been developed with the ability to better withstand contact with *water*, *heat* and *sweat*." [6]

The authors have imagined an advanced sunscreen products must meet the following criteria: efficient, natural, easily available in large quantities, cheap, non-toxic, antioxidant. As a first step, fulvic acids were taken into account, and the authors examined if, on the basis of the UV absorption of these substances, it may be used as the component of the sun protection cream.

FULVIC ACID

"Agricultural soils contain approximately 3% soil organic matters, 3% water and 94% inorganic compounds. The soil organic matters consist of humic substances (humic acid , fulvic acid and humin) and smaller amounts of carbohydrates, N-containing compounds and lipids . Chemically, the structure of humin is similar to that of humic acid but it is strongly complexed by clays and hydrous oxides and cannot be extracted by either dilute base or acid. humic acid and fulvic acid consist of similar amounts of aliphatic and aromatic carbon atoms. In addition, fulvic acid has components with lower molecular weight but it is richer in carboxylic groups." [7]

Humic substances include fulvic acids. The real humic substances are macromolecules of complex composition, having acidic character formed of plant and animal residues in soil. They cannot be described by a molecular formula, and their molecules have similar characteristics, but their molecular structure and configuration is different.

The classification of humic substances

The humic substances are divided into three basic groups in the soil science literature, by selective solution:

1. fulvic acids
2. humic acids
3. humin materials

Fulvic acids dissolve in dilute alkali solution, and even if using weak acidic solution they are not precipitated. These substances are the smallest molecular size, they have a molecular weight of about 2000 daltons. It has the highest oxygen content (45-48 %) and lowest nitrogen content (less than 4%). Due to the low molecular weight, in neutral or slightly alkaline pH range, the excess of negative charge on their surface is sufficient for the peptization of the macromolecules, thus means a significant mobility in soil. [8] *"Fulvic acid (Buffle's model) consists of naphthalene rings substituted with hydroxyl, carboxyl and short aliphatic chains containing alcohol, methyl, carboxyl and carbonyl groups. "* [7]

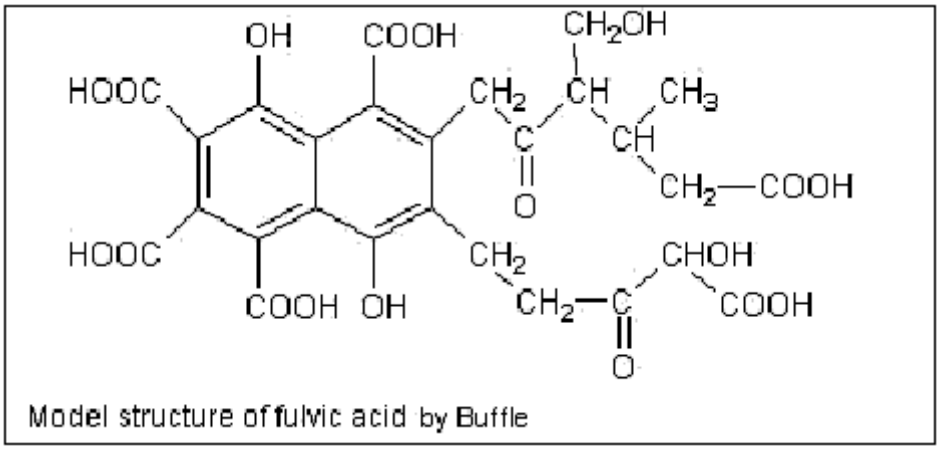


Figure 3. Model structure of fulvic acid [9]

Production of fulvic acid

After the extraction of peat, acidify the solution of the humic acid with dilute hydrochloric acid and then the grey brown humic acids exude and precipitate. The fulvic acids remain in the solution and they are yellow. This yellow aqueous layer is separated by aspiration or decantation and concentrated where the temperatures do not exceed 70°C. The dried residue is the fulvic acid.

UV absorption of fulvic acid

In order to use the fulvic acid as sunscreen substances, need to examine if it absorbs in the adequate ultraviolet spectrum. During the study, the authors found that the solution of fulvic acid absorbs in both UVA and UVB spectrum. This is illustrated in the following graph:

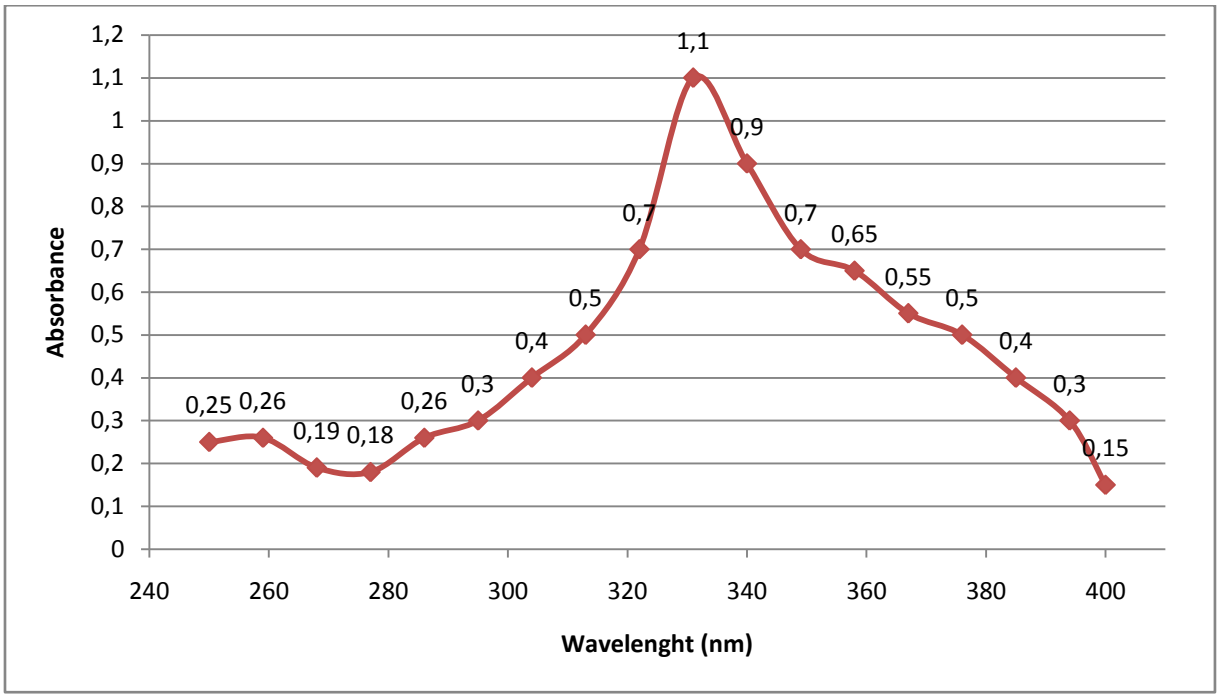


Figure 4. Rate of absorbance of fulvic acid (source: authors)

SUMMARY:

In this article, the fulvic acid was presented, a naturally occurring, non-toxic substance that can be expensively produced as potential sunscreen substance. As a result of the absorption test, a new substance fitted in their planned set of experiments was known, that can be the component of the sunscreen substance the authors had planned.

The authors are planning the similar analysis of other substances i.e. red grape extract, polyphenol, and the UV protective effect of the different composition of these substances.

