HADMÉRNÖK

KATONAI MŰSZAKI TUDOMÁNYOK ONLINE

VIII. Évfolyam 3. szám 2013. szeptember

NKE
BUDAPEST

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:

Bonnyai Tünde – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Dobor József – Nemzeti Közszolgálati Egyetem, KI adjunktus
Dr. Bottyán Zsolt – Nemzeti Közszolgálati Egyetem
Fábos Róbert – Nemzeti Közszolgálati Egyetem, HHK, adjunktus
Gulyás Attila – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Halász László – Nemzeti Közszolgálati Egyetem, HHK, professzor emeritus
Dr. Kassai Károly – Honvédelmi Minisztérium, HIICSF, osztályvezető
Kiss Béla – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Kolonics Gábor – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Kórórdi Gyula – Nemzeti Közszolgálati Egyetem, KI egyetemi docens
Kovács Zoltán – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Kozlovszky Miklós – Óbudai Egyetem, NJIK
Dr. Kende György – Nemzeti Közszolgálati Egyetem, HHK, egyetemi tanár
Lucas Grégory – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Madobács Katalin – MH GEOSZ
Dr. Meglécz Katalin – MH KJSZ
Mórocza Árpád
Nikodém Edit – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Pellérdi Rezső – Nemzeti Közszolgálati Egyetem, KI, egyetemi docens
Dr. Póserné Valéria – Óbudai Egyetem, NJIK egyetemi docens
Prém Dániel – Óbudai Egyetem, NJIK
Pöcher, Harald – Bundesheer
Dr. Rajnai Zoltán – Óbudai Egyetem, egyetemi tanár
Schubert Tamás – Óbudai Egyetem, NJIK
Schüller Attila– Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Schweickhardt Gotthilf– Nemzeti Közszolgálati Egyetem, KI
Dr. Solymosi József – Nemzeti Közszolgálati Egyetem, HHK, professzor emeritus
Szaniszló Zsolt– Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Szendi Rebeka– Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Tímár Tamás – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Tuba Zoltán – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Venekei József – Nemzeti Közszolgálati Egyetem, HHK, főiskolai docens
Vidnyánszky Zoltán – ELTE TTK, Matematika Doktori Iskola doktorandusz
Wantuch Ferenc – Nemzeti Közlekedési Hatóság Légügyi Hivatal

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Szaniszló Zsolt
sunnyboymi24@gmail.com

AZ OROSZ KATAPULTÜLÉSEK KIFEJLESZTÉSI FOLYAMATÁNAK BIZTONSÁGTECHNIKAI SZEMPONTOK SZERINTI VIZSGÁLATA I.

Absztrakt

A repülőeszközök mentő- és vészelhagyó berendezései az őket szállító repülőszerkezetekkel hasonló ütemben fejlődnek mind a mai napig, de azokhoz mérten általában egy lépéssel mindig lemaradva. Ez mérvadó kockázati szintet jelent. Annak érdekében, hogy ez a kockázat csökkenjen és a minimális, 0 értéket megközelítse, mérnökök, berepülőpilóták és ejtőernyő-kipróbálók összetett munkájára van szükség. A K-36 típusú katapultülés sikeres működését az orosz MiG-29-es vadászrepülőgép néhány rosszul sikerült bemutatórepülése során milliók láthatták. Az ehhez szükséges tudást a mentőberendezések tervezői és kipróbálói évtizedek alatt, sokszor vérrel írva gyűjtötték össze. Az orosz katapultülések kifejlesztésének sorozata a hidegháború kezdetén, a MiG-15 típussal kapcsolódott össze. Az első orosz katapultülés kifejlesztési folyamatának a biztonságtechnika tudományának szempontjából vett bemutatása jól szemlélteti ennek a speciális szakmának a különlegességét. A sikersorozat ugyanis itt kezdődött…

The acceleration of emergency- and ejection systems' evolution has been in paralell with their aircrafts, but it has always been one step behind. It creates a significant level of risk. In order to minimise this risk and converge it to zero, the engineers, test-pilots and test-jumpers' joined effort is necessary. The successfull operation of the type K-36 ejection seat was seen by million during some failed dynamic displays of the world wide known jet fighter MiG-29. The lesson learnt of it has been gathered by the inventors and test-persons during many decades, sometimes unfortunately through the died testers. The innovational period of the Russian ejection seats were in close connection with the type of jet fighter MiG-15, at the beginning of the Cold War. The invention of the first Russian ejection seat is examined from the point of view of the study of security's technics demonstrates the speciality of this profession, very well. And the story of success started from here…

Kulcsszavak: *katapultülés, pilóta mentőernyő, ejtőernyő-kipróbáló ~ ejection seat, emergency parachute, test-jumper*

BEVEZETÉS

Az egyén és a belőle alkotott emberi társadalom csakis nyugodt körülmények, biztos háttér megléte mellett képes érdemes termelő tevékenységet folytatni. A biztonság a latin „securitas” szóból eredően, [1] egyszerűen megfogalmazva bizonytalanság nélküli állapotot jelent. A vele kapcsolatos kutatások végrehajtása összességében a biztonságtudományok terület feladatrendszerébe tartozik, amelynek technikai részével a biztonságtechnika tudománya foglalkozik.

Az egyén sokszor kerülhet olyan bizonytalan helyzetbe élete során, amikor az abból való kikerülés határozott, gyors, néha visszafordíthatatlan döntés meghozatalával jár együtt. Sok esetben az irreverzibilis módon végleges és visszavonhatatlan legmegfelelőbb elhatározást – külső kényszerítő hatások jellege miatt -, néha nagyon rövid időintervallum alatt kell meghoznia. Vannak olyan szakmák illetve hivatások, amelyekben a gyors, határozott, de ugyanakkor helyes döntések meghozatala egyértelműen elvárt alapkövetelmény a munkakört betöltő személlyel szemben, amelyen sokszor a saját élete is múlhat. Ilyen pl. a berepülőpilóták és az ejtőernyő-kipróbálók hivatása, ahol a csúcsot természetesen az új típusú, még fejlesztés alatt álló honvédelmi célú repülőfeladatok ellátására tervezett légijárművek, illetve légieszközök tesztelése, majd azok rendszerbe állítását követően a további biztonságos üzemeltetés körülményeinek kikísérletezése jelenti.

A légijárművek légi üzemeltetésével megbízott szakemberek biztonságát sok esetben a fedélzeten elhelyezett ún. egyéni vészmentő berendezések megléte, azok maximális szintű alkalmazhatósága kell, hogy garantálja. A légijármű vezetőjének tudatában kell lennie annak, hogy járműve visszafordíthatatlan módon történő meghibásodása esetén is maradt még esélye a túlélésre. De ennek értéke csak akkor éri el ideális esetben a maximális 100 %-ot, ha azt az előírt módon és az előírt üzemeltetési paramétereken belül alkalmazza.

Ez természetesen nemcsak a technikai feltételek – lásd mentőberendezés -, hanem egyéb alapfeltételek - pl. az azt alkalmazni kívánó személy kiképzettségét, külső körülmények stb. - meglétét ideális, sok esetben egy bizonyos megengedhető tűréssel rendelkező, az optimális szinten túllépve, a maximális érték felé konvergálva követeli meg.

Azért, hogy röviden bemutassam mindazon munkának bonyolultságát és szépségét, amelyet a fent nevezett repülő-hajózó- és ejtőernyős kollégák a repülés biztonságosabbá tételének céljából nap mint nap végrehajtanak, azt a döntést hoztam, hogy az ún. *„technikai eszköz”* fogalmának – biztonságtechnikai szempontból való - szemléltetését választom egy adott, speciális vészmentő berendezés gyakorlati példája alapján.

A bemutatás során felhasználtam mindazon ismeretanyagot, amelyet a Nemzeti Közszolgálati Egyetem oktatói a biztonságtechnika tudományterületéről átadhattak, valamint amelyet a magyar katonai repülés történetének tanulmányozása során saját kutatásaim során összegyűjtöttem.

A REPÜLŐ EMBER ÚJABB BIZTONSÁGI KIHÍVÁSA: A NAGYSEBESSÉGŰ REPÜLÉS KORSZAKA

A XX. század története szorosan összefonódott a repülés történetével, amelynek során az ember a szárazföld, majd a víz után fokozatosan meghódította a harmadik közeget, a levegőt is. Ez a küzdelem ugyanúgy nem volt áldozatok nélkül való -, mint az emberiség történelme során a természet fölött aratott egyéb győzelmei sem - annak ellenére, hogy az ezt lehetővé tevő repülőtechnika folyamatos fejlődésen ment át.

Az adott repüléstörténelmi korszak vizsgálata (A biztonságtechnika tudományának fejlettségi szintje)

A történelem során az ember folyamatosan érezte a biztonsági problémák meglétét, és a technikai fejlődés állapotát tekintve a biztonság megismerése, a biztonság tudománya, folyamatát tekintve eljutott az ún. *„rendszer biztonság”* korába. [2] Ez nem jelent mást, mint azt, hogy az ember elkezdte tudatosan tervezni a – mindennapi életét átható, szinte valamennyi cselekvéssorozatának - biztonságát, ami együtt járt biztonsági rendszerek kifejlesztésével, azok tudatos alkalmazására való törekvésekkel.

A nagysebességű repülés megjelenésével a már világszerte rendszerbe állított, különböző konstrukciójú pilóta mentőejtőernyő megléte önmagában kevésnek mutatkozott a túlélés szempontjából a menthetetlen helyzetbe került repülőgép vezetője számára. A jelentősen megnőtt repülési sebesség jóval nagyobb légerőket okozott, amelynek leküzdésére az emberi izomerő nem bizonyult kielégítőnek. [3] Így a „habselyem őrangyal” biztonságos alkalmazásának alapfeltételét egyedül csakis a katapultülés beépítése és annak szakszerű használata jelenthette. Erre természetesen mind a világ nyugati, mind a keleti felén megindultak a kísérletek.

A katapultülés létrehozásának igénye (A biztonságtudomány kapcsolata más tudományterületekkel)

Mivel a biztonságtechnika tudománya soha sem önmagában létezik, - azért, hogy komplex egészet alkosson -, más tudományterületeket is segítségül kell, hogy hívjon a rendszer mindnél teljesebb körű megismerésének érdekében. [4] Az egyes tudományterületek kölcsönösen kell, hogy kiegészítsék és segítsék egymást, és erre nagyon jó példa volt az a tervezési gyakorlat, amelyet a volt Szovjetunióban a repülés területén, elsősorban állami (politikai) döntések révén kialakítottak.

Noha magát a repülőgépet az A. I. Mikojan - M. I. Gurjevics páros vezette tervezőiroda hozta létre, a vészmentő berendezés tervezésével megbízott V. M. Beljajev és Sz. N. Ljusin mérnökök [5] pszichológusok és orvosok szakmai javaslatait, tanácsait is kikérték munkájuk során, a minél biztonságosabb működés megteremtése érdekében. Ez magyarázható a feladat újdonságával, ugyanis a folyamat eredményeképpen születhetett meg az első szovjet katapultülés.

A katapultülés tervezett biztonságos alkalmazhatósági feltételei, a pilóta túlélőképességét biztosító kritériumok meghatározása

A tervezőgárda feladata elsődlegesen az volt, hogy megállapítsák a vészmentő rendszer biztonságos működését magába foglaló kritériumok összességét, mind a katapultülésre, mind a pilóta mentőejtőernyőjére vonatkozóan.

A katapultüléssel szemben támasztott, megoldani kívánt kritériumok:

1. A túlterhelés nagyságának az emberi szervezetre megengedett értékhatárokon belül való tartása a működési folyamat teljes időtartamán belül.
2. A légáramlattal történő találkozás és az ülés elfordulásával járó szöggyorsulás hatására bekövetkező végtag-szétcsapódások megakadályozása.
3. Az arc és test védelme a légáramlat közvetlen hatásától.
4. Az ülés pilótával együtt való nem megengedett szöggyorsulást eredményező elfordulásának megakadályozása, a katapultálás pillanatától a pilóta katapultüléstől történő elválásáig tartó folyamata során.
5. A pilóta katapultüléstől történő időbeni elválásának biztosítása.

A pilóta mentőejtőernyővel szemben támasztott, megoldani kívánt kritériumok:

1. Az ejtőernyőkupola és ejtőernyőrendszer - igazodván kis és nagy magasságok különféle valós sebességeihez -, meghatározott torlónyomás határértékeken belül léphet működésbe.
2. Az ejtőernyő magasban történő működésbe lépése pillanatában a kupola belobbanásához és az ereszkedési sebességre történő csillapodásához szükséges sebesség, valamint a földetérési sebesség nagysága, az emberi szervezetre megengedett értékhatárokon belül maradjon.
3. A pilóta zuhanási sebessége az ejtőernyő működésbe lépésének pillanatában nem lehet nagyobb, mint az ejtőernyő típusára megengedett kezdeti belobbanási sebesség értéke.
4. Az ejtőernyő rendszernek biztosítania kell a pilóta stabil zuhanását nagy magasságból, ahol a repülőeszköz vészelhagyása megtörtént, egészen a mentőejtőernyő nyitását lehetővé tevő alacsony magasságig. [6]

A fenti problémák megoldására természetesen már akkor is voltak többé-kevésbé kész megoldások, köszönhetően a Szovjetunió ejtőernyős-ipar területén addig összegyűjtött elméleti tudásnak és a megszerzett gyakorlati tapasztalatoknak. Viszont azt tudni kell, hogy egy-egy jónak tűnő megoldás is felvethet újabb problémákat, amelyeket ismételten orvosolni kell.

A következőkben csak a legfontosabb gondolatokat szedem össze, amelyek egy kiindulási alapot biztosíthattak a tervezők részére is.

Az ejtőernyő

Az ejtőernyő, mint az egyéni mentőberendezés legfontosabb eleme sohasem opciós, hanem kötelező felszerelési tárgya az adott típusú repülőeszköznek, melynek típusát az adott légijármű gyártója írta elő. A Szovjet Légierő repülőcsapatainál a hajózó mentőeszközök között ebben az időben mind a hát-, mind az has-, mind az ülőejtőernyő megtalálható volt, majd a modernebb katapultülések alkalmazásával (pl. SzK-1, KM-1 stb.) a későbbiekben megjelent a katapultülés fejtámlájába beépített mentőejtőernyő is.

A hátejtőernyő kényelmes megoldás, alapvetően ez zavarja a repülőeszköz vezetőjét a repülési feladat végrehajtása során a legkevésbé. Azon kívül vészelhagyást követően is biztonságosabban üzemeltethető, a kupola kihúzódása során kisebb az elakadás lehetősége, mint az ülőejtőernyők esetében. Ez köszönhető „a szovjet rendszerű" repülő-hajózó kiképzés során megszerzett ejtőernyős tapasztalatoknak, ugyanis a kiképzés során kivétel nélkül háti rendszerű kiképző- és gyakorló ejtőernyők kerültek alkalmazásra.

A hasejtőernyő viselése repülés során meglehetősen kényelmetlen, ezért sok esetben a pilóták csak magát az ejtőernyőhevedert viselték repülés közben, amelyre az ejtőernyőt csak vészhelyzet esetében csatolták fel. Ez viszont alapvetően időveszteséggel járt, és az azonnali gépelhagyás végrehajtását tette lehetetlenné.

Az ülőejtőernyő elhelyezésére egyértelműen adódik a légijárművezető üléscsészéjének belseje, amely viszont azzal a hátránnyal jár együtt, hogy az egyéb mentőberendezések (egyéni túlélőkészlet) elhelyezésére kevesebb hely adódik. Mivel ennek a problémának a megoldása járt a legkisebb nehézséggel, ilyen kialakítású lett a szovjet repülőtechnikákon leggyakrabban alkalmazott egyéni mentőejtőernyő mind a helikopterek, mind a hangsebesség alatti repülőgépek repülő-hajózó személyzetei részére.

A vészelhagyás végrehajtása

Lehet bármilyen jó minőségű az ejtőernyő, ha a menekülni akaró pilóta nem képes kijutni a légijárműve belsejéből, hogy képes legyen azt biztonságosan alkalmazni. A nagysebességű repülőeszköz elhagyó pilóták sok esetben annak valamely elemével ütközve szenvedtek az élettel összeegyeztethetetlen sérülést, még olyan esetben is, amikor az ejtőernyő tökéletesen működött, illetve amikor a már kis magasságban végrehajtott gépelhagyás nem tette lehetővé az ernyő biztonságos belobbanását. Mindkét esetre volt példa.

A fenti példák egyértelműen bizonyítják, hogy a hajózószemélyzet alapos kiképzése nélkülözhetetlen az ejtőernyős vészelhagyáshoz szükséges döntés adott időben történő meghozatalához, valamint a vészelhagyás előírt módon történő végrehajtásához.

Az ejtőernyő nyitása

Az ejtőernyő biztonságos belobbanását bizonyos késleltetési idő betartásával kell biztosítani. Ez szükséges ahhoz, hogy elkerülhetővé váljon a belobbanó ejtőernyő, s vele együtt a pilóta felakadása az általa elhagyott repülőszerkezetre. Továbbá fontos dolog a pilóta mentőejtőernyő automatikus nyitására is megoldást találni, ugyanis fennállhat annak az esélye, hogy a pilóta a katapultálást során cselekvésképtelen állapotba kerülve képtelen lesz ejtőernyőjének manuális nyitására. Erre vagy aneroid szelence vezérelte rugós mechanizmust, vagy pirotechnikai elven működő ejtőernyő-nyitó (fél)automata berendezést kell felhasználni, a minél teljesebb biztonság megteremtése érdekében. [7]

A nagy magasságú gépelhagyás veszélyei

A repülőeszközt nagy magasságban elhagyó pilótára a Föld légkörében, kabinon kívül is sok veszély - nagy kezdeti légsebesség és az abból adódó torlónyomás, alacsony hőmérséklet, alacsony barometrikus nyomás, oxigénhiányos környezet stb. – leselkedik. Ezek olyan speciális, mobil védőfelszerelések (túlnyomásos ruha, hajózósisak, mobil oxigénberendezés, stb.) meglétét követelik meg, amelyet a katapultálás során is képes magával vinni a pilóta, hogy azok az életben maradás feltételeit – az ejtőernyőn függve, egészen a földet érésig - biztosítsák számára.

Látható, hogy nem volt egyszerű a feladat. Ráadásul egy adott eszköz csak akkor képes feladatát teljesíteni, ha az üzemeltető is megfelelő felkészítést kapott annak szakszerű alkalmazásával kapcsolatosan. Vagyis a hajózószemélyzet alapos kiképzése szintén nélkülözhetetlen az ejtőernyős vészelhagyás végrehajtásához, az ahhoz szükséges döntés adott időben, előírt módon történő meghozatalához.

Mivel egy repülőeszköz egyéni vészmentő berendezésének biztonságos működését bemutató tanulmány megírását tűztem ki célul, nem felejtkezhetünk el a biztonságtechnika tudományterület alaptörvényeire történő kitekintésről sem. A vizsgált esetben a katapultülés és az ejtőernyőrendszer tervezése során is hasonló rendszerszemlélet alapján haladhattak előre a tervezőgárda tagjai. Ezt a feltételezést a repüléstechnikai tények közvetett módon igazolják.

Éppen ezért a biztonságtechnika tudományának alaptörvényeit a vészmentő berendezés tervezésével egybekötve mutatom be.

A katapultülés tervezése
(A biztonságtechnika tudományának alaptörvényei)

Kapcsolati törvény

Ez a biztonságtechnika tudomány vizsgálati színterére vonatkozva a katapultülés működését az ún. *„ember-gép-környezet”* hármas rendszerben [8] vizsgálja. Azt kutatja, hogy az alkotórendszerekben bekövetkező változások közül melyik hordoz veszélyt magában a katapultülés nem a gyártó által biztonságos alkalmazás garantáló alapfeltételek egyikének vagy több együttes kombinációjának jelentkezése esetén.

Fontos megemlíteni, hogy a teljes rendszer biztonságos működése szempontjából minden rendszerelem pontos működése egyaránt fontos, de az emberi tényező a vizsgált esetben kiemelt szerepet játszik! Ugyanis az adott vészmentő berendezés működése csakis a benne ülő személy pontos, a katapultálási folyamatra történő előkészületi mozdulatsora révén lehet csak majdnem teljesen biztonságos, és csakis ebben az esetben garantálhatja az adott személy sérülésmentes megmenekülését.

Eloszlási törvény

Ez a törvény nem mást, mint az adott technikai eszköz – jelen esetben a vizsgált katapultülés – alkalmazása során bekövetkező balesetek, sérülések okainak főbb eloszlását vizsgálja. [9]

Sajnálatos tény, hogy a katapultülés sem működhet mindig a tervezett paramétereknek megfelelően, így az - annak nem előírt, a gyártó által garantált módtól történő működése, esetleg működésképtelensége esetén -, a benne helyet foglaló, a repülőgépet elhagyni kényszerülő pilóta súlyos sérülését, esetleg halálát is okozhatja.

Az ezeket előidéző okok között mind a megmagyarázhatatlan, mind a technikai jellegű hibák is előfordulnak ugyan, de nem olyan mértékben, mint azok, amelyek az ember által a repülési fegyelem megsértéséből, az adott eszköz üzemeltetési előírásainak be nem tartásából következnek be. Nem szabad elfelejtkezni arról, hogy az adott vészmentő berendezés is rendelkezik alkalmazási korlátokkal, melyek túllépése nem a biztonság irányába történő elmozdulást jelenti az adott eszköz szükségessé vált használata során.

Az eloszlási törvény alapteóriáját megfogalmazó H. W. Heinrich 2 %, 10 %, 88 % értékekben határozta meg ebben az emelkedési sorrendben a megmagyarázhatatlan-, a technikai jellegű-, valamint az ember által okozott hibák arányait. [10] Hogy ezek az értékek mennyire igazak a Magyar Néphadseregben vészelhagyásra ténylegesen felhasznált, adott típusú katapultülések vonatkozásában, részleteiben a tanulmány II. részében kerül bemutatásra.

A biztonság tervezésére vonatkozó törvények

„A teljes biztonságot megvalósítani nem lehetséges!”

Bármennyire körültekintően történik is meg egy folyamat végrehajtásának menete, a teljes biztonságot soha sem lehet tökéletes módon garantálni. Tapasztalatok szerint soha sem lehet az összes zavaró, befolyásoló tényezőt kiküszöbölni, [11] egy adott bizonytalansági sáv a végrehajtás kimenetelével kapcsolatosan mindig fennmarad. A tervezők csakis azt a célt tűzhetik ki maguk elé, hogy a meglevő technikai lehetőségek, valamint a gyakorlati életben eddig összegyűjtött tapasztalatok összegzésével, azok kiértékelésével megpróbálják a folyamat végkimenetelével kapcsolatos bizonytalansági faktort a lehető legalacsonyabb szinten tartani.