References

[1] Kolonics Gábor: A korszerű UV sugárvédelem szükségessége a Magyar Honvédségben-Hadmérnök IV. évf. 3. szám (2009. szeptember)

[2] Nicholson WL, Schuerger AC, Setlow P. 2005: The Solar UV Environment and Bacterial Spore UV Resistance: Considerations for Earth-to-Mars Transport by Natural Processes and Human Spaceflight; Mutat Res. 571 (1-2): 249-264.

[3] Hegedüs Márton - DNS alapú biológiai dozimetria kiterjesztése széles spektrumú UV hatásra Budapest 2006 - Semmelweis Egyetem Doktori Iskola – Elméleti Orvostudományok Program: I/3. Ionizáló és nem ionizáló sugárzások biológiai hatásai

[4] Dobozy Attila dr. -Tabularium dermatologiae 2002 Melania Kiadói Kft.

[5] Nilsson A. 1996: Ultraviolet Reflections: on the basis of Life Under a Thinning Ozone Layer

[6] http://en.wikipedia.org/wiki/Sunscreen#cite_note-1 2013.03.15

[7] Patchreenart Saparpakorn , Jae Hyoun Kim and Supa Hannongbua: Investigation on the Binding of Polycyclic Aromatic Hydrocarbons with Soil Organic Matter: A Theoretical Approach - Molecules 2007, 12, 703-715 ISSN 1420-3049

[8] http://mkk.szie.hu/dep/talt/czi/soilchem/talkem.pdf 2013.03.15

[9] Buffle, J.; Greter, F. L.; Haerdi, W. Measurement of complexation properties of humic and fulvic

[10] acids in natural waters with lead and copper ion-selective electrodes. Anal. Chem. 1977, 49,

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Molnár Zsolt
molnar.zsolt@kvk.uni-obuda.hu

INTEGRATED CIRCUIT FOR MILITARY AND DEFENSE PURPOSES, SUPPORTING THE TESTING OF ANALOG CIRCUITS WITH USE OF BIST

Abstract

The increase in the number of electronic systems – just like in electronic military systems –, the increase of complexity, and the high demands of reliability and operation safety requires new error diagnostic methods. It is relatively simple testing by method of BIST (Built-In Self Test) the digital devices which are compatible to IEEE-1149.1 boundary scan standard. On the other hand, built-in self testing analogue or mixed signal circuits are difficult, or it is can't implement. In this paper I suggest to create an integrated circuit, or functional "building block", which can be controlled over IEEE-1149.1, and it is able to generate the current for measurement purposes, and to sense the produced voltage.

Az elektronikai rendszerek – és így a katonai elektronikai rendszerek – számának növekedése és összetettebbé válása, valamint a velük szemben támasztott megbízhatósági és üzembiztonsági követelmények teljesítése új hibadiagnosztikai módszerek alkalmazását teszi szükségessé. A peremfigyeléssel (IEEE-1149.1) rendelkező digitális áramkörök bevonása a beépített öntesztbe viszonylag egyszerűen megvalósítható. Ezzel szemben az analóg vagy kevert jelű áramkörök beépített öntesztbe vonása nem, vagy csak nehézkesen valósítható meg. Jelen cikkben javaslatot teszünk egy olyan integrált áramkör, illetve funkcionális egység létrehozására, amely IEEE-1149.1 peremfigyeléses buszon keresztül vezérelhető, és képes előállítani a kevert jelű áramkörök beépített öntesztéléséhez a gerjesztő áramot, és mérni a válaszfeszültséget.

Keywords: *self test, mixed signal test, boundary scan, automatic testing ~ önteszt, kevert jelű teszt, peremfigyelés, automatizált tesztelés*

INTRODUCTION

The large part of the military and defense electronic devices and equipment not work at a fixed location, but they are mobile. These mobile devices the user brings to its destination, then uses (enjoying the benefits of mobility, such as hand or body-mounted operation), or may be temporarily installs them. A part of the field devices operates autonomously for some time (e.g unattended ground sensors), then after a while it becomes inoperable or will be destroyed. However, during the operation, these devices should provide highly reliable data, because they often give strong points for high-level decisions. As an example, can have an autonomous land or air robot's operation safety: case of failure they can make personal injury and/or property damage.

At field devices – in electronic aspects – there are many problems due to the extreme conditions during the operation and testing. Examples are the extreme temperature or relative humidity, impurities such as dust, solid and liquid materials (e.g. sand, rain), and mechanical stress (shock and vibration). These problems are not (or only moderately) occur at a non-field equipment.

During the manufacturing of electronic devices, the Boundary Scan technique became a very important, almost indispensable technology. Most of the modern, complex digital devices (e.g. processors, FPGAs, FLASH memories, ASICs) contain the additional circuits (overhead) for Boundary Scanning, which also used for testing the individual integrated circuit, before the installation. On a circuit board, or in an electronic system, the number of the electronic devices, which can be tested by Boundary Scan can be increased by appropriate component selection (e.g. using a boundary scanneable bus driver instead of one without it), or in complex systems by using additional or extra components such as Scan Path Linker or Addressable Scan [1]. By using the technique described in the standard IEEE-1149.1 [2], the test tasks arising during the production can be performed by the inspection of digital circuits and their surroundings (connections, clusters), and the programming and configuring of programmable devices, such as FLASH memories, FPGAs and processors.

But a system – in most cases – cannot be considered pure digital, because the most of the "real world" signals are analog, so the system's interface is analog too (e.g. input and output ports of a data acquisition board). Therefore there are digitizers and "analogizers" (A/D and D/A converters), and additional functions (amplifiers, filters, etc.). To involve these analog and mixed-signal circuits into the tests is very difficult, or – in some cases – impossible. However, to increase the fault-coverage, and need to apply only one test technique, it can be beneficial, if analog circuits could be tested by boundary scan technique. The analog, or more precisely the mixed-signal boundary scan test method was standardized in 1999, known as IEEE-1149.4 [3]. In certain applications, it is very important to understand, that the circuit testing could be performed without connecting external devices. For example in a difficult to access field or remote device it is a very big advantage, if there is a built-in test controller, which can conduct the test, and can evaluate the results. In this case, the investigation can be remote-initiated, or it can be a scheduled, and can be executed by the built-in test controller. This technique is called Built-in Self-Test (BIST).