A MiG-15, MiG-15bisz és MiG-15UTI repülőgépek katapultülésének tervezési folyamatát vizsgálva, már meglévő, elsősorban hazai – a Szovjetunión belüli - fejlesztési tapasztalatok gyakorlatilag nem léteztek. Továbbá a külföldi licensz alapján történő mintadarab-beszerzés sem tűnt kivitelezhetőnek, a történelmi kor ismeretében ennek oka nem szorul magyarázatra. Így egyedüli megoldásként maradt a háborús német zsákmányanyagból származó katapultülések vizsgálatából nyert, valamint a nyugati repülőtechnikák fejlesztésének területén végzett ipari kémkedés során „beszerzett” tapasztalatok tudatos, alkotó módon történő felhasználásának lehetősége.

Erre nagyon jó példa az ún. szalagejtőernyő[1] alkalmazása pilóta mentőejtőernyőként, elsősorban a háborús német tapasztalatok alapján. Később a Szovjetunióban kifejlesztették az Sz-3 típusú pilóta mentőejtőernyőt, így ezek alkalmazásától a továbbiakban eltértek. [13]

1 A nagy belobbanási sebesség miatt olyan speciálisan kialakított ejtőernyő, amelynek ún. „konvencionális” (hagyományos kialakítású) kupolaformája megmaradt ugyan, de az alapvetően nem összefüggő kupolaanyagból, hanem széles szalagokból van összevarrva. Ez a kialakítás egy hagyományos kupolaanyag légáteresztő képességét „a konstrukciós kialakítás segítségével” megnöveli, amelynek hatására a kupola belobbanásakor fellépő dinamikus terhelés mind az ejtőernyő rendszerre (rendszerbiztonsági szempontból), mind az ejtőernyős ugróra (élettani szempontból) vizsgálva elviselhető nagyságú marad. Ez szalagejtőernyő esetében visszavezethető a szalagok egymáson történő elcsúszására, [12] amely kis mértékben fékező hatással van a kupola belobbanására, így a dinamikus terhelés nagyságát a megengedett értéken belül tartja.

„A biztonsági tevékenységek eltérő hatékonyságúak!”
Az előzőekben megfogalmazott célkitűzés elérésére általában egy bizonyos véges számú lehetőség alkalmazása merül fel, amelyek közül a hatékonyság, valamint a bekerülési költség dönt a befutó megoldás mellett. A technikailag biztosítható, de ugyanakkor gazdaságilag még teljesíthető biztonságnövelési szint meghatározása nagyon nehéz kérdés. [14]

Az adott vészmentő berendezés esetén is fontos szempont volt, hogy olyan repülőeszközbe tervezik beépíteni, amelyet nagy tömegben, a kor technikai szintjén történő, fejlett gyártástechnológia segítségével kívánnak előállítani. És itt jön el az ideje az ún. *„társadalmi határköltség”*-fogalom értelmezésének is.

„A biztonsági szint megvalósításának van egy ún. társadalmi határköltség-kritériuma!”
Kijelenthető, hogy egyetlen múltbeli, jelenkori és nyílván jövőbeli társadalom sem volt, van és lesz elég gazdag ahhoz, hogy egy adott technikai eszköz, berendezés működésének biztosítása érdekében minden pénz rááldozzon. Az anyagi erőforrások korlátozott rendelkezésre állása miatt sokszor magának a társadalomnak, vagy az ő nevében egy adott csoportnak vagy személynek kell döntést hoznia arról, hogy hol van a biztonságra történő ráfordítás határa. [15] Ez a döntés nem könnyű, sok későbbi baleset kivizsgálása során az azt előidéző okok közé is besorolásra kerülhet.

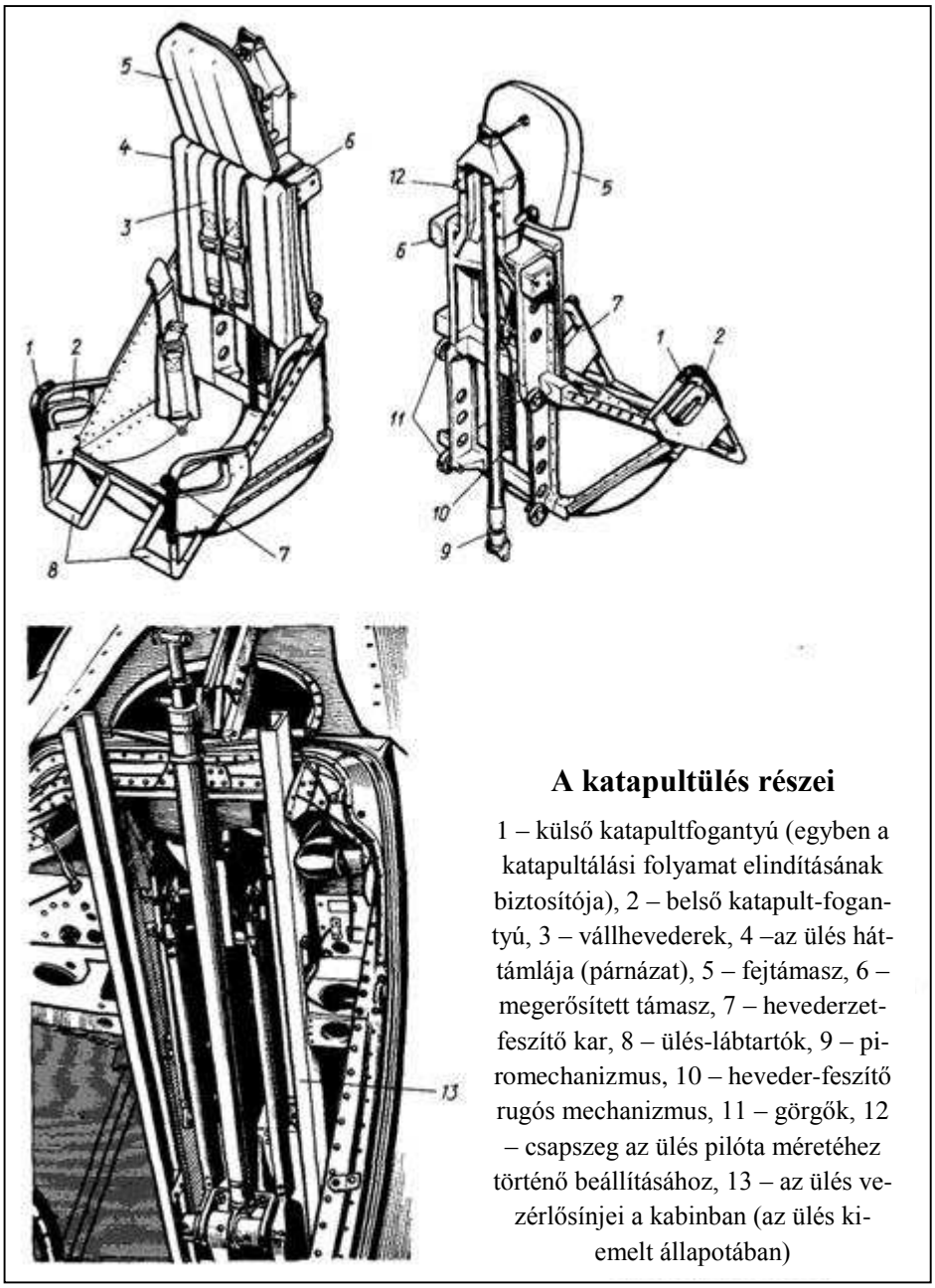
A vizsgált példa meglehetősen kétarcú jelenséget mutat, ugyanis a volt Szovjetunióban gyakran hangoztatott jelmondat szerint: *„A legfontosabb érték az ember!”*, a valóság viszont ennek sokszor homlok egyenesen az ellenkezőjét mutatta. A Szovjet Légierő mind katonailag, mind - a társadalomban betöltött szerepe miatt – politikailag is kiemelt fontossággal bírt, ezért a tervező, fejlesztő munka legteljesebb körű anyagi támogatása nem szenvedhetett csorbát, ha a pilóta, mint ember lény biztonságának elsődlegességét akarták szem előtt tartani.

„Oksorozati törvény”
Ennek a törvénynek alapvetően a különféle balesetek, katasztrófák elemzése során történő felhasználását kell kiemelni, miszerint annak bekövetkezéséért általánosságban mindig több, egymás mellett, illetve egymásra épülten ható esemény játszott szerepet. [16]

Mivel a teljes biztonságtechnikai rendszer összetétele meglehetősen összetett, így több esetben is kell, hogy visszacsatolást kapjon a felhasználó az általa üzemeltetett rendszer - jelen esetben az adott vészmentő berendezés - megbízható működéséről. Ebben az esetben már nem elég a tervezőasztal, szükségesek a „kézzelfogható” gyakorlati teszteredmények is.

Meglehetősen kevés adatot lehetett találni a katapultülés kifejlesztése során végrehajtott gyakorlati tesztek eredményével kapcsolatosan, így ezt a gyakorlati repülésben az adott típuson már nagy tömegben alkalmazott katapultülésekkel végrehajtott katapultálások eredményességével fogom jellemezni. A biztonságtudomány talán „leglátványosabb” elemét képező alapelv szemléltetésére a Magyar Néphadsereg MiG-15, MiG-15bisz és MiG-15UTI repülőgépeiből „éles” körülmények között végrehajtásra került katapultálások rövid esetleírásait fogom felhasználni, a tanulmány II. részében.

A katapultülés (1. ábra) és a pilóta mentőejtőernyő teljes megalkotási folyamata közel két évig tartott, végül 1948-ban született döntés az ún. Állami Bizottság részéről a sorozatgyártás elindításáról. [17] Mielőtt azonban ez megtörtént, a prototípust természetesen a gyakorlatban is ki kellett próbálni, hogy bebizonyosodjon működőképessége, valamint megállapíthatóak legyenek elsődleges üzemeltetési korlátai. Ez a feladat már a légi (berepülési/beugrási) vizsgálatok csoportjába tartozik.



A katapultülés részei

1 – külső katapultfogantyú (egyben a katapultálási folyamat elindításának biztosítója), 2 – belső katapult-fogantyú, 3 – vállhevederek, 4 –az ülés háttámlája (párnázat), 5 – fejtámasz, 6 – megerősített támasz, 7 – hevederzet-feszítő kar, 8 – ülés-lábtartók, 9 – piromechanizmus, 10 – heveder-feszítő rugós mechanizmus, 11 – görgők, 12 – csapszeg az ülés pilóta méretéhez történő beállításához, 13 – az ülés vezérlősínjei a kabinban (az ülés kiemelt állapotában)

1. ábra Az elkészült, és 1948-ban már sorozatgyártásra bocsátott katapultülés szerkezeti kialakítása

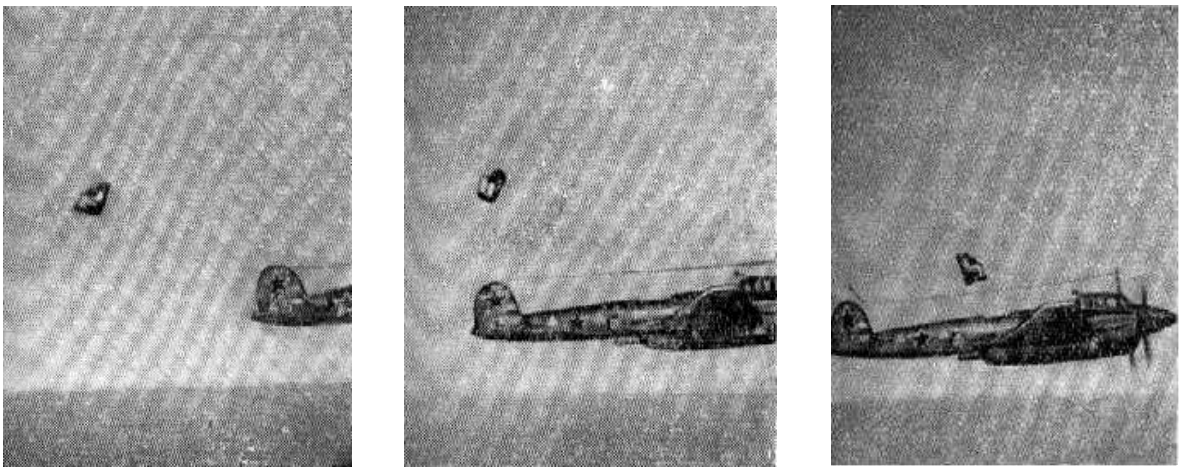
Forrás: А. Г. Агроник, Л. И. Эгенбург: Развитие авиационных средств спасения. Издательство Машиностроение, Москва, 1990.–256 с: ил ISBN 5-217-01052-5. 103. o.

A katapultülés légi vizsgálata (beugrása)

A biztonságtechnika tudományának elméleti módszereként a biztonsági filozófia a biztonsági problémák tudományos meghatározását elősegítve, már előre jelzi annak jellegét, [18] az azt fenyegető veszélyekre történő előzetes felkészüléssel. A legsúlyosabb problémát a katapultülésnek a repülőgép függőleges vezérsíkjával való összeütközésének veszélye jelentette, ezért a katapultpróbákra kezdetben a Pe-2 típusú bombázórepülő átalakított példányait használták fel, amely osztott függőleges vezérsíkkal rendelkezett. [19]

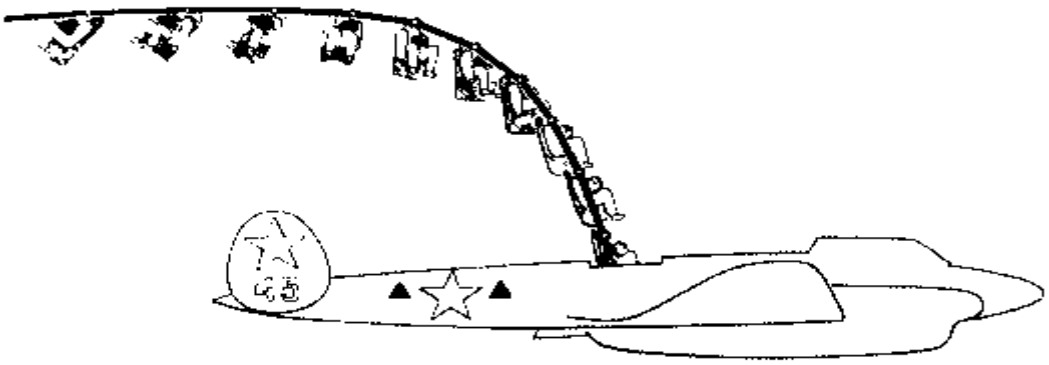
Az igazi „emberes próbát” azonban még egy lépésnek meg kellett előznie, szintén a biztonsági kockázat csökkentése érdekében. Ennek megfelelően először a katapultülés légi

kipróbálásának végrehajtására jelentkező hat ejtőernyő-kipróbáló egyikének méretei alapján elkészített bábú játszotta az ülésben ülve a főszerepet. A katapultülésben ülő „főszereplő” repülőből történő kivetődését, majd a levegőben az üléstől történő elválását filmszalagra rögzítették. Ezt mind a kísérleti gép rádiós-lövészének fülkéjéből – ilyen lesz majd az 5. és 6. ábra -, mind egy másik, a Pe-2-vel kötelékben repülő repülőeszközből (2. ábra) elkészítették.



2. ábra Kísérleti katapultálás végrehajtása Pe-2 típusú repülőgépből
Forrás: a szerző gyűjteményéből (Kastély Sándor jóvoltából)

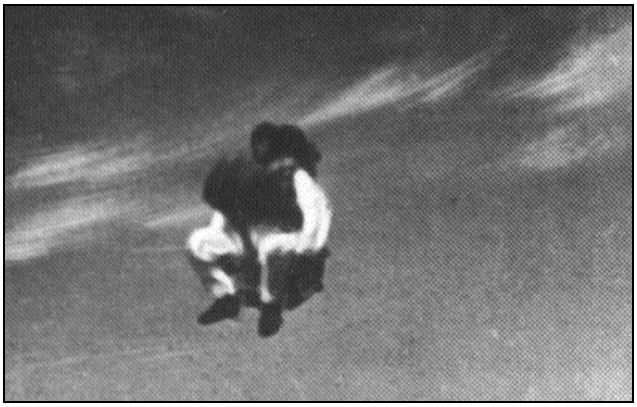
A filmfelvétel alapján készült ún. kinogramm[2] segítségével, majd az az alapján készült vázlatrajz felhasználásával nagyszerűen lehetett szemléltetni és elemezni a kezdetben katapultülés-ejtőernyős ugró komplexum (3. ábra), majd azok szétválását követő további önálló mozgáspályájukat a levegőben.



3. ábra A katapultülés-ejtőernyős ugró komplexum mozgáspályája, a filmfelvétel alapján készült ún. kinogramm alapján készült vázlat segítségével szemléltetve
Forrás: a szerző gyűjteményéből (Kastély Sándor jóvoltából)

1947. június 24-én G. A. Kondrasov (4. ábra) hajtotta végre biztonságosan a katapultülés első emberes kipróbálását (5. és 6. ábra), [20] amelyet hamarosan több is követett. Mint a biztonságtechnikai tudomány célkitűzése, ezek már a biztonság minél magasabb szintű biztosításának érdekében kerültek végrehajtásra.

2 A filmszalag kockánkénti kiválogatása alapján készült el, melynek eredményeképpen a legfontosabb pillanatokat ábrázoló képek kerültek egymás mellé, néhány képkockából álló sorozatot alkotva.



4. ábra. A katapultülés első gyakorlati alkalmazója, G. A. Kondrasov ejtőernyő kipróbáló, aki a végrehajtás után megkapta a Szovjetunió Hőse címet.
5. és 6. ábra. A két kisméretű, fekete-fehér képen a katapultálás első pillanatai láthatóak, a Pe-2 rádiós-lövész fülkéjéből készített filmen
Forrás: a szerző gyűjteményéből (Kastély Sándor jóvoltából)

Az emberes tesztsorozat biztonságos befejezését követően a katapultülés már magát a biztonságtechnika tudomány technikai alapfeltételét, pontosabban már kellő számú vizsgálaton átesett technikai alapfeltételét – amely egyben a technikai eszköz is - szimbolizálta.

A katapultülés gyakorlati kipróbálása során megvalósult biztonságos alkalmazhatósági feltételeinek, valamint a rendszerbe állítását megelőző üzemeltetési biztonság kritériumainak összegzése

Miután egy beszerzésre kerülő új haditechnikai eszköz nemcsak az általános, hanem a speciális katonai szempontokból vizsgálat alá kerülő kritériumoknak is megfelel, az átvevő bizottság pozitív döntést hoz rendszeresítésével kapcsolatosan. Ez egy ún. rendszerbe állítási terv elkészítését is előírja, melynek során speciálisan kiképzett emberek gyűjtik össze az új berendezés biztonságos üzemeltetésével kapcsolatos javaslataikat.

A vizsgált esetben, a katapultülés rendszerbe állítása során olyan – elsősorban katonai – ejtőernyő-kipróbáló szakembergárdát állítottak össze erre a célra – természetesen ismét állami irányítással -, amely kellő alapot biztosított az új vészmentő berendezés üzemeltetési szempontjainak minden oldalról történő vizsgálata szempontjából.

Rendszertechnikai szempontból vizsgálva a feladat mindazon kritériumok megállapítása és olyan üzemeltetési előírás-gyűjtemény megalkotása, amely biztosítja a berendezés üzemeltetési folyamatának biztonságos végbemenetelét. [21]

Ennek megvalósítására is sokféle eltérő szempont szerint vizsgálható, de az adott esetben érdemes a biztonságtechnika tudomány oldaláról végezni az elemzést. Éppen ezért nem felejtkezhetünk meg arról, hogy: *„Az üzemeltetési folyamat elsősorban szervezési probléma, s mint ilyen, nagymértékben meghatározott az embertől.” [22]*

A katapultülés, mint technikai eszköz üzemeltetésének általános folyamatát a felhasználó és a biztonsági elemezhetőség szempontjából három részre érdemes bontani: előkészítésre, üzemelésre és értékelésre.

Az üzemeltetésre történő előkészítés biztonsági kérdései

Ezen felkészítési folyamat feladata az adott eszköz üzemeltetéséhez szükséges tárgyi, jogi és személyi feltételek megteremtése. Mindez biztonsági szempontból az adminisztratív, a technikai és a személyi felkészítéssel kapcsolatos kérdések megválaszolását jelenti.

Az adminisztratív előkészítés feladatai

Mivel a vizsgált példában a katapultülés már készen állt, így az üzemeltetésre történő előkészítés adminisztratív oldala alapvetően az üzemeltetői előírások rendszerezését, sokszorosítását, azok üzemeltetői szintű elterjesztését jelentette.

Vagyis: *„Ha már megvan az eszköz, tegyünk meg mindent annak érdekében, hogy azt az üzemeltetői szint szakértő módon használhassa!”* Ez vonatkozik mind a repülő-hajózó (üzemeltetői), mind a repülő-műszaki (üzembentartói) állomány dokumentációjára, a berendezés vészelhagyás során szükséges alkalmazására történő, illetve időszakos vizsgálatra történő előkészítésével kapcsolatos munkák dokumentációjának elő-, illetve elkészítésére is.

A technikai előkészítés feladatai

A biztonságtechnika szempontjából vizsgálva az adott eszközökről mindig úgy kell az őket használatra előkészítő, üzembentartó szakember(ek)nek gondoskodnia, hogy az üzemeltetői részről ezen a területen, az adott berendezés rendeltetésszerű használatával kapcsolatosan semmilyen kétség se merülhessen fel. Ebbe a csoportba tartozik bele az adott berendezés beszabályozása, speciális felszereléssel történő ellátása, stb.

Nagyon fontos, hogy az adott berendezés technikai előkészítése összhangba kerüljön a teljes technikai rendszer többi elemének előkészítő munkálataival is. Ez egyrészt leegyszerűsíti a karbantartási és előkészítési munkálatok szervezését, ezáltal anyagi- és munkaóra megtakarítás, valamint a munkát végrehajtó állomány optimálisabb feladatmegoldása is elérhető.

Nem hanyagolható el ebből a szempontból az sem, hogy a berendezés tervezése során a konstruktőr milyen szabvány szerint dolgozott, a teljes rendszer egyes elemeinek élettartama milyen viszonyban van a többiével, illetve a teljes rendszer működésképtelenné válhat-e egyetlen alkotóeleme meghibásodásakor, stb.

A személyi felkészítés feladatai

Eddig több esetben is említésre került, hogy az adott berendezés biztonságos alkalmazásának egyik alapfeltételét, az ún. *„ember-gép-környezet”* hármas rendszer legfontosabb, de egyben leggyengébb láncszemeként az őt kezelő ember jelenti, aki az esetek döntő többségében felelős annak nem megfelelő módon történő üzemeltetéséért.

Repülő-hajózó tisztként szemlélve a kérdést, alapvetően a repülő-hajózó állomány katapultálás végrehajtására történő felkészülésének, felkészítésének folyamatát vizsgálom.

A kezelői kiválasztás jelentősége

A legfontosabb kiválasztási kritérium, hogy a kezelő legyen képes végrehajtani minden szükséges részfunkciót (érzékelői, információ feldolgozói, döntéshozói stb.) az adott

berendezés kezelésével kapcsolatosan. Ennek feladata nagy megterhelést jelent a kezelőre, s egy adott szinten túl megnőhet a hibázás, a rossz döntés(ek) meghozásának lehetősége, amely akár tragédiához is vezethet.

A tények a későbbiekben sajnálatos módon bizonyították, hogy mind a Szovjet Légierő, mind a Magyar Néphadsereg sok fiatal pilótája esetében – a tanulmány II. részében erre részletesen kitérek -, pontosan így történt. A rossz, nem teljesen kiforrott kiválasztási rendszer, valamint a nem megfelelő előképzettséggel rendelkező repülő-hajózó állomány repülési feladatának pontos végrehajtása, illetve sok esetben maga az életben maradás elengedhetetlen módon megkövetelte azok mindnél alaposabb, feladatra történő felkészítését.

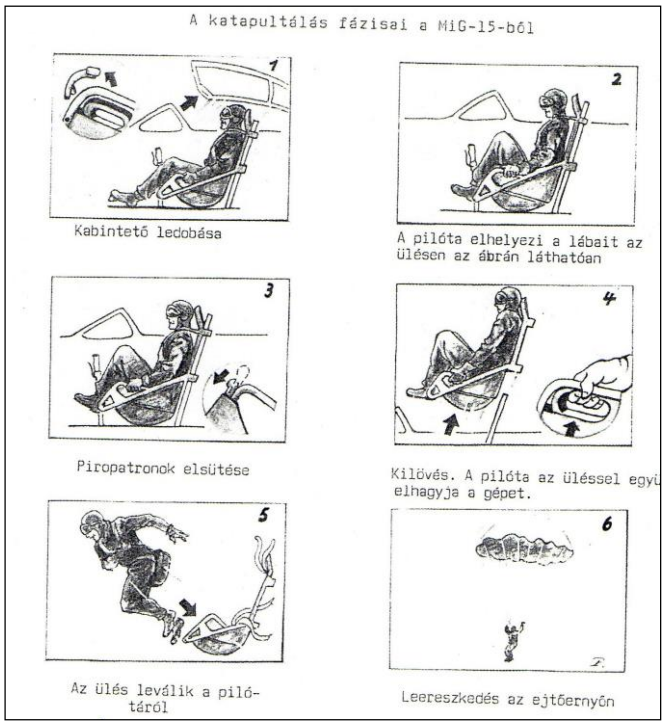
Ennek megfelelően a legtöbb fiatal éppen a kiképzése kezdetén, az első önálló repülési feladatok végrehajtása során halt repülőhalált, annak ellenére, hogy az akkori repült óraszám nagysága, valamint a speciális kezelői felkészítés révén szerzett tapasztalatok mind növelték az életben maradás esélyét.

A kezelői felkészítés jelentősége

Ahhoz, hogy valaki tudatára ébredjen annak, hogy veszélyben van, megfelelő tapasztalatokkal kell rendelkeznie az adott feladat teljes végrehajtásával, annak veszélyes momentumaival kapcsolatosan.

Az ún. „repülési rezsim” betartása: az adott típusú repülőeszközzel, adott feladat végrehajtásra történő előzetes elméleti és gyakorlati felkészülés (kabintrenázs), az oktató által végzett repülés előtti ellenőrzés, a repülés során a folyamatos műszerfigyelés, a számított repülési és üzemeltetési paraméterektől történő eltérés(ek) repülés közbeni vizsgálata, értékelése mind egy-egy kis részlete az adott repülési feladat biztonságos végrehajtásának.

Ebbe beletartozik a katapultberendezés készségszintű alkalmazásának begyakorlása is. Ugyanis a vészelhagyást meg kell, hogy előzze egy olyan tevékenységi sorrend végrehajtása a repülőgépvezető részéről (7. ábra), amely az adott berendezés működését elősegíti, valamint a pilóta egészségét maximálisan garantálja a vészelhagyás végrehajtása során.



7. ábra. A repülőgépvezetők részére készült vázlat a katapultálás végrehajtásának folyamatáról.
Forrás: Zsák Ferenc: Katapultáló magyarok. Aeromagazin, 2009. február, 53. o.

Mindez azért kell, hogy a pilóta ismerje fel azt a pontot, amikor az ún. „bonyolult helyzet”-be kerülés esetén, amikor már nincs lehetősége a repülőeszköz megmentésére, hozza meg a döntést annak vészelhagyására, a saját életének megmentése érdekében. Ennek végső határát alapvetően a vészmentő berendezés, a katapultülés és a pilóta mentőejtőernyő üzemeltetési paraméterei határozzák meg. A vészelhagyásra vonatkozó döntést mindig az ún. „végső pillanat”-ig kell meghozni. Utána már nem érdemes...

Azért, hogy a repülő-hajózó állomány idejében képes legyen meghozni a katapultálásra vonatkozó elhatározását, az eredeti szovjet üzemeltetési leírásban minimálisan 250÷300 méteres földfeletti magasság, valamint maximálisan a 700 km/h [23] műszer szerinti repülési sebesség értékét határozták meg, a katapultálás biztonságos végrehajthatóságát szemléltető diagram alapján. Ezt mindenkinek tudnia kellett elméletben. De mi a helyzet a gyakorlati ismeretekkel?

A MiG-15bisz és UTI típusú repülőgépek esetében a Szovjet Légierő repülő-hajózó állománya az NKTL-3 típusú berendezést (8. ábra) [24] használta, amelyen be kellett gyakorolniuk a vészelhagyást megelőző mozdulatsort, valamint kipróbálhatták a katapultálás érzését is, gyengített piropatronok segítségével (9. ábra) [25].

8. ábra. Az NKTL-3 típusú gyakorló katapult-berendezés.
Forrás: В. Г. Романюк: Заметки парашютиста-испитателя. Военное Издательство Министерства Обороны СССР, Москва, 1973. 103160. 250. o.

9. ábra. G. Ty. Beregovoj repülő ezredes, a Szovjetunió Hőse, kozmonauta-kiképzése során a gyakorló katapult-berendezés ülésében[3].
Forrás: G. Beregovoj: Egy űrhajós feljegyzései. Kozmosz Könyvek, Budapest. 1973.

3 A katapultülés, amelyben a későbbi kozmonauta (és egyben első űrhajós tábornok) helyet foglal, többek között a MiG-17, MiG-19, Jak-25 típusú sugárhajtású repülőgépek mentőberendezéseként kapott fontos szerepet. [26]

Ez azért volt fontos, hogy a pilóta ne féljen a katapultálás ismeretlen érzésétől, és a gyakorlatban – földi körülmények között – legyen lehetősége kipróbálni saját szervezetén annak hatásait. Ennek hiányában ugyanis fennállhat a veszélye annak, hogy sokkal jobban fél a katapultálástól és az ejtőernyő nyílását megelőző szabadesés fázisától, mint attól, hogy a repülőgépével együtt – ismeretlen kimenettel – érjen földet.

Személyes tapasztalataim csak megerősítik az ún. „szovjet" típusú repülő-hajózó kiképzési tematikából átvett gyakorlati ejtőernyős kiképzés létjogosultságát. Mivel adott helyzetben egyedül csak az itt megszerzett gyakorlati tapasztalatok biztosíthatják magát az életben maradást, így véleményem szerint ez a jövőben is fontos szerepet kell, hogy kapjon katonai pilótáink újabb generációinak felkészítésében.

Az üzemelés biztonsági kérdései

A katapultülés biztonságos üzemelési folyamata alapvetően az ejtőernyő-kipróbálók által, az adott katapultülés ún. rendszerbeállítási tervében foglaltaknak megfelelően végrehajtott tesztek eredményein alapul és tulajdonképpen magát a konkrét feladatvégrehajtást jelenti. Esetünkben ez a folyamat akkor kezdődik, amikor a repülőeszköz vészelhagyására való elhatározást a pilóta meghozza, felveszi a katapultáláshoz szükséges testhelyzetet és megindítja a katapultálás folyamatát. A vészelhagyás többi része teljesen automatikusan, már a pilóta akaratától függetlenül történik. Ekkor sorrendben:

1. Ledobódik a kabintető.
2. A piropatronok segítségével a teleszkópos rúd kiveti az ülést a repülőgép kabinjából.
3. Az AD-2-es típusú ejtőernyő-nyitó félautomata[4] - az előre beállított, az ülés megindulásának pillanatától számított - 3 s-os késleltetési idő elteltével kioldja az ülésrögzítő hevedereket az üléscsészében elhelyezkedő pilóta körül, aki így eltávolodhat az üléstől a levegőben.
4. Egy másik ejtőernyő-nyitó félautomata gondoskodik az ejtőernyőtok nyitásáról, amennyiben az az ejtőernyő hevederzetén, egy zsebben belehelyezett kézi kioldófogantyú meghúzásával valamilyen ok miatt, a pilóta által manuálisan nem történt meg. A késleltetési idő ebben az esetben is 3 s, az üléshevederek feloldásától számítva.
5. A katapultált hajózó a biztonságosan belobbant pilóta mentőejtőernyő alatt lengedezve – lehetőleg sérülésektől mentesen – földet ér.

Láthatóan a vizsgálatok ekkor ismét az ún. *„ember-gép-környezet"* hármas egységre kell, hogy korlátozódjanak, mivel az adott feladatra tervezett és felkészített berendezés – jelen esetben a vizsgált típusú katapultülés – ebben a rendszerben kerül működtetésre. A biztonságos működést környezeti körülmények befolyásolják, amelyek vizsgálata alapvetően két területre korlátozódik. Most ezeket vizsgáljuk meg!

Megbízhatóság

Ez tulajdonképpen nem jelent mást, mint az adott rendszer működési biztonságának statisztikai adatokkal történő ábrázolását. Önmagában ez a számítási rendszer az adott berendezés egyetlen elemének meghibásodási valószínűségén alapuló kísérleti adattal jellemezhető, amelyet előre meghatározott körülmények között végrehajtott nagyszámú kísérlet végrehajtása eredményezett. [27]

A berendezés egyetlen elemének meghibásodásából kiindulva határozható meg – az adott berendezés bonyolultságából, szerkezeti elemeinek kapcsolatából, azok működési sorrendjének ismeretéből stb. – az ún. *„eredő megbízhatóság"* fogalma. Ez a szám – mely

4 Az AD rövidítés az orosz „Автомат Доронина" kifejezés rövidítése, amelynek jelentése Doronyin automatája. Az adott ejtőernyő-nyitó félautomata típus a tervezőjük, az ejtőernyős-mérnök Doronyin-fivérek után kapta a nevét. A későbbiekben ezt is korszerűsítették és AD-3-as típusra cserélték.

elsősorban szintén statisztikai módszerrel kerül meghatározásra [28] -, már közel egzakt módon jellemzi az adott berendezés üzemeltetési biztonságát.

Noha általában egy adott berendezés esetében két meghibásodás közötti hibaszámot, illetve adott időintervallum alatti meghibásodások számát érdemes alapul venni, ezt a módszert esetünkben kevéssé lehet alkalmazni. Magát a katapultülést egyszeri alkalmazásra tervezik. Továbbá, a repülés történelme során olyan eset sem igazán fordult még elő, hogy egy szándékosan elindított katapultálási folyamat során a meghibásodott ülés – a berendezés technikai hibája miatt - a repülőgépben maradjon. Sőt, majd miután a pilóta sikeres kényszerleszállást hajtott végre, és ezt követően kivizsgálták a műszaki meghibásodás okát, engedték tovább üzemeltetni ugyanazt az ülést, esetleg már egy másik repülőgépbe beépítve.

Esetünkben a berendezés működésének vizsgálatára a tisztán statisztikus értelmezés nem alkalmazható. A katapultülésnek a katapultálási folyamat során egyszerűen nem szabad meghibásodnia! A rendszer tökéletes működését garantáló időintervallum - katapultülés esetére – történő meghatározása az azt működésbe hozó piropatronok szavatossági ideje, valamint a pilóta mentőejtőernyő áthajtogatási ciklusideje alapján történik. Ezeket a repülő alakulat repülő-műszaki szolgálatának katapult berendezés időszakos- és javító műhely, valamint az ejtőernyős szolgálat szakemberei tartották karban, alapvetően a jól bevált időszakos üzemeltetési rendszer előírásainak megfelelően.

Balesetbiztonság

Ez tulajdonképpen nem jelent mást, mint az adott rendszer üzemeltetése, valamint üzemeltetésre kész állapotban tartása során bekövetkező, emberi életet veszélyeztető, vagy súlyos sérülést okozó folyamatok – szintén – statisztikai módszerekkel történő vizsgálata, amelyek szabályozatlan fizikai törvényszerűségek hatására következnek be.

A bekövetkezésük alapvetően adminisztratív úton történik, [29] a vizsgált berendezés típusvizsgálata alapján megalkotott technikai, humán és szervezési intézkedések betartása és betartatása segítségével. Ez alapvetően bonyolítja az adott rendszer üzemeltetését és üzemben tartását, de mivel esetünkben vészelhagyó berendezés biztonságos működésének garanciája a kitűzött cél, az alkalmazott előírások hatékonyságát semmiféleképpen sem szabad pusztán az adott előírás betartása miatti költségnövekedés szempontjából vizsgálni, hiszen a berendezés emberéletet ment(het). És csak ez számít!

A statisztikai módszer felhasználása alatt ebben az esetben a megtörtént „éles” alkalmazások elemzését értem, amelyek „első kézből” gazdagítják az adott vészelhagyó berendezés biztonságos üzemben tartási előírásainak, üzemeltetői szintű utasításainak összességét. A vérrel írt tapasztalatok ezen a speciális területen ténylegesen életmentő szerepet kapnak. Ezt nem szabad figyelmen kívül hagyni!

Az általuk meghatározott üzemelési kritériumok alapján kerül be az adott repülőeszközzel történő repülések végrehajtási módszereit leíró szabályzatba a vészelhagyással kapcsolatos kötelező cselekvéssor leírása, azok betartandó paraméterei (minimális repülési (vészelhagyási) magasság, maximális repülési (vészelhagyási) sebesség a katapultálás végrehajtásához és a pilóta mentőejtőernyő biztonságos belobbanásához).

Az adott vészmentő berendezés rendszerben tartása során bekövetkező használatának üzemeltetési tapasztalatait mindenképpen érdemes felhasználni az adott berendezés további üzemeltetésének még biztonságosabbá tétele érdekében. Erre a katapultált pilóták jelentéseit, a lezuhant repülőeszközök fedélzetén elhelyezett objektív kontroll berendezések adattároló egységei által szolgáltatott repülési információkat, valamint az esetleges szemtanúk beszámolóit lehet felhasználni, több-kevesebb sikerrel, de mindenféleképpen a biztonság irányába történő esetleges „tévedéssel”.

Az ún. „elszámolási fázis” biztonsági jelentősége

A katapultülés biztonságos üzemelési folyamata során ennek a fázisnak ún. lezáró szerepe van. Hatását olyan szinten fejti ki, hogy a megtörtént sikeres alkalmazások száma pozitívan befolyásol(hat)ja a berendezés használatán gondolkodó személyt.

Ennek az adott vészmentő berendezés „karrierjének” kezdetén van óriási jelentősége, amikor a berendezés biztonságos működését még csak elenyésző számú „éles” alkalmazás támasztja alá.

Az általam leírásra kerülő valódi esettanulmányok a Magyar Néphadsereg repülőalakulatainál kezdetben szintén nem a katapultülés használata mellett tették le a voksot. Ahogy azonban megtörtént az első sikeres katapultálás, - majd sorban a többi is –, az adott katapultülés respektje hirtelen nagyot nőtt a repülő-hajózó állomány szemében.

Az esetek leírása a tanulmány II. részében, a Hadmérnök következő számában olvasható.

Felhasznált irodalom

[1] Bakos Ferenc: Idegen szavak és kifejezések szótára. Akadémiai Kiadó, Budapest, 2007. Változatlan utánnyomás, első kiadás: 1994. ISBN 978-963-05-7875-25. 590. o.

[2] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 12. o.

[3] V. Zsukov mérnök-százados: Katapultálás hangsebesség feletti repülés közben. Újdonságok a haditechnikában. Zrínyi Katonai Kiadó, Budapest. 1960. 254. o.

[4] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 14. o.

[5] А. Г. Агроник, Л. И. Эгенбург: Развитие авиационных средств спасения. Издательство Машиностроение, Москва, 1990. ISBN 5-217-01052-5. 100. o.

[6] Н. А. Лобанов: Основы расчёта и проектирования парашютов. Издательство Машиностроение, Москва. 1965. Заказ 1101/5727. 269. o.

[7] Nuttal J. B.: Repülőgép és kozmikus jármű kényszerelhagyása. (rövidített fordítás) Ejtőernyős Tájékoztató, 1978/1. LRI Repüléstudományi és Tájékoztató Központ kiadása, Budapest. 31-35. o.

[8] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 16. o.

[9] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 17. o.

[10] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 17. o.

[11] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 18. o.

[12] Repülési lexikon. Második kötet M-Z. Akadémiai Kiadó, Budapest. 1991. ISBN 963 05 6209 337. o.

[13] Re/552 Az ejtőernyők szerkezete, felépítése és üzemeltetése. A Honvédelmi Minisztérium kiadása. 1964. 21-33. o.
[14] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 18. o.
[15] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 18. o.
[16] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 18. o.
[17] А. Г. Агроник, Л. И. Эгенбург: Развитие авиационных средств спасения. Издательство Машиностроение, Москва, 1990. ISBN 5-217-01052-5. 101. o.
[18] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 15. o.
[19] Zsák Ferenc: Katapultáló magyarok. Aeromagazin, 2009. február, 52-55. o.
[20] А. Г. Агроник, Л. И. Эгенбург: Развитие авиационных средств спасения. Издательство Машиностроение, Москва, 1990. ISBN 5-217-01052-5. 101. o.
[21] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 38. o.
[22] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 38. o.
[23] А. Г. Агроник, Л. И. Эгенбург: Развитие авиационных средств спасения. Издательство Машиностроение, Москва, 1990. ISBN 5-217-01052-5. 104. o.
[24] В. Г. Романюк: Заметки парашютиста-испитателя. Военное Издательство Министерства Обороны СССР, Москва, 1973. 103160. 250. o.
[25] G. Beregovoj: Egy űrhajós feljegyzései. Kozmosz Könyvek, Budapest. 1973.
[26] А. Г. Агроник, Л. И. Эгенбург: Развитие авиационных средств спасения. Издательство Машиностроение, Москва, 1990. ISBN 5-217-01052-5. 104. o.
[27] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 42. o.
[28] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 42. o.
[29] Dr. Kiss Sándor mk. alezredes: Biztonságtechnika alapjai. Főiskolai jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar, Budapest. 2004. 43. o.

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Kiss Béla
kiss.bela1979@freemail.hu

A MAGYAR HONVÉDSÉG HELIKOPTEREINEK TÍPUSVÁLTÁSA, MODERNIZÁLÁSA, ANNAK LEHETSÉGES HATÁSI A KATASZTRÓFAVÉDELMI FELADATOK ELLÁTÁSÁRA

Absztrakt

Az új helikopterek beszerzésénél két fő prioritást kell figyelembe vennünk. Az első az ország védelmi képességéhez szükséges és a NATO szövetségi rendszerből adódó elvárásoknak való együttes megfelelés, a másik a katasztrófavédelmi feladatok ellátásához szükséges repülő technikai képességek birtoklása. A Magyar Honvédség a 70-es évektől folyamatosan beszerzett és mai napig használatban lévő helikopterei napjainkra korszerűtlenné váltak és a többségüknek a repülési üzemideje lejárt, ezért cseréjük szükségessé vált. Az új repülőeszközök hadrendbe állításáig megoldást jelenthet a jelenleg még műszaki üzemidővel rendelkező, de ipari nagyjavításra, főalkatrész-cserére váró helikopterek üzemképessé tétele.

While purchasing new helicopters, we have to focus on two vital priority. First, is to buy helicopter which meets with homeland defensive measures and to maintain NATO requirements within the alliance. The other to obtain a aerial capability to carry out missions in disaster recovery role. The helicopters – what by HDF were buy from the '70-s and are still in use – for these days became obsolete and most of their operating time are up, therefore the substitution is necesarry. Until the deploy of the new helicopters, can be a temporary solution to make ready to operate of the existing helicopters which are waiting for renewal but still have operating time.

Kulcsszavak: *képesség, helikopter, katasztrófavédelem, védelmi képesség, multifunkcionális ~ ability, helicopter, disaster recovery, defensive capabilities, multifunctional*

BEVEZETÉS

Napjainkra a parlamenti pártok között konszenzus alakult ki a Magyar Honvédség helikopterei és repülőgépei beszerzésének szükségességéről. Az ország szükségleteit és igényeit figyelembe véve megfogalmazott követelményrendszer alapján a tervek szerint Magyarország kormánya 2014 tavaszáig elkészíti és kiírja a helikoptertendert. A típusváltás elsődleges oka a jelenleg rendszerben lévő forgószárnyas technikák elavultsága, hiszen beszerzésüket még a Varsói Szerződés idején írták alá. A honvédség egy olyan képességéről beszélünk, amely nem csupán katonai, hanem egyidejűleg katasztrófavédelmi célokat is szolgálja. Az elmúlt évek és évtizedek tapasztalatai alapján elmondható, hogy a katonai helikopterek ott voltak és tették a dolgukat minden olyan súlyos katasztrófahelyzet során, amely megkövetelte alkalmazásukat. (tiszai árvizek 2001, 2006, borsodi árvíz 2010, vörös-iszap katasztrófa 2010. október 4-én). A helikopterek típusváltására eddig több koncepció is született, amelyeket végül elvetettek. Az első változat alapján az - 1. számú ábrán látható - amerikai UH-1N típusú helikoptereket szerzett volna be a honvédelmi tárca.

1. ábra. UH-1N helikopter [1]

„A HM által nyújtott tájékoztatás alapján, a felajánlott helikopterek műszaki üzemidejük felét használták fel, így még gépenként átlag 8-9000 repült óra állt volna rendelkezésünkre, ami magyar viszonyok között, körülbelül 25 év rendszerben tartásra elegendő. Megjegyzendő, hogy a tűzoltó eszközök, közöttük a tűzoltó gépjárművek is szabvány szerint 20 évig üzemeltethetőek. [2] Ezzel egy időben érkezett az olaszországi Augusta Westland AW139-es típus ajánlata, melynek hírek szerinti anyagi vonzata számunkra közel azonos volt a használt UH-1N-ével. Az AW139-esek beszerzésétől – vélhetően a gyártó cég sajtóból olvasható korrupciós botrányai miatt (is) - a magyar fél elállt. A probléma megoldása azonban égető fontosságú, hiszen a katonai feladatok mellett egyre gyakrabban lenne szükség a helikopterekre a katasztrófavédelmi helyzetekben is. Jó példa erre az idei március. 15-ei hóvihar, amely több autópályát és útszakaszt megbénított Magyarország területén.