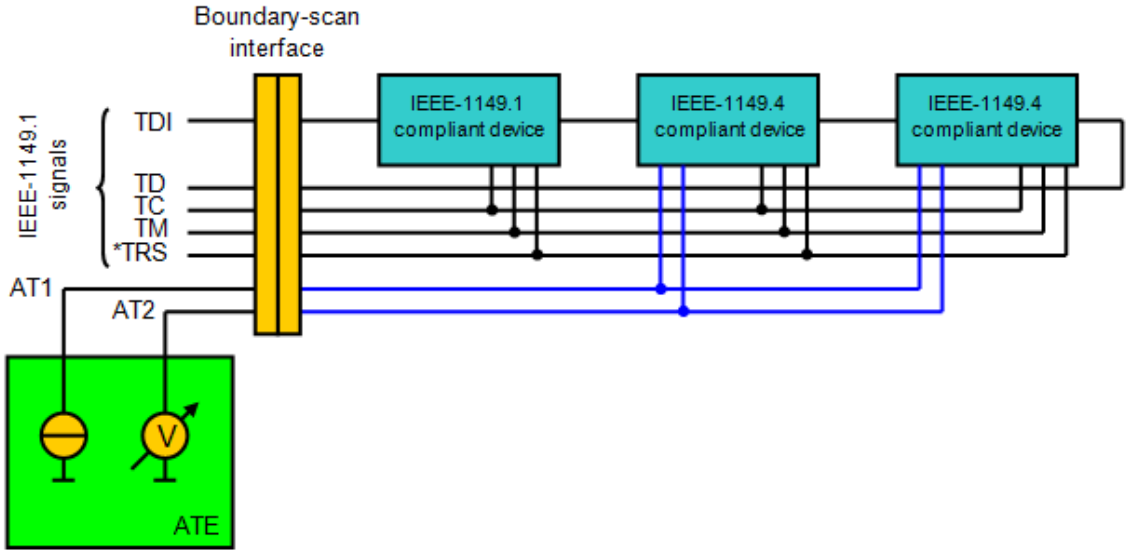
I. EXAMINIG CIRCUITS BY MIXED SIGNAL BOUNDARY SCAN TEST

For preparing a mixed-signal boundary scan test, there must be an additional infrastructure compared to digital scanning. Addition to the required digital lines, required by IEEE-1149.1 (TDI, TDO, TCK, TMS, *TRST), there is a need for two analog lines (AT1 and AT2). The line called AT1 is to carry the stimulating current, and line AT2 is for measuring the induced

voltage. The target in IEEE-1149.4 standard is to measure impedances at 1% precision, in range 10 Ω…100 kΩ, and recommends the following [3]:

- the upper cutoff frequency is a minimum of 100 kHz, the allowed variation in the transmission is 0.5% between 10 Hz and 10 kHz
- the minimal range of the excitation (measuring) current is in a range of ±100 μA (this current the line AT1 must have to endure)
- the induced voltage must stay in the range of Vss-100 mV and Vdd+100 mV

According to the standard, for testing it is necessary to apply an external current source, for providing the measuring current trough the line AT1, and a voltmeter on AT2, for measuring the voltage generated by the measuring current on the tested impedance. (Of course, if one only wants to measure a voltage on a test point, the injection of the measuring current is not necessary.) In most cases, the current source and the voltmeter are provided by an Automatic Test Equipment (ATE) as seen on Fig. 1.



1. figure. The IEEE-1149.4 infrastructure, and the connection of an external AutomaticTest Equipment (edited by the author)

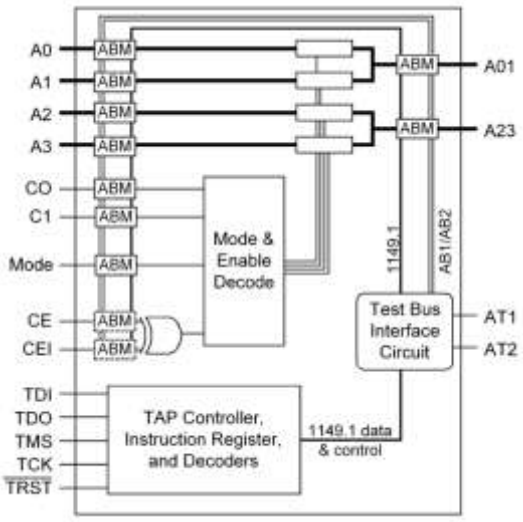
The IEEE-1149.4 standard defines 10 commands, of which are mandatory, and optional. These commands are described in details in the standard [3].

Mixed signal boundary scan solutions according to IEEE-1149.4, and non-compliant solutions

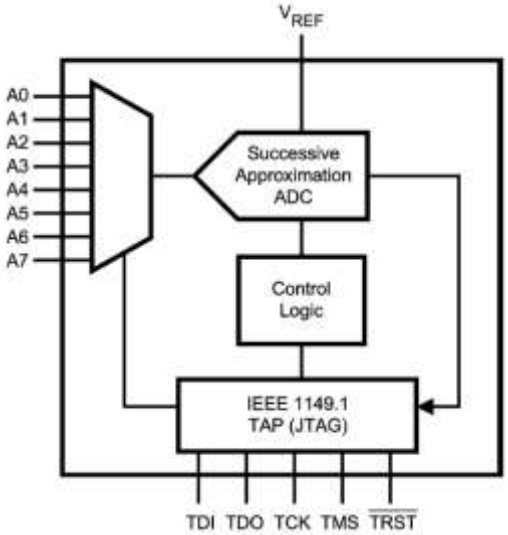
Unfortunately, nowadays testing analog circuits using mixed-signal boundary scan is not widespread, actually an untapped potential. There was only one purchasable device, which fully implemented the IEEE-1149.4 standard. This device called STA400, manufactured by National Semiconductor until 2011, when Texas Instruments acquisited National Semiconductor. In 2013, it is not known, that TI intends to manufacture this device (or an improved one) or not. The STA400 is a dual 2:1 analog multiplexer, which can be configured as a single 4:1 multiplexer [4]. On 11 pieces of analog pins there are Analog Boundary Modules (ABM), and the device can be connected to the IEEE-1149.4 test bus. It can be also interesting, that the device can be configured to "virtual probe" mode. In this mode the user can use 9 of the device pins as a voltmeter input (PROBE operating mode).

The other device, which is suitable to measure analog voltage on multiple points, designated as STA476, but this device is not IEEE-1149.4 compliant. (STA476 was also manufactured by National Semiconductor, and this component is manufactured by Texas

Instruments in 2013.) This device contains a 12 bits A/D converter, and an 8-input analog multiplexer [5]. The A/D converter has a voltage reference input, so the measuring range can be fit to the application. The multiplexer can be programmed via boundary scan bus, and the result of A/D conversion can be read by this way. The main application of STA476 are diagnostics, testing and service-supporting [5]. The internal structures of STA400 and STA476 are shown on Fig. 2 and Fig 3.



2. figure. Structure of STA400 [4]



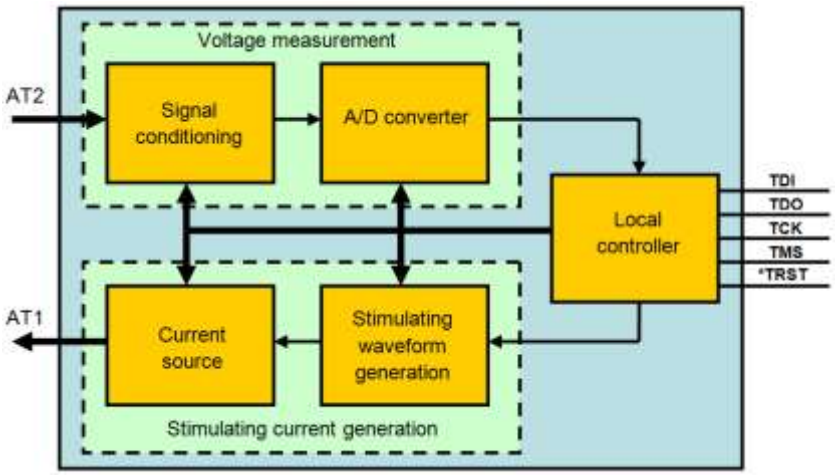
3. figure. Structure of STA476 [5]

II. REQUIREMENTS FOR AN INTEGRATED CIRCUIT SUPPORTING THE TEST OF MIXED SIGNAL COMPONENTS

If a digital circuit is tested by an embedded test controller, the test controller must generate test vectors for boundary testing. The test vector generation can be performed by an implemented algorithm, or by reading the previously computed vectors from the memory. After the evaluation of responses of the tested circuits one can decide, whether it is operating error-free or not. The stimulus and the response are both serial digital information, and it is optimal for a digital test-controller.