HELIKOPTEREK A KATASZTRÓFAVÉDELEM SZOLGÁLATÁBAN

A Magyar Honvédség helikopterei katonai feladatokon túlmenően nagyon fontos szerepet töltenek be az Országos Katasztrófavédelmi Rendszer elemeként, Magyarország katasztrófavédelmi feladatainak ellátásában. A Honvédelmi Katasztrófavédelmi Rendszer 24 órás helikopteres szolgálatai (Légi Kutató Mentő Készenléti és Légi Sugárfelderítő Szolgálat) a nap 24 órájában állnak készen feladatuk végrehajtására. A Légi Kutató Mentő Készenléti Szolgálat (továbbiakban LKMSZ) rendeltetése, az ország légterében bajba jutott légi járművek keresése, kutatása, esetlegesen sérült személyek elsősegélyben részesítése, életben tartása a magasabb szintű orvosi ellátáshoz jutásig. Hazánkban jelenleg két LKMSZ működik, az egyik Pápa Bázisrepülőtéren, a másik az MH 86. Szolnok Helikopter Bázison települ. A

szolgálatok kelet és nyugat magyarországi körzetekre bontják a légteret, melyek választóvonala a Duna. A feladatok ellátásához 6 fős szakszolgálati személyzet (2 fő hajózó, 2 fő ejtőernyős, 1 fő felcser, 1 fő technikus), és egy Mi-8-as közepes szállítóhelikopter áll a rendelkezésre (2. számú ábra).

2. ábra. Lángoló domb 2005 kutató-mentő gyakorlat [3]

A Légi Sugárfelderítő Szolgálat rendeltetése hadiállapot, vagy ipari szerencsétlenség következtében létrejövő nukleáris katasztrófa esetén a szennyezett terepszakasz felmérése, detektálása, illetve pontszerű sugárforrás (esetlegesen „piszkos bomba”, ellopott nukleáris fegyver) keresése, felkutatása. A szolgálat szakszemélyzeti állománya 2 fő hajózóból, míg technikai eszközeit tekintve: egy Mi-24-es harci helikopterből, egy GPS készülékkel összekapcsolt sugármérő konténerből áll. A légi sugárfelderítő járőr szennyezett terepszakasz esetén képes 300 km^2/h, pontforrás esetén pedig 18-20 km^2/h terület felmérésére. A felderítés megkezdésének legkorábbi időpontja a kihullás végétől számított 2 óra.

A honvédség helikopterei árvízvédelmi feladatokból is számos alkalommal vették ki a részüket, melynek fő területei:

- életmentés – kimenekítés: a víz által körülzárt települések lakóinak orvosi ellátáshoz jutatása, a körülzárt településről történő kimenekítésük;
- a védekezéshez szükséges anyagok utánpótlásának szállítása;
- külső függesztmények beemelése megindult gátszakaszok esetében. (A speciálisan erre a célra készített és megerősített homokzsákok befogadóképessége 1 tonna, amelyeket általában homokkal, sóderrel vagy földel, töltenek meg.)

A Mi-8-as típus 3 tonna külső függesztmény vagy 24 fő, míg a Mi-24-es 2,4 tonna külső függesztmény és 8 főt képes szállítására alkalmas.

3. ábra. Tűzoltás a levegőből [4]

Az erdőtüzek levegőből történő oltásának egyik leghatékonyabb eszköze a helikopter, melynek egyik lehetséges bevált kelléke egy kanadai gyártmányú összecsukható gumifalú víztartály (3. számú ábra), az úgynevezett „Bambi Bucket”, amely. Ennek vízzel való feltöltése, utántöltése történhet mesterséges víztárazókból, medencékből, vagy természetes vizekből (tavakból, folyókból), illetve tűzoltó fecskendővel. A helikopterről való tűzoltás működési elve, hogy a Bambi Bucket-ben lévő vízmennyiség a kiáramlását követően szétporlad a levegőben, lehűti azt, ezáltal az éghető anyag hőmérséklete a gyulladási hőmérséklet alá csökken.. A feladat végrehajtásának meghatározó összetevői: a repülési sebesség és magasság, a szél erőssége és iránya, valamint a kibocsátás magassága [13].

LEHETSÉGES KONCEPCIÓK A MAGYAR HONVÉDSÉG HELIKOPTREINEK A TIPUSVÁLTÁSÁRA

Jelenlegi helikoptereink váltó típusának kiválasztásánál mindenképpen a tervezet és végrehajtani kívánt feladatból kell kiindulni. Ehhez Magyarországon – megítélésem szerint - egy multifunkcionális helikopterképességre van szükség, amely képes a haza védelmének és ezzel egy időben a katasztrófavédelmi feladatokból adódó kihívásoknak is eleget tenni. A feladatrendszer komplex áttekintésének részeként fontos vizsgálni a gazdaságosság és költséghatékonyság kérdését is. Véleményem szerint luxus, olyan típusokat olyan feladatrendszerhez használni, ami drága, mivel az üzemeltetés költségi egy közepes helikopternél, sokkal jelentősebbek, mint egy könnyebb, kisebb egyszerűbb típusénál. Ezért a honvédelmi vezetésnek célszerű olyan helikopter típust keresni, amely a védelmi feladatok mellett légi rendészeti, kutató-mentő és katasztrófaelhárító feladatokra - például árvízi védekezés, légi tűzoltás - is használható. A követezőekben - a teljesség igénye nélkül - bemutatom ezen elvárásoknak megfelelő, a hazai típusváltás során - megítélésem szerint - számításba vehető típusait.

Mi-171

A Magyar Honvédség jelenlegi helikoptereinek géptípusai szinte kivétel nélkül a Mil család részei (Mi-8-as, Mi-17-es, Mi-24-es), amelyeknek beszerzését a 70-es évektől kezdték el. A Mi-17-es korszerűsítése, továbbfejlesztése révén készült el a 4. számú ábrán látható Mi-171-es közepes, többfeladatú helikopter.

4. ábra. A Mil-Mi-171 [5]

A típus sokoldalúságának és nagy teljesítményének köszönheti népszerűségét és azt, hogy a Mi-8 és Mi-17-es típusokkal együtt közel 11000db-ot adtak el belőlük, illetve jelenleg is a világ 80 országában alkalmazzák. Teherszállító képességét tekintve a helikopter közel 4000 kg, vagy 26 fő szállítására alkalmas a $27m^3$ –es rakterében, és ugyanannyi 4000 kg külső

függesztmény felemelésére képes. A helikopter speciális rendszereinek köszönhetően viszonylag alacsony zajszint és vibráció mérhető az utastérben.

A Mi-171-es alkalmazható személyek és rakományok szállítására, szárazföldi csapatok tűztámogatására, katonai oszlopok kísérésére, légi oltalmazására. A helikopter felszereltségét, repülési jellemzőit és az 1. számú táblázatban láthatóak harcászattechnikai adatait tekintve kivallóan alkalmazható katasztrófavédelmi feladatok végrehajtására is. Kutató-mentő feladatok ellátásához két külső csörlős emelővel szerelték fel, amelyekhez 150 kg, 270 kg, vagy 300 kg emelésére alkalmas kosár tartozik. A mentőhelikoptert 12 hordággyal lehet berendezni, maximális evakuálási képessége pedig 37 fő. A kutatás-mentési feladatok ellátásában a személyzet munkáját segíti a fedélzeten telepített Doppler időjárási radar, az infravörös kamera és a navigációs rendszer. A helikopter rendelkezik a Night Vision (NVG) „éjjel látó" képességgel, ezért a szakszolgálati személyzet éjszaka is végre tudja hajtani a katatás-mentési feladatokat. Tűzoltási feladatokhoz egy 3500 literes Bambi Bucket-et rendszeresítettek, ezen kívül a helikopter képes 34 tűzoltót teljes felszereléssel elszállítani a kárhelyszínre. A típushoz külön megvásárolható egy Simplex rendszer, amely kiválóan alkalmazható horizontális tűzoltáshoz, többemeletes lakóépületek tűzeseténél.

Felszálló tömeg	**Rakodótér mérete:**	**Helikopter mérete:**	**Forgószárnylapátok száma: 5 db.**
Normál: 7489 kg	Magasság: 1,8 m	Hosszúság: 18,65 m	Személyzet: 3 fő
Max.: 12000 kg	Szélesség: 2,34 m	Magasság: 4,75 m	Utasok száma: 27 fő
	Hosszúság: 5,34 m	Szélesség: 5 m	Hordágyak száma: 12 db
Alkalmazási területek: teherszállítás, tűzoltás, beemelés, egészségügyi, katonai, evakuálási, személyszállítás, kutatás-mentés. Utazó sebesség 230 km/h			

1. táblázat. Mi-171-es helikopter harcászattechnikai adatai [6]

A helikoptertípus rendszerbeállításának elsődleges előnye a pilóta és műszaki állomány meglévő szakismerete az elől típusokra. Egy minimális átképzés elvégzésével a műszaki és hajózó állomány máris üzemeltethetné a haditechnikát.

AgustaWestland AW139M

A közelmúltban az Egyesült Államok felajánlott 30 db, náluk a rendszerből kivont, de üzemképessé tehető UH–1N típusú szállító helikoptert, melyek hazai üzembe állítása, alkatrészellátása, a kiképzés mintegy 350 millió dollárba kerülne. Ez a helikopter jelenleg is nagy számban repül, a világ számos országában, de ennek ellenére egy kiöregedő típusnak számít. Az Egyesült Államok felajánlása után nem sokkal – sajtóhírek szerint hasonló árért – egy olasz ajánlat is érkezett 20 db AugustaWestland AW139 helikopterekről [7]. Az AW139M új generációs, két gázturbinás, közepes szállítóhelikopter, elsősorban polgári felhasználásra tervezve. Azonban az AW139 militarizált változata megfelel a katonai és belbiztonsági elvárásoknak és kiválóan alkalmazható katasztrófavédelmi feladatok ellátására. A helikopter harcászati-technikai adatai a 2. táblázatban láthatóak. Felszerelhető katonai, MEDEVAC (Medical Evacuation / egészségügyi kimentés), CASEVAC (Casuelity Evacuation / sebesült kimentés), SAR (Search and Rescue / kutató mentő), CSAR (Combat Search and Rescue / harci kutató mentő) és légi tűztámogatási feladatok ellátásához szükséges felszerelésekkel. „Az AW139M az AW139 katonai változata, továbbfejlesztett, erősebb gázturbinás hajtóművekkel. Az AW139 által elért sikerekre alapozva fejlesztették ki az AW139M-et, megcélozva a külföldi piacokat is. Célul tűzték még ki, hogy a különleges katonai követelményeknek megfeleljenek, valamint az adott ország belbiztonsági és kormányzati tevékenységét is biztosíthassák." [8]

Az 5. számú ábrán látható harctéri támogató változat kabinjában 15 személy, vagy 10 fegyveres katona szállítható. A típus külső függesztmény ként, 2200 kg-ot képes továbbítani. A szárazföldi csapatok tűztámogatása 5,56-os, vagy 7,62, mm-es, illetve egy rögzített 12,7 mm-es géppuskával biztosítható. A rakéta támadások elleni védelemre a helikoptert felszerelték rakétaközeledés jelző és zavarótöltet szóró rendszerekkel.

Emelkedő képesség: 10,9 m/sec	**Helikopter mérete:**	**Forgószárnylapátok száma: 5 db**
Normál felszálló tömeg: 3622 kg	Hosszúság: 16,66 m	Szállítható személyek: (2+15) fő
Max. felszálló tömeg: 6800 kg	Magasság: 4,96 m	Utazó sebesség: 306 km/h
Max. hatótávolság: 1061 km	Szélesség: 2,26 m	Hordágyak száma: 12 db
Alkalmazási területek: felderítés, teher és személyszállítás, speciális erők feladatai, MEDEVAC, CASEVAC, SAR, CSAR, légi harcálláspont és légi tűztámogatási feladatok		

2. táblázat. AgustaWestland AW139M helikopter harcászattechnikai adatai [9]

E légijármű hatékonyan képes segíteni a parancsnokok munkáját a hadműveleti területen, az úgynevezett Blue Force Tacker, ellenség barát felismerő rendszerével, amely műholdas térkép segítségével ábrázolja a saját illetve az ellenséges csapatok elhelyezkedését.

5. ábra. AgustaWestland AW139M [10]

Katasztrófavédelmi feladatok ellátásához a mentő típus a legjobb választás, amely a közel 8 m^3 kabinjának köszönhetően 2-6 db hordágy elhelyezését teszi lehetővé. A helikopter kiválóan alkalmazható MEDEVAC és CASEVAC (egészségügyi/sürgősségi mentés) feladatok ellátására. A vásárló igényei szerint alakíthatja ki és szereltetheti fel a számára szükséges felszerelésekkel az alap helikoptertípust. A teljesség igénye nélküli felszereltsége a következő: zárt, túlnyomásos üzemanyagtöltő rendszer (utántöltés járó hajtómű mellett is), pót üzemanyagtartály (500 l), jégtelenítő rendszer, 1 vagy 2 db csörlőberendezés (272 kg teherbírással), mentőcsónak, keresőfényszóró, moduláris páncélzat, deszant ülések és MEDEVAC hordágy, alpinkötelek / FAST ROPE (gyorsköteles ereszkedés) kit, időjárás és keresőradar, NVG-kompatibilitás (külső és belső lámpák), külső fegyverzet (géppuska konténer és 70 mm levegő föld nem irányított rakétablokk), mozgatható géppuskák (ajtólövész feladatokhoz), levegő-föld rakéták. A típus eddig még nem bizonyított a katonai alkalmazás területén, csak papírforma szerint, így megkérdőjelezhető a valódi alkalmassága a feladatra.

Változatok:

- AB139 – ebből a változatból 54 darab épült Olaszországban;
- AW139 – Olaszországban és az Egyesült Államokban is készült;
- AW139 LNC18 – hosszított orrésszel rendelkezik, mind Olaszországban mind pedig az Egyesült Államokban gyártják;
- AW139M – az AW139 katonai változata akár 15 katona vagy 6 hordágy és 4 fő orvosi kísérő szállítására is alkalmas. Emellett rakéta-blokkokkal, levegő-föld rakétákkal és külső tartályokkal felszerelhető;
- HH139A – az Olasz Légierő számára tervezett kutató mentő változat. Eddig 10 darab készült belőle. [11]

6. ábra. AgustaWestland HH-139A pilótafülkéje

A 6. számú ábrán az Olasz Légierő kötelékébe tartozó AgustaWestland HH-139A típusú helikopter pilótafülkéje látható, amelyet 10 in x 8 in aktív mátrix, folyadékkristályos kijelzőkkel szereltek fel és rendelkezik digitális, 4-tengelyes automatikus repülésirányító rendszerrel.

ÖSSZEGZÉS

A Magyar Honvédség forgószárnyas repülőgépeinek naptári üzemideje lejárt, nagyjavítás csak néhány gépen végezhető el. Azonban a helikopteres képesség megőrzése elsődleges szempont az ország védelmének és katasztrófavédelmi feladatainak ellátása érdekében. Az ezekhez kapcsolódó feladatrendszerek vizsgálatával megalapítható, hogy ma Magyarországon egy olyan multifunkcionális helikopterképességre van szükség, amely egyidejűleg alkalmas a haza védelméből és a katasztrófavédelmi feladatokból adódó kihívásoknak is megfelelni. A haditechnika típuscseréjénél fontos figyelembe venni a gazdaságosság és költséghatékonyság kérdését, hiszen a helikoptervásárlás nem olcsó, hatalmas, közel 100 milliárd Ft-os kiadást jelent a honvédelmi tárca számára. Éppen fiskális okok miatt 2012-ben Magyarország visszautasította az amerikaiak 32 db-os UH-1N típusú helikopter ajánlatát, hiszen az ingyen gépek karbantartása, logisztikai utánpótlása, a pótalkatrész ellátás és a személyzet kiképzése így is közel 426 millió dollárba került volna. A jelenleg is zajló típusváltási eljárás és az új helikopterek típus hadrendbe állításáig a meglévő flotta néhány helikoptere üzemben tartható, de ehhez el kell végezni rajtuk a szükséges nagyjavítási feladatokat. A helikopterek jövőbeni feladatrendszerét tekintve egy, a honvédelmi és a katasztrófavédelmi feladatok ellátására egyaránt alkalmas, többfunkciós típus beszerzése jelentene optimális megoldást.

Felhasznált irodalom

[1] Jesse Lopez, USAF: Az USAF, azon belül a Minot légi bázis egyik UH-1N forgószárnyasa http://htka.hu/2012/11/03/elesedik-a-harc-a-honvedseg-kegyeiert/ (letöltés:2013.05.31)

[2] Dr. Csutorás Gábor: Az UH-1N típusú helikopter baleseti tűzoltás-mentésének.) kérdési http://www.szrfk.hu/rtk/kulonszamok/2012_cikkek/35_Csutoras_Gabor.pdf (letöltés: 2013.05.21.)

[3] Dr. Toperczer István: Lángoló domb 2005 kutató-mentő gyakorlat http://www.jetfly.hu/rovatok/legter/domb_050607/ (letöltés:2013.05.22.)

[4] Balogh Ákos: Tűzoltás a levegőből http://lhsn.hu/tuzoltas-a-levegobol/ (letöltés: 2013.05.22.)

[5] A Mil-Mi-171 http://avia-russia.com/mil-mi-171.html (letöltés: 2013.05.28.)

[6] Kiss Béla főhadnagy: Mi-171-es helikopter harcászattechnikai adatai http://jets.hu/news?id=165 (letöltés: 2013.05.28.)

[7] HTKA, Haditechnikai Kerekasztal, (e-dok.) http://htka.hu/2012/05/21/olasz-helikoptereket-vehet-ahonvedseg/ (letöltés: 2013.05.21.)

[8] AW139M AgustaWestland, (e-dok.) http://www.agustawestland.com/product/aw139m (letöltés: 2013.05.23)

[9] Jets.hu: AgustaWestland AW139M helikopter harcászattechnikai adatai http://jets.hu/news?id=255 (letöltés: 2013.05.23.)

[10] Balogh Ákos: AgustaWestland AW139M http://htka.hu/2013/01/06/egy-tipusvaltas-margojara/ (letöltés: 2013.05.30.)

[11] Papp István: Helikopterváltás a Magyar Honvédségben – az AgustaWestland AW139. PP. 381. http://www.szolnok.mtesz.hu/sztk/kulonszamok/2012/cikkek/2012-32-Papp_Istvan.pdf (letöltés: 2013.05.29.)

[12] Giovanni Maduli: Inside a modern (combat) helicopter: the AgustaWestland HH-139A glass cockpit http://theaviationist.com/2012/07/18/hh139a-glass-cockpit/#.UanO6kCjdBh (letöltés: 2013.05.29.)

[13] Restás, Á. [2011c] Az erdőtűzoltás hatékonyságának közgazdasági megközelítése; Védelem, XVIII.Évfolyam 5. szám, Budapest, 47-50 oldal, ISSN: 1218-2958

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Venekei József
venekei.jozsef@uni-nke.hu

ROLE OF BULK FUEL INSTALLATIONS (BFIS) AND FIELD PIPELINE SYSTEMS IN OPERATIONAL SUPPLY CHAIN

Abstract

Bulk Fuel Installations and Field Pipeline Systems (FPSs) can be considered as logistic installations for the purpose of fuel management in the operational area. Mobility, capability of force elements depends mainly on provision with fuel. Operation of Bulk Fuel Installations and Field Pipeline Systems in the area of operation based on utilization of Host Nation Support (HNS) capabilities and Contractor Support to Operations (CSO). In the article the author introduces the designation, main parts, capabilities and role of BFIs and FPSs in Operational Support Chain.

A folyékony üzemanyagok tárolására szolgáló létesítmények (Tábori üzemanyag raktárak) és tábori csővezeték rendszerek alapvető rendeltetése a műveleti területen tevékenykedő erők üzemanyaggal való ellátása. Az erők mobilitása, műveleti képessége nagyban függ a hatékony üzemanyag ellátástól. Az alkalmazott létesítmény működtetésének sikere a műveleti területen csak a Befogadó Nemzeti Támogatás képességeinek kihasználásával és a szerződéskötésen alapuló támogatás alkalmazásával érhető el. A szerző cikkében bemutatja a folyékony üzemanyagok tárolására szolgáló létesítmények és tábori csővezeték rendszerek alapvető rendeltetését, fő részeit, alkalmazási lehetőségeiket és a műveleti támogatási láncban betöltött szerepüket.

Keywords: *Bulk Fuel Installation, Field Pipeline System, Operational Support Chain ~ Tábori üzemanyag raktár, tábori csővezeték rendszerek, műveleti támogatási lánc*

INTRODUCTION

Application of pipeline systems can't be considered as a new supply method with fuel in military support chain. During the WWII[1] Russians used a field pipeline to support citizens in Leningrad, that was surrounded by german troops. They managed to lie down the pipes under the ice of frozen lake Ladoga. Later on field mainline pipeline systems proved themselves as a primary method to support russian troops with fuel during the war in Afghanistan[2]. Member states situated in Central Europe also recognized the advantages of military pipeline systems.

The Central Europe Pipeline System (CEPS) is the largest cross-border multi-product petroleum pipeline system in NATO. The CEPS crosses the Host Nations of Belgium, France, Germany, Luxemburg and The Netherlands and is over 5,599 km long. With 33 depots, its storage capacity is over 1,250,000 m^3. The NATO Central Europe Pipeline System (CEPS) Programme manages the operation, financing and maintenance of an integrated, cross-border fuel pipeline and storage system in support of NATO's operational military requirements during peacetime, crisis and conflicts, including expeditionary operations. The day-to-day pipeline operations and maintenance is executed by four National Organisations and their respective dispatching centers. The CEPS Programme member nations are Belgium, France, Germany, Luxemburg, the Netherlands, and the United States. The member nations with CEPS assets within their territory are called the Host Nations and comprise: Belgium, France, Germany, Luxemburg and the Netherlands.The CEPS Programme Office assures operational, technical, budgetary and administrative control of the CEPS in peace- and wartime in accordance with the Charter of the NATO Support Organisation. [1]

1. Figure. Scheme of NATO CEPS
(www.nspa.nato.int)

Application of military pipelines has many advantages and disadvantages. However, pipelines and hose lines have their limitations too.

Advantages

- Pipelines offer many advantages over other conventional means of transporting petroleum products. From an economic point of view, the pipeline is the least expensive transportation method in which to send large quantities of products over distances.
- Pipelines are all-terrain modes of transportation which allow access to areas that not suitable for other forms of transportation.
- Pipelines relieve the burden of fuel transportation from rail and road nets, which are more expensive and congestive. Bear in mind, approximately sixty percent of logistic

[1] Second World War
[2] Soviet-Afghan War, 1979-89.

tonnages is bulk petroleum. Using a tactical mainline pipeline system, we can deliver almost 2.5 million litres of fuel forward each and every day. This will free up approximately 250 military tankers (with the capacity of 10 cubic metres) to move forward to support the tactical fight.
- Pipelines offer extremely poor targets for enemy aircraft.
- Pipeline damage can be repaired much faster than damaged railroads or highways.
- Pipeline operations are not affected by adverse weather conditions.
- Pipeline use frees up large numbers of personnel and vehicles that can be used for other logistic activities.

Disadvantages

- Pipelines are subject to disruptions by sabotage and guerrilla attacks.
- Marine terminals, pump stations, and tank farm complexes are attractive targets for enemy air and missile attacks.
- Locating leaks and damage is time consuming.

Conventional warfare will use pipelines in much the same way as they were during WWII and the Soviet-Afghan War. Although equipment and technology change, the concept does not change. Employment, however, will require increased quantities of fuel and a pipeline system capable of quick deployment and emplacement.

DESIGNATION AND CONSTRUCTION OF BULK FUEL INSTALLATIONS

Bulk fuel installations are logistic installations for the purpose of fuel management. Bulk fuel installations can be categorized by means of their size and logistics support area as follows:

- *Forward BFI* with a storage capacity of up to 10 m³ for highly mobile and immediate fuel supply – in particular for Army Aviation units;
- *Battlefield BFI* forward BFI of the in-theatre forward logistic base with a storage capacity of up to 900 m³ for immediate fuel supply;
- *Main BFI* BFI of the in-theatre logistic base or on a deployed operating base (DOB) with a storage capacity > 500 m³.[2]

As a general rule, an in theatre logistic base BFI or a DOB BFI (Main BFI) will be filled by civilian or military road tank trucks, rail tank cars, inland vessels or seagoing ships according to the supply principle (i.e. the fuel will be delivered to the BFI) involving Host Nation Support or Contractor Support to Operatnios (HNS/CSO). Connection to another type of pipeline system (stationary or field-type) is possible.

BFI consists of the following technical equipment:

1. Field Pipeline Equipment (used by German Bundeswehr)
2. NATO Mobile Pipeline Repair Equipment (MPRE).

Field Pipeline Equipment is used to construct BFIs, to temporarily restore the working order and operability of damaged or destroyed installations, and it is used to set up stationary pipeline systems, fuel supply installations on airfields as well as further pipeline systems. It includes individual components, like pipes, fittings, pipe connectors, hose lines, volumetres, reduction valves, flow limiters, gate valves, fuel pumps with different flow capacities, filtering devices and flexible tanks.

The MPRE was procured using NATO funds and serves the purpose of temporarily repairing damage at NATO pipeline systems and erecting replacement installations. The equipment was provided to the respective host nations for the purpose of training and sustainment training and for usage at NATO pipeline systems. This equipment is used to

repair damage at the CEPS [3]and is generally not used for BFI construction or damage repair in national responsibility.

Pipes used for BFI are made of steel, have length of 4800 mm and a nominal diameter of 150 mm. For couplings of pipes steel shackles are used with rubber washer. Coupled pipelines must not rest on the ground. Couplings must be tensionless, accesible and visible for inpection. They must feature a drip pan underneath.

2. Figure. Coupling
(Photo made by the author)

Fuel pumps for unloading have volume flow of up to 250m^3 cubic metres per hour, pumps for loading have volume flow of up to 150 m^3 per hour.

3. Figure. Fuel Pump for loading
(Photo made by the author)

Hose lines used for unloading and loading tankers, railway tankers, vessels and have connectors with multiple diameter. Volumetres (flow metres) are necessary for the registration of fuel handed over for endusers. Filtering devices are capable to clean fuel from contamination and water, the latter is extremely important for Jet fuel. It is equipped with differential manometer to measure the fuel pressure before and after the filter that let us know the time we have to change the filter cartridge.

Flexible tanks are used to store bulk fuel in it. It is made of synthetic rubber and has relatively big mechanical strength. Its material consists of three different layers which are connected to each other with glue. The outer layer is made of weather resistant synthetic rubber, the inner layer is resistant to chemical materials and there is a relatively thin but strong textile layer in the middle to provide mechanical strength. Flexible tanks have two connections for filling and a valve for evaporation.[3]

[3] See NATO Central Europian Pipeline System

4. Figure. 50 m3 Flexible Tank in Dyke
(Photo made by the author)

FUNCTIONAL ELEMENTS OF BULK FUEL INSTALLATIONS

BFIs functionally can be divided into four parts.

1. Unloading station

Unloading station of BFI is designed to unload civilian or military tankers outside of the fuel depo. Depending on construction it is possible to download tankers in paralell using hose lines with the appropriate connection type. In this case the unloading suction pump will pump the unoaded fuel into the flexible tanks situated in tank farm.

5. Figure. Unloading Section with two ends
(Photo made by the author)

2. Main manifold

Main manifold is used for the control of fuel flow amongst the functional elements inside BFI. For the regulation of fuel flow the main manifold joins the pipeline sections that are connected to the functional elements and uses gate valves to control the direction of fuel flow.

6. Figure. Main Manifold of BFI
(Photo made by the author)

3. Tank Farm

Tank farm is designed to store ground fuel with the capacity of 150m^3 and aviation fuel with the capacity of 1200 m^3. The total capacity of BFI is 1350 m3. In ground fuel section there is a 38 m^3 flexible tank installed for safety purposes. Each flexible tank in tank farm has set up in his own dyke. Dykes are used in case of damage of flexible tanks, because the drained away fuel is easy to collect and won't contaminate the ground. Flexible tanks in ground fuel section and the aviation fuel section too are connected to each other thus the stored fuel can be pumped over from one tank to another.

7. Figure. Ground Fuel Section (150 m3)
(Photo made by the author)

4. Loading station

The loading station for aviation or ground fuels is used for filling up to two aircraft or road tankers simultaneously. The fuel is conveyed by the tank group pump through the main manifold to the tankers. When filling aircraft tankers with aviation fuels a filter with water separation unit shall be placed immediately upstream of the filling points in order to remove any remaining quantities of water from the fuel. Bearing in mind that tankers may be filled at a maximum rate of 60 m^3 per hour, a flow limiter (60 m^3 per hour) shall be installed in each filling point. In addition a volumeter (flow meter) shall be installed at each filling point to registrate the quantity of the handed over fuel.

8. Figure. Filling Point with Flow Limiter
(Photo made by the author)

CONCLUSION

Conventional warfare with large-scale military operations will be supplied with bulk fuel up to or near front lines. It is reasonable to expect that packaged fuels will be only used as a supplement to bulk supply methods when some forward areas are not accessible to bulk fuel transporters or in some cases, when rapidly advancing tactical situations dictate the need for additional fuels to exploit the situation. To some extent, some fuels may be packaged strategically and delivered directly into a combat theater to the end user. Regardless, throughput will be used as much as possible to bypass the levels of storage.

Beyond conventional warfare, application of field mainline pipeline systems are loosing their importance, while the Bulk Fuel Concept using BFIs in the oprational area is getting more important in the operation of support chains in many hot spots of the world.

References

[1] http://www.nspa.nato.int/en/organization/CEPS/network.htm

[2] Construction and Operation of Bulk Fuel Installations BesAnFüEins 31/10-10-90-0053, Joint Support Command, Cologne, 27 th February 2009, 106.

[3] Venekei József - Üzemanyag szaktechnikai eszközök, BJKMF jegyzet, Budapest, 1993.

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Venekei József
venekei.jozsef@uni-nke.hu

LESSONS LEARNED FROM THE MULTINATIONAL LOGISTIC TRAINING PROGRAM MAGLITE 2013/1

Abstract

The exercise organised within the framework of the MAGLITE 2013/1 Multinational Logistic Training Program was conducted in June 2013 with the participation of three nations: Hungary, The United Kingdom and the Czech Republic. The Training Program was held at the Faculty of Military Science and Officers Training of the National University of Public Service. The exercise with its content and operational design approved itself as a great challange for the hungarian officers' syndicate. In the article the author summarizes the lessons learned from the exercise and describes the possibilities which may improve its succesful execution in the future.

A MAGLITE 2013/1 Multinacionális Logisztikai Kiképzés 2013 júniusában került végrehajtásra három nemzet, köztük Magyarország, az Egyesült Királyság és a Cseh Köztársaság tisztjeinek bevonásával. A képzési programnak a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kara adott helyet. A júniusi gyakorlat tartalmát és koncepcióját tekintve új kihívások elé állította a gyakorlaton résztvevő magyar tiszti munkacsoportot. A szerző cikkében összegzi a gyakorlat végrehajtásának főbb tapasztalatait és azokat a lehetőségeket melyek a jövőben tovább segíthetik a gyakorlat sikeres végrehajtását.

Keywords: *Logistics training program, Joint Logistics Operations ~ MAGLITE, Logisztikai képzési program, Összhaderőnemi logisztikai műveletek*

PRELIMINARY STEPS OF THE EXERCISE MAGLITE

First part of the Multinational Logistics Training Program MAGLITE 2013/1 was conducted in June 2013 at the Faculty of Military Science and Officers Training of the National University of Public Service with participation of three nations: Hungary, The United Kingdom and The Czech Republic.

The exercise MAGLITE is based upon the Joint Logistics Operations Course (JLOC) organized for the senior officers (majors, lieutenant colonels) of the Army, Navy and Air Force in Deepcut at the Defence Logistics School. In spite of the fact, that JLOC organized mainly for the British officers, nowadays it is getting more international due to the ivitation of foreign higher rank officers by the Defence Logistics School. MAGLITE is traditionally held in Hungary, where the officers studying at the Department of Operational Logistics joining the British syndicates can get knowledge in the field of operational level military decision making process. MAGLITE also provides a good opportunity for them to improve their common and specialized language skills and get some experience of common staff work.

In April 2013 I arrived to Deepcut to attend a coordination meeting organized by the British party. During the planning meeting I was familiarized by our partner from the British Distaff (DS)[1] Major Hutton-Fellowes with the changes in operational scenario, the joint operational area (JOA) and the size and composition of the British contingent taking part in the operation. Due to the minor changes in operational scenario we had to reconsider the size and role of our contingent which would take part in operation. Since the Humanitarian Assistance task taking place in Africa from our side demanded mainly distribution of aid from the UN bases, we had to put together a completely new force structure with logistic elements that is capable to conduct logistic operations in the operational area. The new force structure also had to give the opportunity to the Hungarian-Czech planning team to work on operational level. By the end of the meeting we agreed to deploy alltogether one transport battalion, an engineer company includig two water purification platoons in their structure and two infantry battalions for force protection. For ownlog a hungarian and a czech National Support Element has been createdas well. The new hungarian-czech force structure was in possession of logistic troops and their necessary military assets to enable the UN[2] and NGO[3]'s effort to alleviate the current Humanitarian Crisis and provide C2[4] logistic functionality to the UN and NGOs. According to the agreement I started to work on the new TOE [5]still in Deepcut.

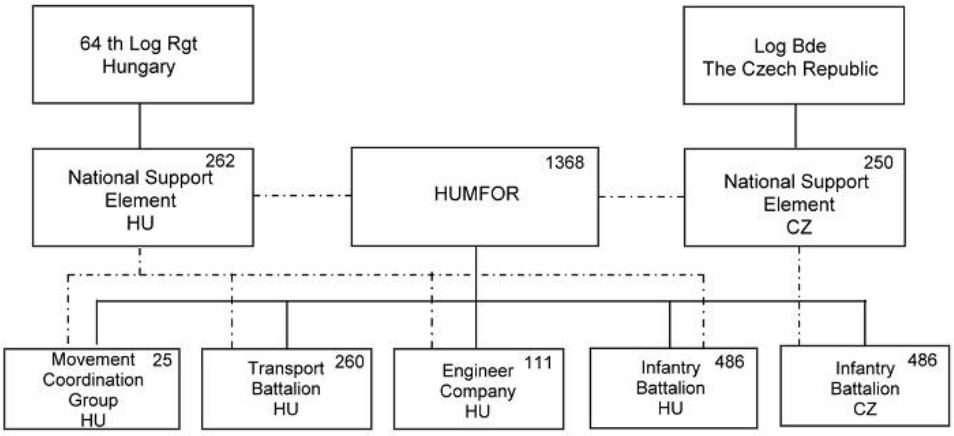
After arriving home the designated members of the Military Logistic Institute immediately started their direct preparation for the exercise.

During the period of preparation we put together the necessary exercise documentation and sorted out to the officers who were taking part in the exercise. We also created the project map for the exercise. Due to the lack of experience in operational level planning, an expert from the MoD[6] was invited who guided the hungarian participants through the steps of planning process. The preparational period of the exercise was complicated by the fact, that our team in the role of the Operation Planning Team of the Joint Force Command had to follow the new planning directive that was published in the Staff Service Regulation of HDF[7]. Two hungarian officers were delegated to each of the British Syndicates who from one hand played the role of the liaison officers of the HUMFOR[8], from the other hand took part in the

[1] Directors' staff
[2] United Nations
[3] Non Governmental Organization
[4] Command and control
[5] Table of Organization and Equipment
[6] Ministry of Defence
[7] Hungarian Defence Forces
[8] Humanitarian Forces, consisting of hungarian and Czech force elements

British MDMP[9]. Since there are some signifant differences between the British MDMP and the COPD[10] used by NATO countries, I gave a common overview for them about the steps used by the British party during the planning work.

The situation in the period of preparation has been complicated further by the fact that we faced a serious flood in the country. Since the exercise was planned to take place in the NCO Academy in Szentendre that is situated alongside the Danube river, for safety reasons we had to move the exercise back to the University for one day.



1. Figure. Staff Table of HU-CZ Contingent
(made by the author)

EXECUTIONAL PERIOD OF THE EXERCISE

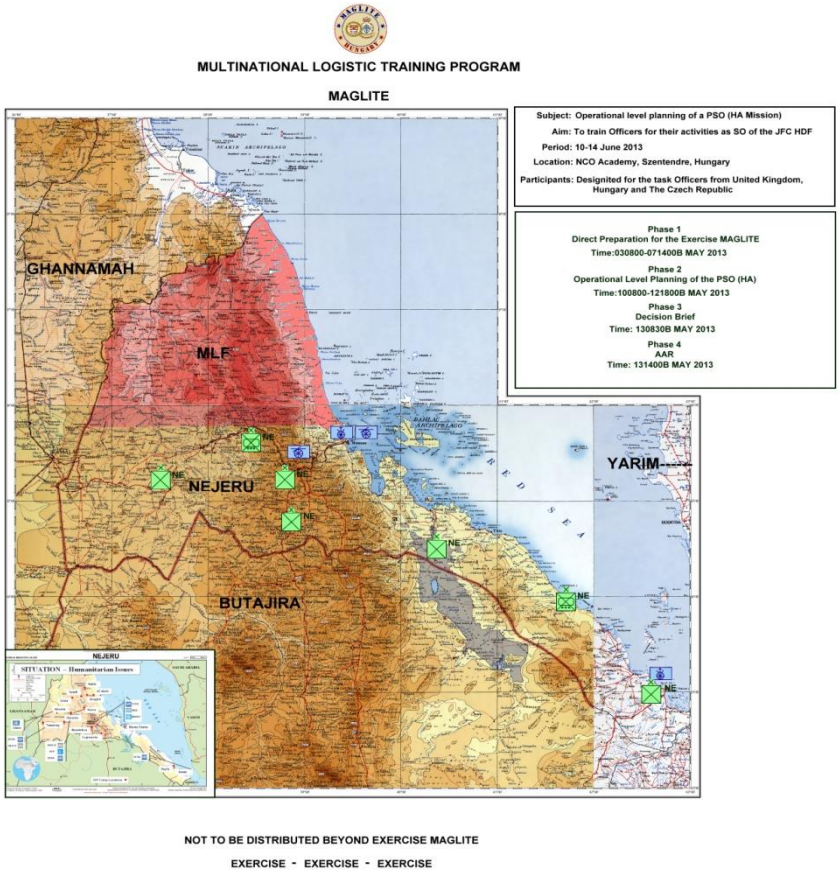
The Operational Area of the exercise was in Nejeru, a fictitious state in north- eastern part of Africa. There are famine and drought in Nejeru, thus several UN and NGO's are operating in the eastern part of the country trying to provide humanitarian assistance to local citizens.

An analysis of the Humanitarian and Development situation in NEJERU focused on the effects of war on displaced persons, the ravages of drought, hunger and HIV. The previous leadership's refusal to allow foreign agencies much scope in country has been replaced by a far more open approach, and this combined with diplomatic pressure will allow the Humanitarian Aid situation to be addressed. A UN Humanitarian Coordinator has been appointed and OCHA[11] has begun to synchronise operations. Cluster activities are being implemented and a Humanitarian Action Plan (HAP) is taking shape. However, the UN and the agencies do not have free access to all parts of the country; in particular the northern half of the country is largely denied to them and conditions in the IDP[12] Camps here are thought to be deteriorating fast.

The situation is complicated by the fact, that the UN agencies are limited by the numbers of vehicles and logistic assets in country and requests for assistance from the Nejeran Defence Forces (NDF) to provide assistance with aid distribution have been refused and the northern part of the country is controlled by a hostile organization called Muslim Legue of Freedom (MLF). NDF as directed is defeating the Muslim rebellion of the Muslim League of Freedom and see the humanitarian problem as something that should be left to others to deal with. The NDF are assessed as overstretched, inadequately resourced, and entirely committed to their

[9] Military Decision Making and Planning Process
[10] Comprehensive Operational Planning Directive
[11] Office for the Coordination of Humanitarian Affairs
[12] Internally Displaced People

existing operational challenges. They consent to the activity of NGOs and the UN but remain unable to provide either logistic lift or force protection to the humanitarian effort.



2. Figure. Project Map of MAGLITE
(made by the author)

The UK and the HU-CZ forces's mission was to conduct operations in the NEJERU JOA[13] which would include the offload and distribution of designated equipment and aid from SPODs[14] and APODs[15] and also to provide military support to the UN (and designated NGOs) to enable the distribution of humanitarian aid within JOA. In need they had to be prepared to offer C2 logistic functionality to the UN and NGO organisations and support the maintenance of secure LoCs[16] and logistic hubs within JOA, in order to create the conditions within NEJERU for the attainment of the MSTP [17]as part of the wider cross government stabilisation plan. Military Strategic Transition Point will have been reached when the UN and the government of NEJERU can stabilise the humanitarian crisis without external military support and military-led capacity building activity is underway, allowing the UK forces to hand over to the internationally appointed follow-on force. The Military Operational Endstate has been achieved when, in the short term, the deteriorating humanitarian situation has been ameliorated and the UN and NGOs working within NEJERU, have the capacity to deal with the Humanitarian Crisis without external military support. [1]

In the executional period three UK and a HU-CZ syndicate were formed from the participants. Each of the syndicates started their planning work independently of one another.

[13] Joint Operational Area
[14] Sea Port of Disembarkation
[15] Air Port of Disembarkation
[16] Line of Communication
[17] Military Strategic Transition Point

Finishing the Mission Analysis a briefing was organized with the aim to give some guidance on development of different courses of actions and the contingent strength taking part in the operation has been limited to 3000. After the briefing it became clear, that such a big reduction in presence of multinational forces in the JOA would make the HUMFOR contingent not indispensable in the operation bearing in mind the initial 5000 strong UK joint forces. To resolve the situation the HUMFOR contingent received a specified task that limited the distribution of humanitarian aid for one IDP camp only. This decision was handed over for the UK syndicates as a caveat that has to be made in consideration in their planning process.

By the end of the operational planning process each of the syndicates have made their courses of action that were reported to Brigadier McLeod, commandant of DLSPA in the framework of Course of Action Brief.

LESSONS LEARNED FROM THE EXERCISE MAGLITE 2011/1

After finishing the Exercise MAGLITE an After Action Review (AAR) was held by the director of Military Logistic Institute where the strong and weak sides of the exercise have been identified. Findings are as follows:

- Preparation for the exercise MAGLITE 2013/1 was a model and elicited universal admiration of the British side;
- Cooperation between the University's and the Garrison Brigade's staff was exemplary, without any friction in spite of the serious flood situation in the country;
- IT[18] infrastructure and network provided by our University for the period of the exercise has proved its efficiency and contributed to the success of MAGLITE considerably.
- The infrastructure provided by the National University of Public Service was acceptable bearing in mind the situation, catering service and lodging has to be improved for the next exercise;
- The level of proffesional knowledge of our MSc officers met the requirements but their language skills have to be improved so they can understand the native english speech. In my opinion NATO STANAG 3.3.3.3 should be the entrance level to take part in MAGLITE.
- Map work (electronic, paper) during the exercise has to be improved significantly.
- In the preparational period MSc officers have to spend more time studying the HDF's Staff Sevice Regulation which is a key element for their planning work.
- The cooperation amongst the UK and HU-CZ syndicates was fluent during the whole period of the exercise;
- The cooperation between the UK and HU DS has been improved significantly thanks to the instructors in the UK DS who are fully commited towards Exercise MAGLITE;
- According to my experiences gained in last three years I can state that the British Distaff shares the detailed task with us only in last moment or during the executional period of the exercise which doesn't allow us to prepare our officers, and leads to the described above complications that is why comletely unacceptable for us. If we are taking into consideration the fact that before the exercise the British participants have a one week long preparation within the framework of JLOC, we start the exercise under the unequal conditions and our role is reduced only for an assistance.

[18] Information Technology

CONCLUSION

Multinational Logistic Training Program MAGLITE is playing very important role in the educational process of the National University of Public Service. It prepares the MSc officers to solve logistic planning tasks on operational level and learn the steps and content of the MDMP which role is nowadays fading away during the staff work.

Although there are some missunderstandings and differences of opinion with our British partners, we have to keep on working and developing MAGLITE which has a key position in the educational process of the Military Logistic Institute.