Testing a mixed signal circuit is a special case. Stimulating an analog circuit requires analog stimulus, and the response is analog too. In a mixed signal circuit to perform a test by an embedded test-controller, without connecting any external equipment, there is a need for an analog source (current or voltage), and an analog measuring unit. For performing these analog tests, the source and the measuring unit must operate with high precision, because the test must be accurate and reproducible. The built-in test controller can be any device, which can be empowered by "intelligence": DSP, FPGA or microcontroller. Some of these devices are not (or not fully) able to generate analog stimulus and measure analog response. The FPGAs are totally digital, and not able to handle analog signals. Most of DSPs do not contain analog peripherals such as A/D or D/A converters. Microcontrollers usually contain analog peripherals: 8…12 bits resolution, multi-channel A/D converter is common, and there are a few types, which have D/A converter. The alternate method to generate analog signals is the PWM module (which is a frequently used peripheral), but it requires a good quality external (active) analog filter, and it is not suitable for frequencies above few kHz. In overall, the quality of a microcontroller's analog peripherals is not good enough for precise tests.

Performing mixed signal self-tests by embedded test-controller in a mixed signal circuit requires an integrated circuit, which can solve the problem described above. Handling, controlling and reading the measurements of this integrated circuit, it is the obvious way to be done it through the IEEE-1149.1 test bus. The main functions of this integrated circuit are: to generate the stimulating current, and measure the response voltage (Fig. 4.) In the local controller can be implemented extra functions, such as computing various signal parameters (e.g. RMS, Fourier-spectrum, etc.). In the following, we discuss the several topics of developing this prospective integrated circuit. The aim is not to perform these built-in tests (for checking the functionality of the analog circuits) at high precision (but relative precisely), therefore yielding a 2% error for the entire measurement chain.



4. figure. Block diagram of integrated circuit supporting mixed signal boundary test (edited by the author)

The primary target is to create a model, which would be built up with existing, factory components, and able to demonstrate the usefulness of the prospective integrated circuit Secondary target is to examine how can be this circuit implemented as an integrated circuit. Researches in connection with these two topics we will review in a future article.

Requirements of generating analog stimulating signal

1. The current source must be able to generate stimulating current from DC to the maximum of the measuring frequency (to line AT1). The variation in signal amplitude must be less than 0,5%
2. The maximum frequency of stimulating signal is at least 100 kHz – in line with the values fixed in the IEEE-1149.4 standard.
3. The peak value of the stimulating current – also according to the IEEE-1149.4 standard – must be at least ±100 μA. (If we want to measure lower impedances at adequate precision, we need to provide higher peak values (at least ±1 mA). This range can be used in that case, if the infrastructure (mainly the analog test line AT1, and the integrated switches and circuits of connected circuits) is able to tolerate this current.

Requirements of measuring analog response signal

1. The measuring "instrument" must be able to measure DC and AC voltages at least between the power lines (0…5 V), up to 100 kHz (or up to the maximum frequency of the current generator).
2. The measurement error must be equal or lower than 0,5%.
3. If it is possible, must be suitable to calculate various signal parameters such as peak voltage, RMS value, Fourier-spectrum, etc.

III. OPPORTUNITIES OF IMPLEMENTATION

The next paragraph is a brief overview of the main ways to generate analog stimulating signal.

Analog function generator

At this technique the frequency of the oscillator is determined by analog components (R-C, L-C). Tuning these components is difficult, it do not fit to the digital systems. Maybe only the resistor of these components can be tuned digitally. The digital potentiometers can't be tuned continuously, there are 64…1024 fixed steps, the value of the resistor can be controlled by host processor via SPI or I2C bus. The voltage on the resistor can't exceed the power supply lines, which is usually in range 0…5 V. These potentiometers can be used up to 50…4000 kHz, the bandwidth depends on the nominal value of the resistor, higher the value, the maximal frequency will be lower. The inductor and the capacitor can't be tuned by this or similar way. Only it is possible to change fixed value capacitors or inductors by an analog multiplexer to change the frequency range. As we know, integrated, continuously tunable capacitor and inductor with suitable precision and stability, and at acceptable price can't be realized using the manufacturing technologies of today. It should be noted that the analog signal generator can generate only one waveform (sinusoidal or triangle), other waveforms can be produced only by signal shaping circuits. My opinion to produce stimulating signal by analog method is not recommended.

Generating stimulus by pulse-width modulation (PWM)

Using pulse-width modulation can be produced DC and AC signal. In digital systems due to the unipolar power supply it is suitable to use unipolar PWM signal (Fig. 5.). The signal amplitude is Vdd (Logic High level) during the pulse, and 0 V (Logic Low) when it is switched off.

If the pulse-width or duration (D) and period (T) of the PWM signal are constant, the average value of PWM signal is DC, and the value is defined by pulse duration (D). If it is desired, can generate AC signal by changing the pulse width. The average value of the PWM signal is:

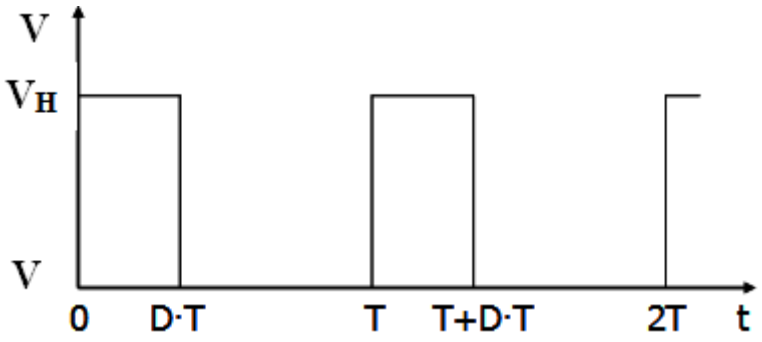
$$\overline{V} = \frac{1}{T} \cdot \int_0^T f(t)dt = \frac{1}{T} \cdot \left(\int_0^{D \cdot T} V_H dt + \int_{D \cdot T}^{T} V_L dt \right) = \frac{1}{T} \cdot (D \cdot T \cdot V_H + T \cdot (1-D) \cdot V_L) =$$