References

[1] Joint Commander's Mission Directive to CJLogFO- Op KREMITY, Exercise paper for MAGLITE 2013/1

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Fábos Róbert
fabos.robert@uni-nke.hu

THE BASIS OF REQUESTING INFORMATION IN MILITARY TRANSPORTATION CONCERNING THE GOODS TO BE TRANSPORTED

Abstract

At present social and economic needs determine transportation needs, and these needs appear quite separately and differently. All transporters and carriers must adapt to these essential differences as the basic requirements of a transportation task are economy, speed, punctuality, and also the minimization or elimination of damage to the goods. These requirements apply not only to civil transportation tasks but also to transportation needs in the Hungarian Army. However, in the 21st century, these needs cannot be fulfilled in any organization, including the Hungarian Army, without an up-to-date information technology system supporting the planning, organization and execution of transportation tasks. The purpose of this study is to summarize the most important data of the database concerning the transported goods. This database can be considered the basis of the IT system supporting road transport.

A jelenkorban a társadalmi és gazdasági igények lényegesen meghatározzák a szállítási igényeket, illetve azok jelentkezése nagyon elkülönülten és különbözőképpen kerülnek felszínre. Ezekhez a lényegi eltérésekhez minden szállítmányozónak és fuvarozónak alkalmazkodnia kell, mivel a fuvarozási feladat végrehajtásának alapkövetelménye a gazdaságosság, gyorsaság és a pontosság, illetve ezek mellett az árukárok minimalizálása. Ezen szempontok nem csak a polgári szállítási feladatokra érvényes, hanem a Magyar Honvédségben jelentkező anyagszállítási igényekre is. Azonban ezen igények kielégítése a XXI. században már nem nélkülözheti egy a kor követelményeinek megfelelő, korszerű szállítási feladatok tervezését, szervezését, végrehajtását támogató informatikai rendszer meglétét minden vállalatnál, szervezetnél, így a Magyar Honvédségnél sem. A cikk célja nem más, mint a közúti szállításokat támogató informatikai rendszer alapjainak tekinthető adatbázis fontosabb – a továbbítandó termékre vonatkozó – információinak összefoglalása.

Keywords: *road transport, product informations, information system, data base ~ közúti szállítás, termék információk, informatikai rendszer, adatbázis*

INTRODUCTION

Strange though it may seem, a transportation task starts when there is an intention in an organization or unit to transport some material, whatever the purpose is. Even at that moment, the person requesting transportation must have information and data necessary to transport the material. The planner of transportation can only obtain this information from that person since this information concerns the goods to be transported and the loading and unloading activity. Data connected to materials largely determine execution since without these data it is quite difficult to organize transportation in an optimal way and minimize adverse effects to goods during carriage and therefore minimize damage to the goods.

Another set of very important information concerns the vehicle of carriage. A transport vehicle basically has three types of capacity concerning the materials to be transported. These are payload, loading volume and loading area. It is important which of the three has to be planned based on the properties of the goods to be carried. Also, in many cases other modes of transport have to be utilized, too, therefore the dimensions of the vehicle can also be important.

A very important information group is data associated with the route, especially if oversized or overweight goods are transported or a transport convoy is involved. Information concerning the driver of the vehicle is important partly for the planning process preceding transport, partly for settling accounts after transport.

Based on the above, the information indispensable for carriage can be grouped as follows:

- Information relating to the transported materials;
- Information relating to the vehicle carrying the materials;
- Information relating to the route, including data of loading, unloading and transfer places;
- Information relating to the personnel executing the transport task.

1. STRESSES AFFECTING THE GOODS [1]

The first step of the planning, organizing process before transport should be the collection of all the information relating to the goods to be transported, if the sender has not done it in the delivery request. Its necessity cannot be questioned. However, before transport it is important to know what stresses the materials are likely to encounter since the materials or their packaging cannot withstand all outside stresses, therefore it can be damaged or it causes damage to the environment. The role of packaging is to protect the goods from its environment and to protect the environment from adverse impact of the goods. The planner and organizer of transport has to know how much the packaging of the goods can withstand the stresses during transport – which may depend on a large number of things including mode of transport – because this information may determine the choice of mode of transport, transport vehicle, loading and fastening tool, etc. (S)he has to have information about the product which helps eliminate adverse effects during transportation.

Stresses occurring during transport can be the following:

1. Mechanical stress:
    a) Static: pressure, aggregate pressure;
    b) Dynamic;
2. Climatic stresses:
    a) Sunshine;
    b) Temperature;
    c) Humidity;

d) Precipitation;
e) Air pressure;
f) Air movement, wind;
g) Air pollution;
h) Various types of radiation.

3. Biological stresses:
   a) Microorganisms,
   b) Insects;
   c) Rodents.
4. Stresses related to humans:
   a) Pilfering;
   b) Faking;

1.1. Mechanical stresses

Mechanical stresses can be divided into two main groups: *static* and *dynamic* stresses. *STATIC* stresses are basically pressures from different directions. The most important and most common of these is the so-called "aggregate pressure", which can be observed in the case of products or unit loads piled on top of one another and is present not only in the case of carriage but also in the case of storage. It is very important to know whether the goods or their packaging can withstand such stress and to what extent.

DYNAMIC stresses primarily occur when the materials move or are moved, which can occur during loading and transport. Such dynamic stresses can be the following:

- shaking, vibrating (caused by the vehicles during loading and transport – its amplitude is low but its frequency is relatively high);
- dropping (occurs relatively frequently during loading and unloading; it can be eliminated if loading/unloading is appropriately mechanized; drop height is the height from which the product can be dropped, in certain cases it is standardised);
- rolling, tipping over (it occurs during loading/unloading or if the goods are not properly fastened; it is important to use packaging that reduces the acceleration of the goods);
- impact (a single stress that occurs in a specific area on the outside surface; usually due to inappropriate handling; cannot be planned beforehand but can be reduced with the proper choice of material);
- collision (happens with two products once or several times; it is common in carriage by rail; it can be eliminated by fastening the goods properly in the vehicle);
- swinging (similar to collision but usually does not come into contact with anything else; its amplitude is relatively high, but its frequency is low).

1.2. Climatic stresses

Climatic stresses are mainly connected to the climate and weather conditions of the transport area. These include the following:

- Sunshine;
- Temperature;
- Humidity;
- Precipitation;
- Air pressure;
- Air movement;
- Air pollution;
- Various types of radiation.

All of the above list have to be taken into consideration for the time of transport, which is not always easy because weather conditions can usually not be predicted precisely. However, it definitely has to be dealt with since various forms of precipitation can cause different kinds of damage, and in transport by sea salty vapours can corrode the containers.

1.3. Biological stress

Biological stresses include all stresses caused in the transported goods by living organisms except humans. These organisms can be visible (noticeable, perceptible), and can be invisible to the human eye (microorganisms). The first group includes various rodents, and insects, which may carry germs, and can also physically damage the product or its packaging.

The second group includes bacteria, fungi and viruses, which can also damage both the product and its packaging. While it is easier to prepare for the damage made by an insect or a rodent because it can be seen, we only learn about the presence of microorganisms if the damage they caused is visible.

1.4. Stresses caused by humans

Stresses caused by humans do not include accidental damage during loading, unloading and transport resulting from accidents or human negligence or mistakes. They include intentional actions which can cause damage to the product or its packaging. The most important and most common of these is pilfering, that is, the intentional changing of the content and amount of the product (reducing the amount of the product). This can be partly avoided by the careful selection of packaging material and tool, and by making the opening of the package complicated.

2. INFORMATION RELATING TO THE TRANSPORTED MATERIAL

Unfortunately, it is not enough to provide the basic information concerning the transported goods, such as their type, amount and some external dimensions. If the sender only provides this information to the planner of transport, the transport job is not executed due to lack of information. Let us consider an example in which chairs have to be carried and only the number of chairs is given. It is also important to know what kind of chairs they are, how they are packaged – if at all – what they are made of, what their dimensions are, etc. Therefore data relating to the goods and materials can also be grouped:

- Information relating to the amount of the material;
- Information relating to the material and name of the product;
- Information relating to the packaging of the goods;
- Information relating to the handling and loading of the goods;
- Information relating to any special properties of the material.

2.1. Information relating to the amount of the material

One of the most important type of information is the amount. However, it is not so easy as it seems at first sight, as it can be given in various units of measure (pieces, ton, box, litre, cubic metre, etc.). The one most characteristic to the transported material has to be selected. Some additional information also has to be given, such as specific gravity or specific volume, etc. This can be important in deciding whether the mass or the volume is the more important criterion for choosing the transport vehicle. Also, giving the whole amount is not always enough, often data relating to the individual items (e.g. kg/piece; kg/l, etc.) may be important as well. It follows from this that the information system has to be able to handle as many different kinds of data as possible. Unit loads also have to be thought of since pallets

containers, boxes, etc. are also often used as a unit of measure, and as units to be carried. In addition, there can be products containing more than one constituent material and the amount of the materials is not the same and all the amounts may have to be given. Let us consider air defence missiles, whose propellant, payload and other structural elements are completely different and special rules have to be observed in transporting them, and the amount of hazardous materials fundamentally determine the planning of their transport. This means that for one type of goods often several designation of materials are necessary along with the accurate amounts, and also their handling in a database. [2]

2.2. Information relating to the material and designation of the product

Hazardous materials whose amount is important information in planning transport have been mentioned above. However, another piece of important information is the accurate designation of the hazardous material(s) or goods. The rule mentioned above concerning the transport of hazardous materials on road classifies these materials and contains regulations concerning them. If the product is not designated accurately, the wrong rules may be applied, which can lead to disaster.

But proper designation is important not only in the case of materials requiring special handling but also in the case of common, often transported materials. A codification process was started in the Hungarian Army a few years ago with the aim of each product being referred to by only a code. Unfortunately, it has been a partial success only. Unfortunately there are records in which two, essentially the same products are listed under two or even more codes. Not to mention cases when the name only partially identifies the equipment, if at all. How much easier it would be to collect the necessary data to plan transport if the inventories contained only one code and name for a specific product and its composition. The planner of carriage could immediately access the relevant data and properties, and his/her work would be much easier and planning time would be reduced.

The accurate designation of the material of the transported product is also important because of the above-mentioned stresses. In every mode of transport there are stresses adversely affecting the products, only their effect and extent may be different. The damage they cause largely depends on the material of the product, the packaging, the mode of transport, and the circumstances of transport (e.g. part of day, season, distance, etc.). If the transported goods are not defined accurately, the wrong type of transport vehicle may be selected and the goods may suffer damage. A simple example is “furniture”. “Furniture” is an umbrella term including many types. However, the material of the furniture is very important. In dry and sunny weather it does not make any difference but wooden furniture may not withstand rainy autumn weather without damage. On the other hand, plastic furniture may get deformed in strong and prolonged sunshine. [3]

2.3. Information related to the packaging of the material

Transported goods are usually packaged is some form. The form, appropriateness and quality of packaging is important information from the point of view of transport. Loading/unloading and the technology applicable in transport are fundamentally determined by the packaging material and the packaging tool. However, it is also important information if the transported material does not have packaging at all and has to be transported in a tank for example.

The material of the packaging is related to the expected transport stresses, the type of the cargo compartment of the transport vehicle and the loading device and its grabbing mechanism. Paper packaging can withstand far less numerous and intense stresses than for example wooden packaging. Also, the material used for packaging can greatly alter the mass, volume and layout of the product on the transport vehicle (for example the products can be

packed on one another). All this information has to be taken into account when determining the necessary capacity of the loading machine and the transport vehicle.

The type of the used or usable packaging device and information relating to it are also important from the point of view of carriage. This does not only include external dimensions but also internal layout (e.g. internal dimensions, number and layout of lashing points, etc.) can be important. Let us take a container, which is one of the most commonly used packaging and unit load device. Containers are typically standardised but various standards are in use. The most common standard is the ISO standard but any company can use its own special container size and also air transport containers (different layout and dimensions) and sea transport containers (resistant to salty vapours) differ from standard road and railway containers. The Hungarian Army also has containers not used anywhere else. In addition, standard containers also have special designs, they can have extra equipment such as an air conditioner, which makes it impossible to use standard loading equipment. Then there are standard but still special designs which are only practical to use with the loading and transport equipment designed specifically for them (e.g. ACTS technology). [4], [5]

2.4. Information relating to the handling and loading of the goods

Information relating to the handling of the transported goods does not only include data mentioned earlier (packaging, material, etc.) but information relating to the necessary activities accompanying the execution of the elements of the transport process. Here information is necessary which will also appear on the packaging of the goods. Such can be information and data relating to the fragility, handling position (e.g. can only be carried in an upright position) or precipitation sensitivity of the goods or whether they can be piled on top of each other and to what extent.

Information concerning handling and the design of the packaging device greatly affect the loadability and the design of the loading device and its grabbing device. It can also be important to know the grabbing points of the product, their design and strength. The same applies to the tie down possibilities of the product, and the type, amount and strength of the applicable lashing devices. In many cases the lashing of the cargo also has to be planned and organized and without the above-mentioned information, it will be difficult and inaccurate. Inappropriate lashing of the cargo is a danger to not only the product and the transport and loading vehicle but to people and other vehicles in its environment. Not to mention the time loss caused by badly planned and organized loading and lashing, especially if a large amount of cargo has to be transported in a short time.

2.5. Information relating to the special properties of the material

Cargo can have very many properties, some of which are the same for almost all types of cargo but there are some which are applicable for a certain type or device or material. Such are live animals, oversized cargo or custom made devices and products which cannot be transported with the usual methods or technologies. In some respect hazardous materials belong here, too, but their properties and the rules governing their transport have already been laid down (ADR) and these rules have to be adhered to. Special properties definitely have to be known to transport a given product.

The Hungarian Army does not transport live animals any more but in civilian life it often happens. The transport technology used largely depends on the properties of the given animal. For example there can be great differences between two horses in size (pony or draft horse) but also in value (draft horse or racehorse). Transportation of each kind requires different organization. The same can apply to the carriage of live fish. Each kind of fish has a minimal oxygen and space requirement. Transporting carp cannot be done in the same way as transporting trout.

Oversized and overweight cargo exceed the size or mass included in regulation. These devices are usually custom made and/or only a few of them are transported. The Hungarian Army has a relatively large number of such devices (e.g. tanks) but they are not carried daily. Some equipment always exceeds allowed size limits but some can be modified to be within the limits by for example dismantling certain parts. In the latter case the organizer of transport has to know about this possibility because this information can greatly reduce transport costs. [6], [7]

SUMMARY

Planners of road transport need a great deal of information to be able to plan execution as accurately as possible. In all cases this information is primarily related to the transported cargo, its properties will determine the other elements of the transport process. In order for these data to be present it is necessary to have a database, which is important from the point of view of the transportation process. Such a database must contain as much information as possible about the transported materials, equipment and products. It is not easy to determine the necessary data as more information is needed than just the amount and the outside dimensions – far deeper professional knowledge is necessary to determine and collect all essential data.

References

[1] Györgyi Adrienn – Tiefbrunner Anna – Varga József: Csomagolástervezés (Papír Press Egyesülés, Budapest, 1999) ISBN: 963 858662 3 0

[2] (38/2009. (VIII. 7.) KHEM rendelet a Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Európai Megállapodás (ADR) „A" és „B" Mellékletének belföldi alkalmazásáról

[3] Dr. Hirkó Bálint: Gépjármű üzemszervezés II. – Közúti áruszállítási technológiák (Tankönyvkiadó, Budapest, 1984.)

[4] Dr. Mátyus János – Szabó Lajos: Áruszállítási technológiák I. (SZIE egyetemi jegyzet, Győr, 1996.)

[5] Dr. Mátyus János – Szabó Lajos: Áruszállítási technológiák II. (SZIE egyetemi jegyzet, Győr, 1996.)

[6] 6/1990. (IV. 12.) KöHÉM rendelet a közúti járművek forgalomba helyezésének és forgalomban tartásának műszaki feltételeiről

[7] 13/2010. (X. 5.) NFM rendelet a meghatározott össztömeget, tengelyterhelést és méretet meghaladó járművek közlekedéséről

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Fábos Róbert
fabos.robert@uni-nke.hu

THE APPLICABILITY IN MILITARY ROAD TRANSPORT OF INDICATORS CHARACTERISTIC TO ROAD CARGO TRANSPORT FLEETS

Abstract

Road cargo transport is not a manufacturing activity but a service. However, a service can also have measurable performance but in a different form. To measure this performance and to assess cargo transport activity a system of indicators were created. In civilian life this system is commonly used by carrier companies to analyse their activity. The cargo transport activity of the Hungarian Army has many similarities to civilian cargo transport. As a result, the method of analysis used there can be well utilized to analyse military transport. The purpose of this study is to examine whether the indicators used in civilian life for vehicles of road cargo transport can be used for military vehicles of road cargo transport. The utilization of capacities and the analysis of carriage performance are not discussed in this study.

A közúti áruszállítás nem termelő tevékenység, hanem a szolgáltatások körébe tartozó tevékenység. Azonban egy szolgáltatásnak is létezhet mérhető teljesítménye, csak más formában. Ennek a teljesítménynek a mérésére, illetve az árufuvarozási tevékenység vizsgálatára alkottak meg egy mutatószám rendszert. Ezt a rendszert a polgári életben előszeretettel alkalmazzák a fuvarozó vállalatuk a tevékenységük elemzésére. A Magyar Honvédség anyagszállítási tevékenysége nagymértékű azonosságot mutat a polgári árufuvarozással. Ennek megfelelően az ott alkalmazott elemzési módszer jól alkalmazható a katonai szállítások vizsgálatára. A cikk célja nem más, mint megvizsgálni a közúti árufuvarozó tevékenységet végző tehergépjárművekre, illetve azok szállítási lehetőségeire a polgári életben alkalmazott mutatószámok alkalmasak-e a katonai anyagszállítási feladatokat elvégző járművekre is. A kapacitások kihasználására és a szállítási teljesítmények elemzésére vonatkozóak jelen írásban nem kerülnek ismertetésre.

Keywords: *road transport, vehicle capacity, capacity utilization ~ közúti szállítás, jármű kapacitás, kapacitás kihasználás*

INTRODUCTION

Carriage can be properly planned and the execution analysed with the help of indicators. Therefore the concept of indicators can be formulated as follows:

"The precisely defined conceptual and numerical form of the relationships of the state, or development of technical and economic activities."[1]

Panning uses the system of indicators – precalculation – since vehicles can be commanded based on how much capacity is available. It can also be used to modify the capacities of the vehicle fleet. A modification of capacities can be reduction, increase or change as sometimes the total capacity does not change but the type of cargo that can be transported is changed or instead of using fewer higher capacity transport vehicles it is reasonable to use more smaller capacity vehicles, as the circumstances of transport have changed. It can also be useful in deciding whether to "repair or buy a new one".

Even during the execution of high-volume carriage tasks – intermediate calculation – it can be reasonable to use indicators to examine the tasks executed so far and to better approximate an optimal utilization of capacity.

After the transport processes have finished – postcalculation – the same formulae can be used as it is also important to know how well the available transport vehicle fleet was utilized. The planner of transportation can make good use of this information to plan the next job better.

A "group" of indicators can only be effective if the individual indicators function as a "system". It is only possible is there is a relationship between the indicators, they can be calculated from one another and they affect each other. Also, the system of indicators is only suitable to analyse road cargo transport if:

- can reflect the transportation process as a whole and in detail;
- can reveal all the major factors affecting the transport process and allows for detailed examination;
- allows for the monitoring of both quantitative and qualitative changes.

In road cargo transportation – as in the case of many other areas – there are different kinds of indicators:

- *Quantitative* indicators: they describe the carriage performance as the amount of production, that is, they are directly measurable and calculable and not derived (e.g.: total mileage, total transported cargo, etc.);
- *Qualitative* indicators: they provide information about the quality of the transport process, that is, they cannot be measured directly, but can be derived from qualitative indicators (e.g.: run utilization factor, average speed, etc.)
- *Development* indicators: they do not have a unit of measure and show the ratio of the same indicators in usually subsequent periods. [1]

1. INDICATORS DESCRIBING ROAD CARGO TRANSPORT VEHICLES

Perhaps the most important step in every process is to define the given time period. It is important whether a month, quarter, half year or whole year is examined. It can perhaps be best seen if development indicators are calculated. It does not make sense to relate a value describing half a year to a value describing a whole year. Therefore the *number of calendar days of the given period (D)* is important, whose unit of measure is: [day]. It is possible to

[1] [1] 138. o.

measure it in [hours], which gives a more precise value in some cases but in other cases it is more useful to measure the time in days.

An important initial indicator is *Vehicle days (N)*, which shows the number of days the cargo transport vehicles spend in service in the investigated period.

$$N = \sum Ni \text{ , [day]}$$

where Ni is the vehicle day of the ith vehicle.

A vehicle day can be divided into *Operational vehicle days (Nü)* and *Repair vehicle days (Nj)*. Nü shows that on these days the vehicle was operational, able to carry out the task. Nj shows that on these days the vehicle was not operational, and could carry out any task.

$$N = Nü + Nj = \sum Nüi + \sum Nji \text{ [day]}$$

Both operational and repair vehicle days can be further divided according to what the vehicle was doing when it was operational and also why it could not work when it could not. As a result operational vehicle days can be further divided into *productive vehicle days (Nt)*, *taskless vehicle days (Nfh)*, and *driverless vehicle days (Ngh)*.

$$Nü = Nt + Nfh + Ngh = \sum Nti + \sum Nfhi + \sum Nghi \text{ [day]}$$

Productive vehicle days indicates the number of days the vehicles were carrying out actual transporting tasks regardless of how many tasks they executed in one day.

Taskless vehicle days shows the number of days the vehicles stood idle because there were no transporting tasks to execute.

Driverless vehicle days indicates the number of days vehicles stood idle because there were no available drivers to drive them. It is important to mention that in some literature2 these days are not classified like this because the authors say that a vehicle is useless without a driver. This thinking is false because if there is no task, the vehicle is also useless. Also, if there is no task or driver the vehicle is still operational and is ready to be used whenever a transport request arrives and a driver can be found to drive it. An operational vehicle day – as its name indicates – shows that the vehicle is operational and ready to use, while a repair vehicle day indicates that the vehicle is not operational, it needs repair or servicing, it cannot carry out transport tasks for some reason.

Similarly to operational vehicle days, repair vehicle days can also be further divided into *Actual repair vehicle days (Ntj), Part-shortage vehicle days (Nah) and Non-serviceable vehicle days (Nnf).*

$$Nj = Ntj + Nah + Nnf = \sum Ntji + \sum Nahi + \sum Nnfi \text{ [day]}$$

Actual repair vehicle days show the number of days the vehicle fleet was actually being repaired in the given period.

Part-shortage vehicle days indicate the number of days the vehicle fleet was waiting for parts. The days when the vehicles were not actually being repaired for some reason also belong here. (e.g. no mechanic, no repairing machine, etc.).

[2] [3], [4], [5]

Non-serviceable vehicle days show the number of days the vehicles could not work even though they were not out of order. Some possible reasons:

- the vehicle does not have an MOT certificate;
- lacks a compulsory accessory required by the Highway Code;
- the repairs have been carried out but the vehicle has not been given back to the transport fleet;
- biologically or chemically contaminated vehicle waiting for cleaning;
- vehicles in long-term storage;
- etc. [2], [3]

From the time periods detailed above various factors and indicators can be calculated, which can characterize the vehicle fleet. These can show the utilization and the conditions of operation (e.g. repair efficiency, operational safety, etc.).