$$\underline{\underline{D \cdot V_H + (1-D) \cdot V_L}}$$

1. Equation.

And whereas $V_L = 0\,[V]$, so $\overline{V} = D \cdot V_H\,[V]$

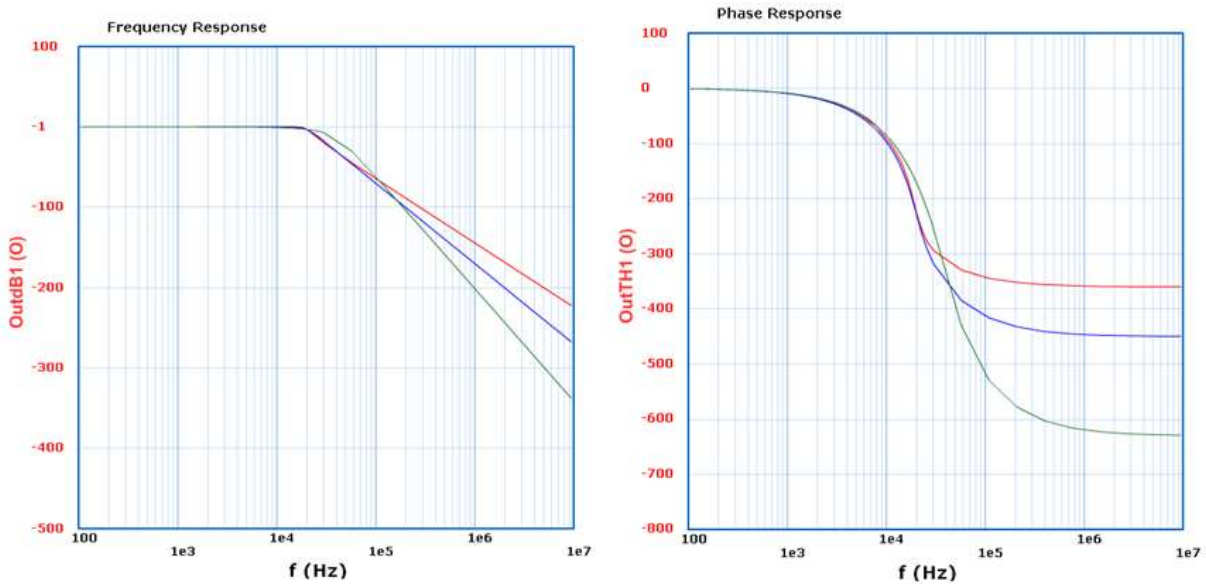
2. Equation.



5. figure. Unipolar PWM signal (edited by the author)

For generating alternating voltage, pulse width should be changed. For basic waveforms (sinus, triangle, square) to achieve an acceptable signal quality (shape fidelity, distortion…) the frequency of the PWM signal must be twice to five times higher, than the frequency of the generated signal. This ratio is affected by the parameters of the averaging circuit.

For averaging, a low-pass filter can be used, which can be realized by passive or active circuit. The closer the generated frequency to the PWM frequency, and the smaller the variation of the response, the higher order filter should be used. Suppose, that the PWM frequency is 100 kHz, and the generated signal frequency is 10 kHz, and we want the PWM frequency presence is no more than 0,1% in the generated signal. In this case at 10 kHz we must provide at least 60 dB rejection to 100 kHz signal components. For demonstrating, I used the Texas Instruments's WEBENCH® Active Filter Designer tool [6]. I simulated a filter, which has cutting frequency of 20 kHz, the stop band starts at 100 kHz, where the attenuation should be at least 60 dB. On the Fig. 6. the simulating results (frequency and phase response) can be seen. There is three different filters, with a minimum required order (Red: 4^{th} order Chebyshev (0.1 dB ripple), blue: 5^{th} order Butterworth, green: 7^{th} order Bessel). The attenuation of the filters at 100 kHz: Chebyshev - 64 dB, Butterworth – 69.9 dB and Bessel – 64-6 dB.



6. figure. Frequency and phase response of the filters designed in the Active Filter Designer (cut out from the Active Filter Designer [6])

For generating alternating voltages, the duty of the PWM signal should be redefined in every signal cycle. This can be done by reading stored (pre-computed) values from a table, or can be computed in run-time. The first solution has a low resource requirement, and can be used well for standard waveforms. The second solution has higher resource requirement, but can be used at special waveforms.

The signal generation by PWM method fits well to digital systems, and can be used for generating DC or AC signals. But the PWM frequency limits the signal frequency (and the PWM frequency is limited by the microcontroller's peripherals). This method requires a high order active low-pass filter, it's parameters are critical.

Generating analog signals by D/A converter

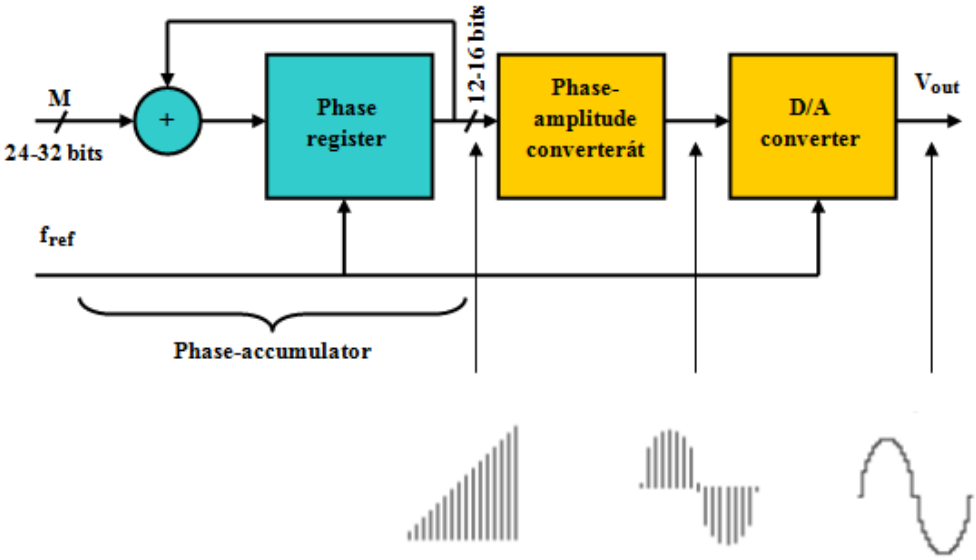
There are many types of D/A converters, they fit optimally to digital systems. They require voltage reference to operate, which determines the accuracy and stability of the converter. Quality characteristics easy to control, and high precision D/A converters can be realized inexpensively. Using D/A converters it is possible to generate AC or DC voltage or current.

To generate AC output, similar methods are possible than as we have seen at PWM, and the problems are similar too. If we want to generate DC voltage, there is no need for filter, but it is necessary for generating AC output. If we want to achieve precision of amplitude of 0,1%, we need at least 10 bits converter. As the converter has errors, we need 11 or 12 bits converter, which can be integrated cheaply and easily.

Using D/A converters is a realistic alternative for generating analog test stimulus.

Generating analog signals using method of direct digital synthesis (DDS)

Direct digital synthesis is a modern method for generating analog signals. It has high precision (high resolution), wide frequency range and excellent stability, because uses crystal oscillator as reference. Can be controlled easily by the host, only one tuning word determines the output frequency. The method is suitable to generate various periodic signals, although it is basically planned to generate sinusoidal output. The structure of the DDS generator is shown on Fig. 7.



7. figure. The structure and basic operation of the DDS signal generator (edited by the author)

The phase accumulator adds the M tuning word to the previous value of the phase register, scheduled by reference frequency (f_{ref}). The upper 12…16 bits of phase accumulator addresses a phase-amplitude converter, which is actually a memory. The memory contains the numeric amplitude values for each phase. The data read out from this memory is the input for the D/A converter, which produces the analog signal. The specialty of the phase accumulator is that, there is no phase-jump passing through the 0 phase point, the output phase is continuous.

The filtering of the analog signal on the DDS generator's output has a very high effect to the signal quality. In our case, the maximum frequency of the generated signal is 100 kHz, and the reference frequency of DDS generator is 20…100 MHz (depends on the used device), the output filter's specification is not very strict: it is enough to use 1^{st} or 2^{nd} order low pass filter. As the DDS technique requires only digitally controlled elements (memory, register, digital multiplexer), so optimally suited for digital systems. DDS technique is suitable for generating basic and special waveforms, and it is suitable for generating DC voltage, if the phase-amplitude converter contains the same value for each phase point.