It is reasonable to keep a vehicle in the fleet or the fleet is reasonable to maintain if the vehicles can carry out tasks as much as possible. This is shown by the *Operationality factor (nü)*, which shows the ratio of operational vehicle days to all days in service.

$$n_{ü} = \frac{N_{ü}}{N} \quad [\,-\,]$$

Obviously, it follows from the above that a vehicle or a fleet that spends too much time being repaired is not reasonable to maintain. The *Repair factor (nj)* shows the ratio of repair vehicle days to all days in service.

$$n_j = \frac{N_j}{N} \quad [\,-\,];$$

$$nü + nj = 1$$

It is worth maintaining a vehicle or a fleet if they "produce", that is, carry out transport tasks as often as possible. Although the vehicles of the Hungarian Army do not do "production" work, it is true that it is not worth maintaining transport vehicles if they are rarely used. There are cases, however, when the vehicles do little actual work but they are still needed to maintain capabilities (e.g. water carrying tanker trucks, etc.).

This leads us to the *production factor (nt)*, which indicates the ratio of productive vehicle days to all days in service.

$$n_t = \frac{N_t}{N} \quad [\,-\,];$$

Within this utilization indicator the extent operational vehicles were actually doing "work" in the given period can be important. This is shown by *Operational fleet utilization factor (na)*, which does not include the whole fleet, only the operational vehicles. [1], [3]

$$n_a = \frac{N_t}{N_{ü}} = \frac{N * n_t}{N * n_{ü}} = \frac{n_t}{n_{ü}} \quad [\,-\,];$$

In addition to the above factors, the number of transport vehicles in the fleet can also be an important indicator. The first such indicator is the *Average fleet (G)*, which shows how many vehicles were in the fleet on average in the given period.

$$G = \frac{N}{D} \text{ [vehicle];}$$

Similarly to vehicle days, it is reasonable to examine the average fleet in detail, too, since not all vehicles in the fleet can carry out transport tasks. The *Average operational fleet indicator (Gü)* shows the average number of vehicles a day that could be used for transport tasks.

$$G_{ü} = G * n_{ü} = \frac{N}{D} * \frac{N_{ü}}{N} = \frac{N_{ü}}{N} \text{ [vehicle];}$$

The average number of vehicles that do not work are called *Average repair fleet (Gj).*

$$G_j = G * n_j = \frac{N}{D} * \frac{N_j}{N} = \frac{N_j}{N} \text{ [vehicle];}$$

Gü + Gj = G

However, from the point of view of "production", that is, carriage performance, these two indicators are not enough. It is also important to know how many vehicles carried out actual transportation tasks on the days of the given period. This is shown by *Average production fleet (Gt).*

$$G_t = G * n_t = \frac{N}{D} * \frac{N_t}{N} = \frac{N_t}{N} \text{ [vehicle];}$$

It is not important in civilian life but in the case of military transport convoys it may be important to see to what extent the table of organization of the given unit is filled with transport vehicles. This is expressed by the *Fleet fullness factor (nG)*. [3], [4]

$$n_G = \frac{G}{G_á} \text{ [-];}$$

where: Gá – the number of vehicles fixed (defined) in the table of organization of the military transport fleet;

INDICATORS CHARACTERIZING THE TRANSPORT CAPACITY OF CIVILIAN ROAD TRANSPORT VEHICLES

The planners of transport tasks can only plan the transport job properly if they know the relevant properties of all transport vehicles (e.g. capacity, ability to carry cargo off-road, etc.) and also their special equipment (e.g. loading mechanism and its capacity, etc).

The best known capacity of a transport vehicle is its *Payload capacity (gi)* [t], which denotes the maximum amount of mass the vehicle can carry. Using this information the *Average payload of vehicles* can be calculated ($\overline{g}$) [t] using the payloads of the vehicles and the days of the given period.

$$\overline{g} = \frac{\sum g_i * G_i}{G} \quad [t]$$

where: Gi – the average number of the ith type of vehicle on the days of the given period
gi – the payload of the ith type of vehicle [t]

Payload is not the only quantity that can characterize the transport ability of a given vehicle since there are cases when the volume of the carried material is relevant, rather than its weight. Such materials are liquids, dusts or very large products. In such cases *Volume capacity (hi)* [m3] is used instead of payload capacity. Volume capacity denotes the maximum volume of cargo a vehicle can carry. Similarly to average payload, the *Average volume capacity of vehicles* can be calculated ($\overline{h}$) [m3].

$$\overline{h} = \frac{\sum h_i * G_i}{G} \quad [m3]$$

The third capacity of road cargo transport vehicles – although it is usually not considered – is *Area capacity (l)* [m2]. This is important for example if the transported goods cannot packed on top of one another for some reason. In the case of military vehicles it more often comes up since in civilian life the platform size of transport vehicles matches the size of unit load devices (e.g. pallet), the platform size of military transport vehicles usually do not, owing to special requirements (e.g. cross-country ability, special bodies, etc.). Similarly to payload and volume capacity, the *Average area capacity of vehicles (* $\overline{l}$ *)* [m2] can be calculated.

$$\overline{l} = \frac{\sum l_i * G_i}{G} \quad [m2]$$

A military peculiarity is that cargo transport vehicles sometimes (e.g. military exercises, at the times of floods, etc.) carry people, too. As a result the *Passenger capacity (b)* [persons] of trucks and the *Average passenger capacity of vehicles* may be needed ($\overline{b}$) [persons]. [2], [5]

$$\overline{b} = \frac{\sum b_i * G_i}{G} \quad [persons]$$

Using these capacities the total amount transportable (movable) by the fleet in the given period can be calculated. This calculation is valid if we assume that each vehicle executes only one transport task each day. If individual vehicles (types or categories) can carry out more than one transport task a day, the number of tasks that can be executed in one day has to be used in the calculation.

Ton day:

$$S_g = \Sigma g_i * N_i = \overline{g} * N \quad [t],$$

which shows the weight that the whole fleet (regardless whether the vehicles were operational or not) could have transported in the given period.

Volume day:

$$S_h = \Sigma h_i * N_i = \overline{h} * N \quad \text{[m3]},$$

which shows the volume that the transport fleet could have transported.

Area day:

$$S_l = \Sigma l_i * N_i = \overline{l} * N \quad \text{[m2]},$$

which shows the total of transport area available including all the vehicles in the given period.

Passenger day:

$$S_b = \Sigma b_i * N_i = \overline{b} * N \quad \text{[persons]},$$

which shows the number of passengers the fleet could have carried.

Besides the transport capacity related to the given period, perhaps the capacity indicators concerning the individual days of the given period are more important and also easier to handle.

Average fleet payload capacity:

$$C_g = \frac{S_g}{D} = \overline{g} * G \quad \text{[t/day]};$$

it shows the weight that the whole fleet (regardless whether the vehicles were operational or not) could have transported on the days of the given period.

Average fleet volume capacity:

$$C_h = \frac{S_h}{D} = \overline{h} * G \quad \text{[m3/day]};$$

it shows the volume the fleet could have transported daily.

Average fleet area capacity:

$$C_l = \frac{S_l}{D} = \overline{l} * G \quad \text{[m2/day]};$$

it shows the total of the cargo area available for the transport fleet on the days of the given period.

Average fleet passenger capacity:

$$C_b = \frac{S_b}{D} = \overline{b} * G \quad \text{[persons/day]};$$

it shows the number of persons the whole fleet could have carried on the days of the given period. [1], [2], [6]

SUMMARY

It can be seen from the above that the system of indicators used in civilian life can be fitted well to military transport tasks. However, special circumstances and unusual tasks require indicators which have no or very little role in civilian road transport. A properly functioning system which is fitted to the given activity greatly facilitates the work of the planner and organizer and provides considerable help to change and plan the capacity of the fleet. It poses great difficulty that at present these indicators exist only in printed form in the Hungarian Army and in the different units they are stored in different places. This means there is no unified and detailed database on the transport capacity of the Hungarian Army accessible for all professionals. For such a system to be created a unified and new approach is necessary, because without it unification and standardization is not possible even in printed form. It would also be very important to include the above indicators in the database of an army-wide information system supporting road transport, since in order to plan and organize transport, accurate, detailed and up-to-date information concerning the transport vehicles and transport possibilities is always necessary.

References

[1] Dr. Hirkó Bálint: Gépjármű üzemszervezés I. – Áruszállítási üzemtan (Tankönyvkiadó, Budapest, 1980);

[2] Illés Béla – Németh János: Közúti áruszállítás rugalmassági-, illetve érzékenységi vizsgálata – Logisztikai antológia 2010. 135-148. p. (Universitas-Győr Nonprofit Kft., Győr, 2010) ISBN 978-963-9505-41-4

[3] Boros János: Katonai közúti szállítások szervezése és végrehajtása I. rész – Katonai gépkocsi szállítások szervezése és végrehajtása (ZMKA, tankönyv, Budapest, 1980)

[4] Dr. habil. Réger Béla: Szállításszervezés alapjai (ZMNE, egyetemi jegyzet, Budapest, 2007.)

[5] Dr. habil. Réger Béla: Közúti szállítási feladatok szervezése (ZMNE, egyetemi jegyzet, Budapest, 2008.)

[6] Dr. Prileszky István – Csonka Béla – Fülöp Gábor: Gépjármű-üzemszervezéstan – Gyakorlati jegyzet (Tankönyvkiadó, Budapest, 1990);

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Bonnyai Tünde
bonnyai.tunde@gmail.com

A LAKOSSÁGFELKÉSZÍTÉS LEHETSÉGES MÓDSZERTANA A LÉTFONTOSSÁGÚ RENDSZEREK ÉS LÉTESÍTMÉNYEK VÉDELMÉNEK RENDSZERÉBEN

Absztrakt

Nehéz megállapítani, hogy mire van szüksége a XXI. század hétköznapi állampolgárának a saját biztonsága szempontjából. Sokan vélekednek úgy, hogy csak a közbiztonság, a vagyonbiztonság és az otthon biztonsága meghatározó számukra, de nem gondolnak bele, hogy milyen komplex rendszerekkel állnak kapcsolatban „az otthoni négy fal között". A hatóságoknak kiemelt feladata a lakosságfelkészítés akár közrendről, közlekedési kultúráról, egészséges életmódról, katasztrófavédelemről, vagy honvédelemről van szó. A következő cikk azt vizsgálja, hogy mindemellett milyen súlya van a létfontosságú rendszerek és létesítmények védelmével kapcsolatos információknak és hogyan valósítható meg ezekre való tekintettel a célirányos lakosságfelkészítés.

It is difficult to identify what are citizens' needs in the 21th Century from a security point of view. Many people believe that only public safety, security of property and their own security is important, and do not think about how complex and multiple systems are they continuously connected to, within "the four walls of their home". Authorities have a priority task about preparing the public even for public order, traffic culture, healthy living, disaster management and national defense. The following study analyses what kind of weight are carrying information related to critical infrastructure protection, and how can be implemented the purposive preparing of public, taking into consideration all of above.

Kulcsszavak: *kritikus infrastruktúra, létfontosságú rendszerek és létesítmények, lakosságfelkészítés ~ critical infrastructure, preparing public, security of information*

„A valós információ létfontosságú,
a téves információ sajnálatos és káros,
de a jól irányzott hamis információ halálos.”
Frederick Forsyth

1. AZ INFORMÁCIÓHOZ VALÓ JOG

Napjaink egyik legmeghatározóbb eleme a média, az információ-szolgáltatási tevékenység, amely a XX. század végére gyakorlatilag a negyedik hatalmi ággá nőtte ki magát. A Montesquieu szerinti hatalommegosztás elve alapján megkülönböztetett, a demokratikus államberendezkedés alapját jelentő hármas tagolás (törvényhozói hatalom, végrehajtói hatalom, igazságszolgáltatás) napjainkban kiegészül a sajtószabadságból eredeztetett információs hatalommal. A klasszikus idézet szerint az *„információ hatalom, ha jól használod győzelem”*, ugyanakkor az információáramlás megfelelő működése/működtetése nem csupán a versengésben (politikai, gazdasági, hadászati stb. területen) biztosíthat fölényt, hanem kifejezetten egy-egy felkészülési folyamat során is előnyt jelent.

Mindezzel párhuzamosan az információ átadására szolgáló technológiai eszközrendszer és módszertan is folyamatosan fejlődik, amelynek köszönhetően a XXI. század korai szakaszát az információ (más nézetek szerint a média) korszakának kezdeteként is kezelhetjük. Ebben a korszakban keresi folyamatos továbbfejlődési lehetőségeit az információs társadalom[1], amelyben az információ felértékelődött, fogyasztási és termelési árucikké vált, amely mérhető értékkel bír, vizsgálható és kutatható, értékesíthető és nem utolsósorban manipulálható egyaránt [2].

A modern társadalmakban az információhoz való jog mindenkit alapjogként illet meg, amelyet az európai uniós normatívák, a nemzeti jogrendszerek az alapvető jogok közé sorolnak.

1. 1. Az információ jelentősége

Az információ – tartalmi kereteinek széleskörű jellegéből fakadóan – nehezen definiálható fogalom, vagy fogalomrendszer. Meghatározása nagymértékben függ a vizsgálat különböző aspektusaitól:

- elemezhető például a gazdasági élet szempontjából, amely esetben olyan adathalmazt jelent, amely a döntés-előkészítési folyamat részeként, egyes döntések meghozatalához szükséges,
- vizsgálható akár katonai nézőpontból, ahol a tervezési és reagálási tevékenység előkészítéséhez nélkülözhetetlen adatok összességét jelentheti, de
- tanulmányozható lakosságfelkészítési szemszögből is, amikor a rendelkezésre bocsátott adatok, ismeretek kifejezetten megelőzési és túlélési célokat szolgálnak.

Fontos megállapítani, hogy az információ és az információ áramlása – tartalmától és jellegétől függően – hatással lehet globális folyamatokra (pl. piaci hírek hatása a tőzsdére), fejlődési irányokra (pl. felfedezések közzététele), a fenntarthatóságra (pl. fogyasztói magatartás változásai), a biztonságra (pl. védelmi képességek nyilvánosságra hozatala), vagy a működőképességre (pl. üzemeltetési technológiák megosztása) egyaránt. Mindezek alapján azonban rendkívüli jelentőséggel bír az információ áramlás biztosítása, a racionális információ-megosztás elve, amely feltételezi az információ célszerű és közhasznú továbbítását.

[1] Az információs társadalmak egyszerűen olyan társadalmak, amelyek mára komplex elektronikus információhálózatoktól függnek és erőforrásaik nagy részét információs és kommunikációs tevékenységre fordítják [1] p. 112.

Amennyiben az egyén szempontjából vizsgáljuk az információ tartalmát és jellegét, érdemes az Oxford Értelmező-szótár szerinti definíciót alkalmazni. E szerint minden adat olyan nyersanyagnak tekinthető, amelynek feldolgozásával-értelmezésével információ jön létre, amelyből a meglévő emberi tapasztalatok és képességek révén tudás lesz [3]. Ez alapján az a hír, amelyet nem tudunk értelmezni, nem tekinthető információnak, mert nem hordoz számunkra jelentéstartalmat. Az értelmezésnek lehetnek nyelvi, vagy intellektusbeli korlátai, ugyanakkor nagyon fontos az érthetőség és a közérthetőség, valamint a valódi tartalom biztosítása, tekintettel arra, hogy a felesleges, értelmezhetetlen információ semleges, de akár káros is lehet a befogadóra, vagy közvetetten a kibocsátóra egyaránt.

1. 2. Az információ hiányának lehetséges következményei

A vizsgált terület szempontjából a történelemben bekövetkezett katasztrófa jellegű események kapcsán mutatom be az információ átadásának, a felkészülésnek és a felkészítésnek jelentőségét. Mógor Judit PhD értekezésének egyik fejezete a lakosság tájékoztatásának szükségességét, az információáramlás jelentőségét is vizsgálja. A bhopali katasztrófa[2] tényszerű bemutatásával láthatóvá váltak azok az alapvető hiányosságok, amelyek a megelőző időszaki információáramlás – felkészítés keretében történő – biztosításával, csökkenthették volna a következmények súlyosságát. A veszélyeztetett lakosság előzetes felkészítése (=passzív információ átadás) nem volt biztosított, a pánikhangulat megakadályozására a riasztó szirénák elindítására (=aktív információ átadás) nem került sor, az alapvető magatartási szabályok azonnali közlését (=aktív információ átadás) elmulasztották az illetékes hatóságok. A következő táblázat olyan baleseteket sorol fel, amelyek esetében az előre történő tájékoztatással, a szükséges és elégséges információ (=tudás) biztosításával valószínűleg csökkenthető lett volna az áldozatok száma, a kár mértéke.

IDŐPONT	HELYSZÍN	ESEMÉNY	ÁLDOZATOK SZÁMA
1990. július	Szaúd-Arábia	Zarándoklat során egy alagútban meghibásodott a szellőztető rendszer.	~ 1400 fő
2006. augusztus	Magyarország	Az ünnepi tűzijáték közben szupercellás zivatar érte el a fővárost.	5 fő
2011. január	Magyarország	Egy szórakozóhelyen a zsúfoltság, illetve a biztonsági szabályok be nem tartása.	3 fő
2013. február	Oroszország	Meteor-becsapódás következtében jelentős – földrengés által okozott épületkárokhoz hasonló – károk keletkeztek	~ 500 sérült

1. ábra. Az információ hiánya által súlyos következményekkel járó események (Szerk.: szerző)

Nem kell azonban tragédiának történnie ahhoz, hogy az információ hiánya jelentős problémákat okozzon. Napjainkban egyre több olyan természeti, vagy technológiai eredetű eseményt szenvedünk el, amelyek a mindennapi életünk rendszerét, folyamatosságát biztosító alapvető szolgáltatásokat lehetetlenítik el. A modern társadalom számára komoly kihívásokat okozhat egy nagy kiterjedésű, több napon keresztül elhúzódó áramszünet, amely megbéníthatja az alapvető rendszereket (távhő-, ivóvíz-szolgáltatás, szennyvíz-elvezetés,

[2] A katasztrófa 1984. december 3-án a reggeli órákban következett be Bhopalban (India), ahol a Union Carbide rovarirtó szereket gyártó leányvállalata baleset következtében mintegy 40 tonna metil-izocianát gázt bocsátott ki, közel 3000 ember azonnali, és 15 000–20 000 ember későbbi halálát okozva. A mérgező gáz irritációs tünetekkel, légúti elzáródás érzésével, vagy köhögő görccsel jár, amelynek forrását nem ismerték és a tanúsítandó magatartásformákkal (pl. ablak bezárása, szükség-légzésvédő eszköz alkalmazása) sem voltak tisztában [4].

klimatizáció), kellő mennyiségű alternatív áramforrás hiányában hatással lehet a gazdasági működésre, az egészségügyi ellátásra, vagy akár a közlekedésre is. Az ezzel szembeni védekezés elsősorban nem a lakosság feladata, de a túlélés (átvészelés) záloga a megfelelő magatartási formák alkalmazásában rejlik, amelyet a felkészítések során biztosított információk birtokában vagyunk képesek elsajátítani. A következő táblázat néhány olyan eseményt sorol fel, amelyek jelentős hatással voltak a fent említett szolgáltatások működésére:

IDŐPONT - HELYSZÍN	ESEMÉNY	HATÁS	ÉRINTETTEK
2003. augusztus USA (8 állam) és Kanada (1 tartomány)	üzemzavar	villamos-energia ellátási zavarokból fakadó rendszerösszeomlás, közel egy hétig tartó helyreállítási időszak	~ 55 millió fogyasztó
2009. január Magyarország (4 megye)	havazás	leszakadt vezetékek, kidőlt oszlopok, tartós kimaradások a vízszolgáltatásban, három napos áramszünet és távfűtés kiesése	~ 87 ezer fogyasztó
2009. január Dél-kelet Európa	orosz-ukrán gázvita	az Oroszországból Ukrajnán át érkező földgáz mennyisége 2/3-ával csökkent, alternatív beszerzésekre, gáztározók igénybevételére volt szükség	~ 87 ezer fogyasztó
2011. augusztus Karibi-térség és Észak-Amerika keleti partvidéke	Irene hurrikán (II. erősségű trópusi ciklon)	lakhatatlan épületek, járhatatlan utak, több napon keresztül tartó áramszünet	25 áldozat, több ezer fogyasztó
2012. október Karibi-térség és Észak-Amerika keleti partja	Sandy hurrikán (II. erősségű trópusi ciklon)	járhatatlan utak, lakhatatlan épületek, áradások, áramszolgáltatás tartós szünetelése	~ 70 áldozat, ~ 7 millió fogyasztó
2013. március Magyarország	rendkívüli havazás	járhatatlan utak, nagymértékű torlódások, leszakadt vezetékek, kidőlt oszlopok miatt közel egy hétig tartó áramszünet	~ 14 ezer fő útközben, ~ 300 ezer fogyasztó

2. ábra. Egyes szolgáltatásokra jelentős hatást gyakorló események a közelmúltban (Szerk.: szerző)

A fentiek összességében alátámasztják, hogy a megfelelő tartalmú és időben rendelkezésre bocsátott információ kulcsfontosságú lehet bizonyos helyzetek kezelésében és átvészelésében egyaránt. A felsorolt esetek között az emberi viselkedés alapvető jellemzőitől függő, a technológiai fejlettségtől független, valamint természeti eredetű események következtében kialakult helyzetek egyaránt megtalálhatóak, következményük pedig szerteágazó jellegű. Önmagukban és együttesen azt mutatják, hogy a váratlan helyzetek hatásainak súlyossága, az érintettek széles skálán mozgó száma, valamint a szolgáltatások működésére gyakorolt hatás egyre általánosabb jellemzővé válik. A lakosság és a beavatkozó hatóságok szempontjából ezáltal kulcsfontosságúnak tekintendő a hiteles, időszerű, érthető, pontos, szükséges és elégséges információ biztosítása.