The current generator

As the stimulus applied to the analog test line AT1 should be a current, so the generated signal must be converted to current, or must be amplified. In that case, if the generated signal is a voltage, there is a need for a voltage-current converter. If the generated signal is a current, it should be amplified to the desired level. The current generator must provide the proper load capacity, the stability and the accuracy. As the full signal chain error was fixed in 2% (1% due to the stimulus, and 1% for the measurement), so the error of the current generator should not exceed a few tenths of a percentage. These criteria are achievable easily with an integrated sub-circuit. This hypothesis is confirmed, if we examine the off-shelf voltage controlled current source devices' characteristics.

In the next, we provide a brief overview of the implementation opportunities of the circuits in relation of the measuring the analog signals.

Signal conditioning

The measuring amplifier, the "analog front end" is a very important chain link. If it has not an appropriate quality, despite the precision of the A/D converter, the conditioned input voltage will be affected by errors, and can't be determined the accurate value of the input voltage. The main function of the measuring amplifier to transform the relative wide input voltage range into the voltage range of the A/D converter, without offset and amplification error, and with high linearity in amplitude and frequency. There is no need for extra protection on the input of the amplifier, because the usual problems (overvoltage, ESD, etc..) will not occur on the input, due to the closed environment.

The IEEE-1149.4 standard of the mixed-signal boundary scan targets to measure impedances between 10 Ω and 100 kΩ. If the stimulating current is the maximal (100 μA), the response voltage will be in the range of 1 mV and 10 V. As can be seen, if we want to transform these voltages into the range of the A/D converter, there is a need for amplification at low voltage levels, and attenuation at high voltage levels. This will provide the optimum conversion accuracy. In the table below (Table 1.) there is a summary of the resistance ranges, stimulating current values in particular ranges (I_m), and the necessary amplification in each range (A_v).

(At the calculations it was considered, that the optimal range is used, i.e. the lower 10% of the ranges is not used.) The shaded lines overfulfill the measurement range described in the standard.

In the signal conditioner there is a possibility to analog computing of some signal parameters, such as peak value, average value or effective value. However these computations can be performed in an intelligent system controller at a higher performance, and with a lower error. If it is necessary it is a need to be implemented an anti-aliasing filter in the signal conditioner.

Range	I_m	A_v	V_{AD}
10 Ω	100 μA	2500	0…2.5 V
100 Ω	100 μA	250	0.25…2.5 V
1 k Ω	100 μA	25	0.25…2.5 V
10 k Ω	100 μA	2,5	0.25…2.5 V
100 k Ω	25 μA	1	0.25…2.5 V
1 M Ω	2.5 μA	1	0.25…2.5 V

1. table. Some parameters of the signal conditioner (impedance measurement) (edited by the author)

The A/D converter

A wide variety of A/D structures are known (e.g. flash, successive approximation, integrating (dual slope), sigma-delta). The today's technology enables to manufacture relatively cheap A/D converters with resolution of 8…20 bits, above this resolution increases the cost of production. The speed of digitizing is one of the important characteristics. If we want to process a signal with a frequency of 100 kHz, it should be sampled at more than 200 kHz, according to the Nyquist rule. So there is a need for an A/D converter, which has at least 200 kS/s sampling rate. The higher the sampling frequency, the lower the requirements of the anti-aliasing filter (e.g. it is enough lower slope, i.e. lower order). In resolution, it is required that at the 10% of the measurement range the measurement error should be less than 0.5%. According to Table 1. the minimum voltage to measure is 0.25 V, so the resolution is lower or equal than 1.25 mV (Eq. 3.)

$$r = 0.25\,V \cdot 0.5\% = 1.25\,mV \qquad \text{(Equation 3.)}$$

If the full scale is 2.5 V, Eq. 3. determines the minimal resolution of the converter:

$$N = \log_2(2.5\,V / 1{,}25\,mV) = 10.97 \qquad \text{(Equation 1.)}$$

so there is a need for an ideal 11 bits A/D converter. If the converter has the error of 1 LSB, we can use a 12 bits A/D converter. In speed, resolution and price one of the options to choose an successive approximation A/D converter. This type of ADCs is widely used in microcontrollers, e.g. in Microchip's PIC30F1010 there is an 12 bits, 2 MS/s successive approximation A/D converter [7].

The reference needed for A/D converter can be integrated well, easily can be found of the manufactured devices, which has the error less than 0.1%, and stability is better than 50…100 ppm.

Controller

The main function of the controller is to communicate through the JTAG interface, and to coordinate the units in the planned integrated circuit. The built-in test controller instructs the measurement controller to perform tests (e.g. to measure an impedance, or voltage), then reads the results from it. The measurement controller sets the stimulating signal's frequency, waveform and amplitude, sets the current source (if necessary), sets the signal conditioner's parameters, then starts the measurement, and collects the results.

Further functions can be implemented in the measurement controller, as mentioned above. If there is a need to compute some signal parameters, the controller must store many digitized values in an interval, then it can compute the required parameters. In this case the controller should have a relatively high intelligence. If we use a DSP, it is able to control the inner units, and to compute signal parameters, so it can be a good choice for measurement controller.

By this time, we use a DSP in the planned integrated circuit, it is only the imagination is the limit to what kind of capabilities will have the device. Also requires additional considerations, where to draw the limits: which functions will be in the measurement controller, and which functions will be in the built-in test controller.

SUMMARY

In year 2013 there is no device which has these features described above. The planned integrated circuit can help to spread the mixed-signal boundary scan, and outlines new built-in self-test applications. If we extend the boundary scan self-test the more circuit element, the fault coverage will be higher, and can be decided more reliably if the circuit or device is functioning well, or not. In many applications it is very important that the occurring faults can be detected before the malfunction can produce incorrect information.

Testing of military and defense field devices is very important due to the increased risk of failure and to achieve the continuous reliability. However, the circumstances of testing are very special. So at designing a field equipment efforts should be made to avoid the need of external devices for testing, and the tests to be carried out by the user or the equipment itself. This aim would be achievable more easily by using this proposed integrated circuit.

In the next, there are a number of questions remain to be examined. It is very important to create a model of this circuit built up with off-shelf parts, and this model will help to decide if the planned structure is functional or not. The basis of experiences can be designed the integrated circuit. The measurement functions to be implemented can be supplemented by special ones, in addition to the standard functions. E.g. in some cases it is useful to perform tests with stochastic stimulus, however, these methods are require very different approach, and a very different measuring methods, as usual.

References[1]

[1] Adam W. Ley, „A Look at Boundary Scan From a Designer's perspective", Asian Sources Media Group, 1996, (http://focus.ti.com/lit/an/scta028/scta028.pdf)

[2] IEEE Computer Society: IEEE Standard Test Access Port and Boundary-Scan Architecture (IEEE1149.1-1990, includes IEEE Std 1149.1a-1993), IEEE Inc., New York, 2003

[3] IEEE Computer Society: IEEE Standard for a Mixed Signal Test Bus (IEEE Std 1149.4-1999), IEEE Inc., New York, 2000

[4] Texas Instruments: AN-1200 Mixed Signal Testing Using the IEEE 1149.4 STA400, Application report, Texas, 2004 (http://www.ti.com/lit/an/snla052/snla052.pdf)

[5] Texas Instruments: SCANSTA476 Eight Input IEEE 1149.1 Analog Voltage Monitor Data Sheet, Texas, 2005 (http://www.ti.com/lit/ds/symlink/scansta476.pdf)

[6] WEBENCH Active Filter Designer program (http://webench4.ti.com/filters/)

[7] Microchip: dsPIC30F1010/202X Data sheet, 2006, (http://ww1.microchip.com/downloads/en/DeviceDoc/70178a.pdf)

[1] Internet links of the documents were available on 13.03.2013.

HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Péri Márton
peri@it.ppke.hu

BOOK REVIEW. MICHAEL M. GUNTER: *ARMENIAN HISTORY AND THE QUESTION OF GENOCIDE.* PALGRAVE MACMILLAN 2011

Abstract

Michael M Gunther, Professor of Political Science at Tennessee Technological University, a renowned expert of the Kurdish question and Armenian terrorism has recently set out to deal with the Armenian Turkish relations with a special attention to the issue of the Armenian genocide. [1] [2] He intends to shed light on the more than a century old enmity between the two nations on the Eastern frontier of NATO which due to its rather complex implications[1] might still pose a major security threat to Europe, not to mention the delicate setting that the overwhelmingly Muslim Turkey as a NATO member has a still unsettled dispute with a nation that is linked to Europe with several ties and has politically influential immigrant communities both in Western Europe and in the USA.

Michael M Gunther, a Tennesse Technological University-n a politikai tudományok professzora, aki nemzetközileg elismert szakértője a kurd kérdésnek, valamint az örmény terrorizmus kutatója nemrégiben jelentette meg új kötetét, mely a török-örmény kapcsolatokkal foglalkozik. A mű a téma kifejtése során különös figyelmet szentel az örmény népirtás problematikájának. A NATO keleti határán élő két nép közötti több mint egy évszázados ellenségeskedés részleteit igyekszik feldolgozni, mely a jelen korban is biztonsági kockázatot jelenthet Európára. Azt a kényes helyzetet nem is említve, hogy a többségében muszlim, NATO tag Törökország egy olyan országgal szemben áll többé-kevésbé nyílt konfliktusban, amely Európához ezer szállal kapcsolódik és politikailag befolyásos emigráns csoportokkal rendelkezik mind az USA-ban, mind Nyugat-Európában.

Keywords*: Turkish-Armenian conflict, holocaust, genocide, Armenian terrorism ~ török-örmény konfliktus, holokauszt, népirtás, örmény terrorizmus*

[1] Especially at the time of the writing of the present review, February, 2013, when the possibility of a conflict between the West and Iran, a neighbour of Turkey and Azerbaijan, cannot be excluded, which event can very easily revive hostile sentiments in the region.

1. INTRODUCTION

In the foreword of his book Gunther claims that since the issue of the massacres during WW I has been approached rather unilaterally by the international literature from the Armenian perspective he proposes to 'present objectively the Turkish point of view on this subject'. By doing so he hopes to establish a more balanced picture of the events, putting it in the context of Armenian terrorism in the second part of the 20th century, and to encourage the improvement of the Turco-Armenian affairs that has reached an important phase in 2009 by the signature of treaties concerning the establishment of mutual diplomatic relations and the creation of a historical commission to analyse their different versions of history.[2] [3]

2. WHAT IS GENOCIDE?

The term first was used by the Polish-born journalist Raphael Lemkin and acted as an American advisor during the Nuremberg Tribunal. In his work *Axis Rule in Occupied Europe: Laws of Occupation, Analysis of Government, Proposals for Redress* (1944), Lemkin suggested that the crucial element of genocide was: a criminal intent to destroy or to cripple permanently a human group. The acts are directed against groups as such, and individuals are selected for destruction only because they belong to these groups. [4] The conclusions of the above mentioned trials and the Nazi atrocities revealed after the war motivated the UN General Assembly of Resolution 96-I (December (1946) which deemed genocide to be punishable by international law and prepared the way for Resolution 260-III (December 1948), which approved the text of the Convention on the Prevention and Punishment of the Crime of Genocide, the first UN human rights treaty ratified by more than 130 countries (the US ratified it only in 1988).

The second article states that the definition of genocide is the following: 'any of the following acts committed with intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such: (a) Killing members of the group; (b) Causing serious bodily or mental harm to members of the group; (c) Deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part; (d) Imposing measures intended to prevent births within the group; (e) Forcibly transferring children of the group to another group.' [5] Nonetheless critics object that governments never disclose their intents openly to exterminate a group rather they tend to label their actions as some lawful steps in connection with the somehow 'problematic' group or simply attempt to reestablish 'law and order' 'breached' by the given community (Saddam Hussein applied chemical weapons against the Kurds in the 1980's in order to suppress their upheaval, the Turks fought the insurgent Armenians and their losses were simply war casualties during WWI, etc.). [6]

The first instance when the genocide convention was invoked before an international court took place in 1993 when Bosnia and Herzegovina expressed its concerns concerning the Yugoslav breach of the above convention. Later the UN convoked the International Criminal Tribunal for the Former Yugoslavia (ICTY) and the International Criminal Tribunal for Rwanda (ICTR) for the clarification of atrocities during these events. The growing international attention in relation to the field is displayed by the fact that the Rome Statute of the International Criminal Court (ICC), adopted in 1998 in Rome by some 120 countries, entered into force in 2002 (It needs to be remarked though that the US, Russia and China was not amongst the participating countries.)

[2] It has to be noted that the treaty is still to be ratified by both parliaments. The Turkish government has made clear that ratification was not due until the question of Karabakh between Armenia and Azerbaijan was not solved at the liking of the latter.

In the course of the twentieth century several events can be mentioned that, according to scholars qualify for being called a genocide somehow corresponding to the above mentioned criteria of genocide. Which are nonetheless sometimes debated being full scale genocides by others for diverse reasons. The unfortunately long list[3] should start with the Herero and Namaqua Genocide in German South-West Africa (1902-1904) as the first in the line throughout such a bloodthirsty century; Armenian, Assyrian and Greek Genocides (1914-1923); the Soviet killings of Cossacks (1919-1920), the artificial famine in the Ukraine and Russia: the Holodomor (1932-33); the Nazi Holocaust of the Jews and the Roma (1938-1945); the Cambodian mass killings by the Khmer Rouge (1975-1979), the Rwandan civil war mass murders 1994, and the Ethnic cleansing in Srebrenica, Bosnia Herzegovina (1995)[4]. [7]

3. THE ORIGINS OF TURKISH-ARMENIAN ANIMOSITY

Gunther starts the history of the hostility by recounting the atrocities committed by Armenian terrorists against Turkish diplomats during the 1970's and 80's. It seems to be understandable from a scholar who intends to represent the Turkish viewpoint in the debate, nonetheless possibly not entirely appropriate since it does not necessarily take the reader closer to understanding the roots of the conflict.

During centuries Armenians lived peacefully within the frontiers of the Ottoman Empire, in a region which is declared to be the homeland of several nations and where Armenians settled approx. 2700 years ago, and formed more states on their own throughout history. [8] Although Armenians, like Christians and Jews, were relegated to a secondary position compared to Muslims, they enjoyed a relative freedom and, due to their well-known talent in trade, prosperity. In the 19th century Armenians feeling more and more oppressed by the Turkish rule and threatened by the depredations of the Kurds, Circassians or other nomadic tribes their growing number started to look on European Christians and as their protectors. [9] As a consequence some Armenians supported the Russians in the course of the three wars against Ottoman Turkey. In spite of the promises Article 61 of the San Stephano Treaty secured no actual guarantees to the Armenian cause and in the coming years the European powers simply sought to play off the Turks and Armenians against each other according to their own interests. [10] The aroused Armenians continued their aspirations eventually manifesting in the formation in 1887 of the Marxist Revolutionary Party, or Hunchaks (Bells), and in 1890 the more nationalistic Hai Heghapokhakan Dashnaktsutiun (Armenian Revolutionary Federation), or simply Dashnaks while as a response Sultan Abdul Hamid II organized a Kurdish cavalry called the Hamidiye, who by tradition were the inveterate enemies of the Armenians. In 1894 Armenians in the Sassum region rejected to pay the extortionate but customary taxes which were viewed as a rebellion by the emperor. The retaliations till 1896 resulted in the death of not less than 200 000 victims.

The next wave of atrocities occurred during WWI. Although Sultan Abdul Hamid II set off a technological modernization and also acted harshly against any attempts towards the disintegration of the empire he was not able to stop the process. In 1908 he was put down by

[3] The list is obviously far from complete.

[4] Robert Melson distinguishes four waves of ethnic conflicts and genocides: the two world wars, the Post-Colonial, and post-Communist eras. He believes the Armenian Genocide and the Holocaust are the quintessence of the genre: 'a deliberate attempt was made by a government to destroy in part or in whole an ethno-religious community of ancient provenance that had existed as a segment of the government's own society.' Later he argues that the Armenian genocide rather than the Holocaust could serve as a prototype of mass murder in the past - Colonial third world as the involved minorities were territorial groups unlike the European Jews. He contends that only the Cambodian atrocities resembled to the Holocaust in the fact that it was aimed against various strata and segments of Cambodian society like the urban upper and middle classes and various ethnic communities like the Vietnamese.

the movement of the Young Turks who started their activities along the liberal and democratic principles of the 1876 constitution. [11] In spite of any hope for Western support for the modernization European powers and their allies took advantage of the Ottoman Empire which lost 40% of its territory and 20% of its population by 1911.

The Young Turks, and their political fraction, the Committee of Union and Progress (CUP), concluded that the liberal experiment failed and turned towards pan-Turkish thoughts. They intended to establish a new Turk state, extending from Anatolia to the Chinese border that would be based on Turkish ethnicity and the Muslim principles.

The war started in 1914 and the newly nationalistic Turkish state entered it on the Axis side to establish the above mentioned empire at the expense of the arch enemy, the Russian empire. This context placed Armenians into an extremely dangerous situation because they could be blamed to be in a league with the Russians and plotting against Turkey to claim its heartland, Anatolia.

4. GENOCIDE?

The traditional Turkish and Armenian historiography become antagonistic at this point. Armenians and around 80% of scholars dealing with the field assert that the Turkish government premeditatedly, under the pretence of emergency deportations, decided to systematically liquidate the whole Armenian population of Anatolia. The deportees on their march from their homeland towards the region of Aleppo were raided upon by Kurdish and Turkish villagers as well as designated killing squads, Teshkilat-i Makhsusiye. Due to the atrocities and famine the death toll is estimated up to 1.5 million according to this view.

Until recently official Turkish historiography violently denied any act of genocide or even any atrocities. It has been claimed to be the consequence of unfortunate events, where Armenian insurgents, guerrillas or bandits rose against their lawful state, the atrocities on both sides took place in a war situation but since these occurred within the border of the Turkish Empire involving its citizens, the claims of genocide should be considered as hostile propaganda.

Gunther acknowledges the distance between the two views, admitting atrocities against Armenians[5] also conceding that as a consequence they were practically wiped out of the region but questions the numbers mentioned and the premeditated nature of the events. He asserts that the Ottoman Empire, pressed by the outside enemy and internal hostility, acted in panic but its primary purpose was to defend its integrity not to initiate and execute genocide. Gunther argues further that the number of victims must be much lower, around 250-400 thousand who mostly fell victim to diseases and malnutrition rather than atrocities. Along this line he suggests that as a solution Turkey should accept some responsibility and as an act of contrition paying some financial compensation which – in his view—would placate persisting hostile sentiments.

In the following chapters the author defines genocide and tries to prove using the example of the Bosnian and Darfur massacres that the term is overused and applied rather to mire adversaries before the world. He asserts that the case of the Armenian massacre is similar, as no proof of premeditation can be found. Moreover, since it took place before the Genocide Resolution it ‘would constitute a legally untenable ex-post-facto proclamation’.

Further on in his book the author presents some secondary sources when trying to refute the claim of genocide. He attempts to establish that although the Armenian losses were painful, these were neither premeditated nor were they simply unilateral, but were rather encountered as a consequence of military activities on both sides.

[5] He agrees with the official Turkish view that the Turks also suffered significan losses in the hostilities.

In the second part of the book Gunther presents how Armenians intended to persuade the world and blame Turkey for a 'never committed genocide' using their political influence mostly in the US and through terrorist activity in the 1970's and 80's. Although this approach of the facts seems rather unfortunate and one-sided these analyses, without their farfetched conclusions, might prove useful to a reader interested in such details.

5. CONCLUSION

With his book Gunter goes further than most scholars on the 'Turkish side', but the methodology used to clarify the issue unfortunately remains questionable. Without careful examination of contemporary, both Armenian and Turkish, primary sources[6] the reasons and details of the events will remain undisclosed and open to doubt, thus allowing former 'soccer diplomacy' to continue. Without this step even the sheer number of victims will be disputed not to mention the questions of responsibility. Turkey as a NATO member, which aspires to join EU one day, will need to take a deep breath and face with this sad part of its own history in all honesty, as all other countries that somehow played a part in it, otherwise this issue will add to the several other questions that might pose a security risk to this region of the world. [12]

References

[1] Michael M. Gunther: *The Kurds and the future of Turkey*. Macmillan, I997.

[2] Mohammed M. A. Ahmed and Michael Gunter (Eds.), *The Evolution of Kurdish Nationalism Kurdish Studies Series* 7. Mazda Publishers, 2007.

[3] http://news.bbc.co.uk/2/hi/europe/8299712.stm, Last accessed 23 Feb. 2013.

[4] Raphael Lemkin: *Axis Rule in Occupied Europe: Laws of Occupation - Analysis of Government - Proposals for Redress.* Carnegie Endowment for International Peace, 1944.

[5] http://www.un.org/ga/search/view_doc.asp?symbol=a/res/260%28III%29. Last accessed 23 Feb. 2013.

[6] George J. Andreopoulos (Ed.), *Genocide: conceptual and historical dimensions.* University of Pennsylvania Press, 1994.

[7] Robert Melson: Paradigms of Genocide: The Holocaust, the Armenian Genocide, and Contemporary Mass Destructions. Annals of the American Academy of Political and Social Science, 548 (1996) 156-168.

[8] "Armenia." Encyclopædia Britannica Online Academic Edition, 2013. Last accessed 23 Feb. 2013.

[9] A. O. Sarkissian, *History of the Armenian Question to 1885.* University of Illinois Press, 1938.

[10] "Treaty of San Stefano." Encyclopædia Britannica Online Academic Edition, Last accessed 23 Feb. 2013.

[11] The Ottoman Constitution, Promulgated the 7th Zilbridje, 1293 (11/23 December, 1876), The American Journal of International Law, 2 (1908) 367-387.

[12] Taner Akçam, *From Empire to Republic: Turkish Nationalism and the Armenian Genocide*. Zed Books Ltd, 2004.

[6] Gunther fails to list any of these among his sources.