1. 3. Az Aarhus-i Egyezménytől az Alaptörvényig

Napjaink nyilvánosságra és információ-szabadságra vonatkozó alapelvei az 1998. június 25-én, Dániában elfogadott Aarhusi Egyezményre (a továbbiakban: Egyezmény) vezethetőek vissza. Az európai környezetvédelmi miniszterek által kezdeményezett Egyezmény a környezeti ügyekkel kapcsolatos információkhoz való hozzáférésről, a nyilvánosság döntéshozatalban történő részvételéről, valamint az igazságszolgáltatáshoz való jog biztosításáról rendelkezik. Ennek értelmében mindenkinek joga van az egészségének és jólétének megfelelő környezetben élni, ugyanakkor mindenkinek kötelessége a környezet aktív védelme és javítása a jelen és a jövő nemzedékei érdekében. Az Európai Közösség környezeti információ nyilvánosságáról szóló 90/313/EGK irányelvét az Egyezmény aláírását követő jogharmonizációs folyamat eredményeként kiadott 2003/4/EK irányelv helyezte hatályon kívül, amely a környezeti információkhoz való nyilvános hozzáférésről szól. E rendelet kötelezettségként állapítja meg a hatóságok részére a rendelkezésükre álló, környezetre vonatkozó információkhoz történő hozzáférés biztosítását, valamint a

tájékoztatásban használatos informatikai és távközlési eszközök fejlődésének követését, fejlesztésük támogatását. Meghatározza, hogy a környezeti információ tárgya lehet például:

- a környezeti tényezők,
- a jogalkotás folyamata, programok, amelyek befolyásolhatják a környezeti elemeket,
- az emberi egészség és biztonság állapota.

Mindezt kiegészíti az Aarhusi Egyezmény rendelkezéseinek alkalmazásáról szóló 1367/2006/EK rendelet, amely a tagállamok szempontjából egyértelműsíti az aktív és passzív tájékoztatás tartalmát, az indoklás nélküli kérelem, a környezeti információ gyűjtésén és terjesztésén alapuló közzététel, valamint a veszélyhelyzeti tájékoztatás módszertanát [5].

Fentieket alapul véve az Egyezmény fontos megállapítása, hogy az információ megtagadását a lehető legszűkebben kell értelmezni, annak mérlegelésekor a közérdeket szükséges előtérbe helyezni. Természetesen az információ megtagadásának olyan speciális esetei, mint a hatósági, a honvédelmi, közbiztonsági, igazságszolgáltatási, kereskedelmi/ipari, vagy a személyes adatokkal kapcsolatos eljárások és folyamatok titkossága, kivételt képeznek a közérdek prioritása alól. Az információ megosztás célja alapvetően tehát a tudatosság kialakítása és a tájékozottság biztosítása, amely hosszú távon a lakossági gondolkodást az öngondoskodás, a felelősségérzet és az önkéntesség irányába mozdíthatja.

Az Egyezményt hazánkban a környezeti ügyekben az információhoz való hozzáférésről, a nyilvánosságnak a döntéshozatalban történő részvételéről és az igazságszolgáltatáshoz való jog biztosításáról szóló, Aarhusban, 1998. június 25-én elfogadott Egyezmény kihirdetéséről szóló 2001. évi LXXXI. törvény hirdette ki. Végrehajtása a környezeti joghoz kapcsolódó jogszabályokba történő integráció, a környezetvédelmi eljárásokban, valamint katasztrófavédelmi engedélyezési szabályokban (pl.: súlyos ipari balesetek elleni védekezés, településrendezés, stb.) való alkalmazás formájában nyilvánul meg. Napjainkban a nyilvánosság elvei minden közfeladatot ellátó szervre vonatkoznak, a magyar jogrendszerben az információszabadság érvényesülésének két alapvető módja figyelhető meg:

- közérdekű adat megismerésére irányuló igény (adatigénylés) → önkéntes, érdeklődésen alapuló információszerzés,
- közérdekű adatokra vonatkozó tájékoztatási kötelezettség (közzététel) → a hatóságok feladata, a legfontosabb információk kérés nélküli rendelkezésre bocsátása, a lakosság alapszintű informáltsága érdekében [6][3].

Mindezeket figyelembe és alapul véve Magyarország Alaptörvénye biztosítja lakossága számára az egészséges környezethez való jogot, amelyet a környezet megóvása jegyében károkozási felelősségvállalással egészít ki [7][4]. Ennek megfelelően került bele a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvénybe az az állampolgári felelősség, amely szerint a katasztrófavédelem nemzeti ügy, az állampolgároknak pedig joguk van:

- megismerni a környezetükben lévő katasztrófaveszélyeztetettséget,
- elsajátítani az alkalmazandó magatartási szabályokat,
- közreműködni a katasztrófák elleni védekezésben – amely egyúttal kötelezettség is.

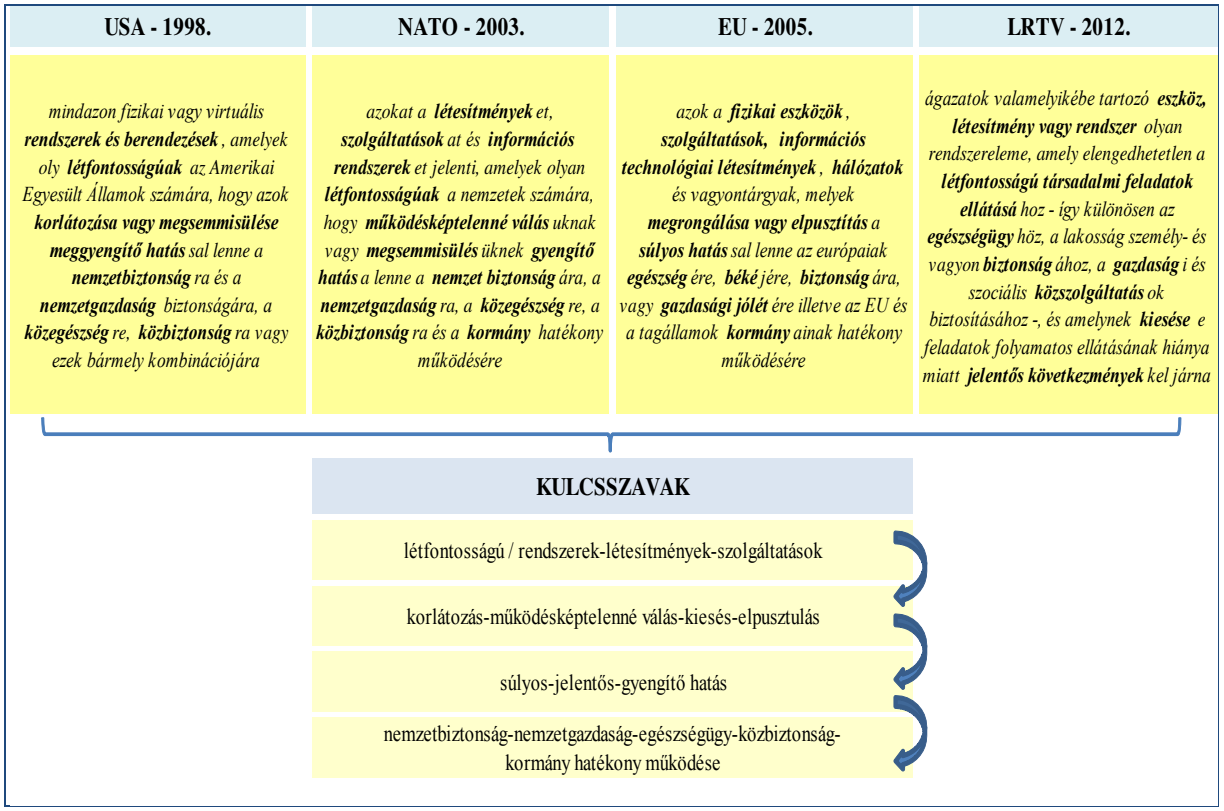
A felelősségek és kötelezettségek teljességét a törvény következő szakasza adja meg, amely rendelkezik arról, hogy a katasztrófák elleni védekezésben érintett szerveknek (ágazati, karitatív és civil) biztosítaniuk kell azokat az információkat a lakosság részére, amelyek a veszélyeztetető hatások megismerését szolgálják [8][5].

[3] [6] III. fejezet
[4] [7] XXI. cikk (1)-(2) bekezdés.
[5] [8] 1. § (1)-(2); 2. § (2) bekezdés.

2. KRITIKUS INFRASTRUKTÚRA VÉDELEM[6] AZ INFORMÁCIÓBIRTOKLÁS SZEMPONTJÁBÓL

2. 1. Sebezhetőség

A kritikus infrastruktúra (ahogy az infrastruktúrák, vagy a szolgáltatások általában) nehezen definiálható fogalom, amely – függetlenül az értelmezését megalkotó ország, vagy szövetség sajátosságaitól – azonos, vagy jelentős mértékben hasonló tulajdonságjegyekkel bír. Az elmúlt évek során kialakított kritikus infrastruktúra védelmi (a továbbiakban: KIV) folyamatok, eljárásrendek igazolják, hogy a potenciálisan veszélyeztetett rendszerek védelmét a Föld minden pontján gyakorlatilag ugyanúgy értelmezik. Ennek szemléltető ábrája alapján nevesíthetőek a kritikus infrastruktúrát (a továbbiakban: KI) meghatározó kulcsszavak:



3. ábra. A KI definíció kulcsszavai (Szerk.: szerző)

A fogalomrendszerből kiindulva meghatározható az infrastruktúrák, illetve konkrétan a KI-k veszélyeztetettségét okozó tényezők, amelyeket a következő csoportok szerint különböztetünk meg:

1) *Ártó szándékú cselekmények* – célirányosan a károkozás és a társadalomra gyakorolt pszichológiai hatás kiváltása érdekében végrehajtott események:

- terrorcselekmény – 2001. USA, 2004. Madrid, 2005. London;
- társadalmi eredetű esemény – 2012. Görögország, 2013. Svédország (zavargások);
- fegyveres konfliktus – 2011 óta Szíria (polgárháború).

[6] Szükségesnek tartom megjegyezni, hogy a nemzetközi irodalom *„kritikus infrastruktúra”* szakterminust használ, míg Magyarországon e kifejezés hivatalos, jogszabályszerű megfogalmazása *„létfontosságú rendszerek és létesítmények”* definícióként elfogadott.

2) *Természeti eredetű események* – nehezen kiszámíthatóak, az elmúlt évtizedben egyre szélsőségesebb formákat öltenek:

- árvíz, belvíz – 2010. Magyarország, 2013. Ausztrália;
- szélsőséges időjárás – 2012. Közép-Európa (szárazság);
- földmozgások – 2012. Észak-Olaszország (földrengés);
- erdőtüzek –2012. Görögország, 2013. New Brunswick (Kanada);
- szökőár – 2004. Indonézia, 2011. Japán;
- hurrikán, tornádó –, 2012. Sandy (Karibi-térség, Észak-Amerika), 2013. Oklahoma;
- rendkívüli hó-helyzet – 2012. Szerbia, 2013. Magyarország.

3) *Ipari eredetű veszélyek* – gondatlan emberi beavatkozás, technológiai hiba, vagy baleset miatt bekövetkező események:

- veszélyes áruszállítási baleset – 2013. Gent-Belgium (vasúti);
- veszélyes ipari létesítmény baleset – 2012. Bad Fallingbostel-Németország (Kraft foods);
- ipari baleset – 2008. Isztambul (tűzijáték-gyár);
- súlyos környezetkárosodás – 2000. Tisza (ciánszennyezés);
- nukleáris baleset – 2011. Fukushima (atomerőmű).

4) *Civilizációs eredetű veszélyek* – az informatikai rendszerektől való függőség miatti és a globális kihívásokból eredő veszélyek:

- informatikai alapú rendszerek – 2003. Észak-Amerika (áramszünet);
- cyber támadások – 2013. The Spamhaus Project (teljes világhálóra hatást gyakorolt);
- egészségügyi járványok – 2010. H1N1 pandémia;
- infrastruktúrák teljesítőképességének kimerülése – ivóvíz készlet csökkenése.

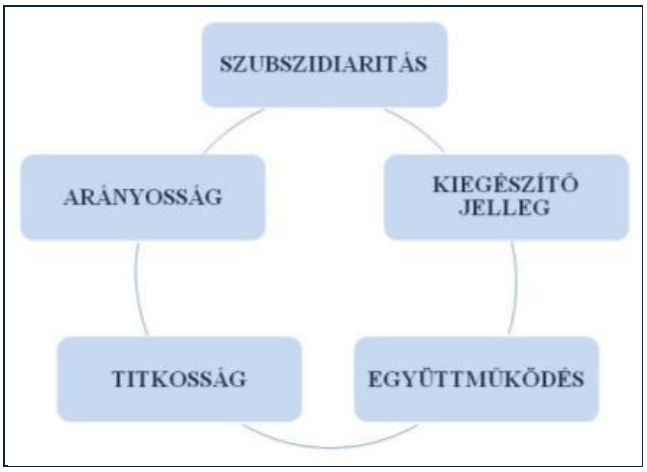
A KI definíciója, speciális működési sajátosságai és veszélyeztetettségi tényezői alapján meghatározható a sebezhetősége is, amelyet különböző mérőszámokkal, leírásokkal lehet nevesíteni. A KIV tekintetében a sebezhetőség definíciója alatt *„az infrastruktúra tervezésének, létrehozásának vagy működésének egyik elemét jellemző sajátosságát”* értjük, *„amely lehetővé teszi az üzemfolytonosság megzavarását, vagy megszüntetését, valamint magába foglalja az egyéb típusú, függőségekből adódó veszélyeket is”* [9] [7]. Figyelembe véve a definíciót általánosságban megállapítható, hogy a lakosságot kiszolgáló létesítmények sebezhetőségi indexe magas, így a védelmüket garantáló biztonsági intézkedések különösen magas prioritást igényelnek [10] [8].

A KI-k azonosítási és kijelölési eljárása során, valamint a védelmi mechanizmusok kialakítása keretében számos olyan adat keletkezik, amely a sebezhetőséget határozza meg, ugyanakkor a sebezhetőség alapján olyan információk is létrehozhatóak, amelyek az adott KI sérülése, kiesése, vagy megsemmisülése esetében az alternatív lehetőségekre, a biztosított szolgáltatás hiányának kezelésére, a következmények során tanúsítandó magatartási szabályokra irányulnak, kifejezetten a fogyasztó (lakosság) szempontjából.

2. 2. A titokvédelem alapelve

A KIV európai uniós programjában öt, egymással szoros összefüggésben álló alapelvet határoztak meg, amelyek napjainkban – a felülvizsgálat keretében is – jelentős mértékben meghatározzák a végrehajtást.

[7] [9] 1. sz. melléklet.
[8] [10] pp. 13-20.



4. ábra. A KIV alapelvei (Szerk.: szerző)

A témakör vizsgálata szempontjából a titkosság elve különösen meghatározó. A KIV uniós programjának kidolgozási fázisában, 2004-ben – nem sokkal a madridi támadásokat követően – az Európai Bizottság közleményt (COM(2004)702 final) adott ki a létfontosságú rendszerek védelme és a terrorizmus elleni küzdelem kapcsolódó pontjairól. A közlemény az európai szintű megelőzés és felkészültség javításának lehetőségeit taglalta, kifejezetten a KI-kat érő terroristatámadásokkal szemben. A KIV program fontos mérföldkövének tekintjük azt az Európai Tanács-ülés által készített megállapítást, amely fentiek alapján kimondta, hogy az európai unió polgárai elvárják, hogy az alapvető emberi jogok biztosítása mellett az EU hatékonyabban kezelje a határokat átlépő problémákat a megelőzés és a következménykezelés terén egyaránt. Mindezek értelmében egyértelművé vált, hogy kiemelt figyelmet kell szentelni a terrorizmus megelőzésére és visszaszorítására, valamint az ezzel kapcsolatos lakossági tájékoztatásra, amely az állampolgárok biztonságérzetét növelheti. Tekinthetjük ezt az első lépésnek afelé, hogy az érintett hatóságok közötti információcsere biztonsági szintjét emeljék és fejlesszék, kifejezetten a hozzáférhetőség biztonságára és a titkosság megőrzésére vonatkozóan.

Ez volt az alapja annak, hogy a KIV európai uniós programjának alapelvei között – a Bizottság állásfoglalása szerint – a titkosság elvére is szükség van ahhoz, hogy a létfontosságú rendszerekkel kapcsolatos információk illetéktelen kézbe kerülése elkerülhető legyen és így csökkenjen a váratlan, súlyos események bekövetkezésének, vagy az infrastruktúrák manipulálásának valószínűsége. Szorosan idetartozik a védelmi tervek uniós és tagállami szinten történő titkosítása is. A titokvédelem különösen prior területnek számít tehát a KIV rendszerében, hiszen egy KI esetében hatványozottan felértékelődik minden információ, amely az infrastruktúra működési képességével és ez által a sebezhetőségével kapcsolatos. A megfelelő szintű védelem kialakítása érdekében az ilyen jellegű adatok hozzáférhetőségét olyan minimális szintre kell csökkenteni, amely a megfelelő és hatékony működést ne akadályozza, de biztosított legyen az illetéktelen betekintéstől.

Ide tartozik azonban a modernkor egyik legnagyobb vívmánya és bizonyos megközelítésből az egyik legkönnyebben sebezhető eleme az infokommunikációs technológiák révén biztosított szolgáltatások kihívása is. A rendszerek törekednek ugyanis a folyamatosan növekvő igények egyre szélesebb körben történő kielégítésére, amely ezzel párhuzamosan fokozatosan sebezhetőbbé teszi az érintett létfontosságú rendszereket (legjobb bizonyítékai ennek a ténynek az elmúlt években fokozatosan megjelenő hackertámadások egyes célpontok, vagy az internet teljes egésze ellen). Az adathalászat, az információszerzési kényszer, vagy az ártó szándék a KI-k vonatkozásában kifejezetten nagy fenyegetettséget hordoznak magukban, amely ellen hatékony és a kor fejlettségi szintjéhez folyamatosan idomulni képes védelmi protokollok alkalmazása szükséges.

3. HAZAI SAJÁTOSSÁGOK ÉS JELLEMZŐK

Hazánk – eleget téve jogharmonizációs kötelezettségének – már 2008-ban megkezdte a KIV európai uniós programjának magyar jogrendbe történő beültetését. Az elmúlt évek tapasztalatai alapján 2011-ben végrehajtott, a hivatásos katasztrófavédelmi szerv rendeltetésének és feladatrendszerének jogi hátterét rendezni hivatott jogszabályi változások eredményeként a KIV feladatrendszere főként a Belügyminisztérium, illetve a BM Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: BM OKF) felelősségi körébe került. Az ágazati érdekeltek aktív közreműködésével és a BM OKF koordinálásával e jogszabályok mentén elfogadásra került a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (a továbbiakban: Lrtv.), majd a részletszabályok kidolgozását követően megjelent a törvény végrehajtási rendeleteként funkcionáló 65/2013. (III. 8.) kormányrendelet (a továbbiakban: Lrtv. vhr.) is.

A lakosságvédelem vonatkozásában a hivatásos katasztrófavédelmi szerv szerepe kiemelkedőnek mondható, tekintettel arra, hogy az Lrtv. vhr. két rendelkezésében is ebben a kontextusban nevesíti:

- a BM OKF-et a közrend, közbiztonság, lakosságvédelem, alkotmányvédelem, nemzetbiztonság, terrorelhárítás szempontjaira tekintettel, a nemzeti létfontosságú rendszerelemmé történő kijelölés vonatkozásában *javaslattevő hatóság*ként jelöli ki [11] [9];
- az üzemeltetői biztonsági tervben meghatározott *rendkívüli esemény* bekövetkezésekor a rendkívüli eseményre való reagálás, a mentés megszervezése, irányítása, továbbá a lakosság tájékoztatása, a károk felmérése, az eredeti állapot lehetőség szerinti visszaállítása a BM OKF *koordinálás*ával történik [11] [10].

Az elmúlt hónapok eseményei (pl.: rendkívüli időjárás miatti, elhúzódó áramszünet Szabolcs-Szatmár-Bereg megyében; a Liszt Ferenc Nemzetközi Repülőtéren történt, váratlan műszaki hiba miatti teljes leállás; a földrengések bekövetkezésének gyakoribb jellege; a hazai és nemzetközi szinten jelentkező, egyre gyakoribb kibertámadások; stb.) alátámasztják a létfontosságú rendszerek és létesítmények védelmének szükségességét. Mindennek elsődleges megnyilvánulása az egyes szolgáltatók és szektorok önálló védelmi mechanizmusainak kialakítása és fejlesztése, de része kell legyen a megelőző időszaki felkészülés hatékonyságának fokozása, az érintett hatóságok és beavatkozó szervezetek felkészítése is. Ugyanakkor meggyőződésem, hogy a lakosság szempontjából is meghatározó feladatot jelent a KI sérülések, kiesések következményeinek kezelése, a lakosságot körülvevő környezetre vonatkozó információk általános ismerete, amelynek ma már a KI-k is részei.

Mindezek alapján a létfontosságú rendszerek és létesítmények működésével, veszélyeztetettségével és kiesésük következményeivel kapcsolatos lakosságfelkészítést indokoltnak tartom, annak végrehajtását a KIV-et meghatározó jogszabályok figyelembe vételével, a jelenleg hatályos lakosságfelkészítésre vonatkozó rendelkezések alapján látom megvalósíthatónak.

3. 1. Az Lrtv. szabályozása és hiátusai

Amennyiben a lakosságvédelemmel kapcsolatos feladatok között a lakosságfelkészítési és lakosságtájékoztatási tevékenységet vizsgáljuk, a hazai KIV jogi szabályozásáról megállapíthatjuk, hogy erre utaló rendelkezést nem tartalmaz. Az Lrtv. és végrehajtási rendelete – igazodva az európai joggyakorlathoz – elsősorban az azonosítási és kijelölési eljárásban érintettek felelősségi körét definiálja. Ebben természetesen fellelhetőek a hatósági

[9] [11] 3.§
[10] [11] 11.§ (6) c.

és üzemeltetői felkészülési feladatok egyaránt, amelyek az egyes létfontosságú rendszerelemek működésének folyamatosságát, a kiesések kedvezőtlen hatásainak csökkentését hivatottak garantálni.

Megállapítható tehát, hogy a felkészülési feladatrendszer három pillérét tekintve kettő (KI-k felkészítése, állami szervek felkészítése) a jogszabályi környezet szerinti előírások alapján valósulhat meg.

5. ábra. A felkészülés elemei (Szerk.: szerző)

Fel kell, hogy merüljön azonban a kérdés, hogy vajon mit jelent a hétköznapok állampolgára számára a KI kifejezés? Mi az első gondolata, amikor meghallja? Egyértelmű lehet-e számára a KIV célkitűzése, megvalósítása és rendszere, ha valójában nem lehetünk biztosak abban, hogy a definíciót jól érzelmezi? Mindebből következik a kérdés: elvárható-e a lakosság részéről a helyes magatartási szabályok alkalmazása olyan esetben, amikor a hétköznapi élet gördülékenységét biztosító valamely szolgáltatás tartósan nem áll rendelkezésre?

Meglátásom szerint a mai társadalomra általánosíthatóak a kényelmes, megszokott, közömbös jelzők – tisztelet a kivételnek –, amely miatt az élet- és vagyonbiztonságot garantálni hivatott szervezetek felelősségi körébe tartozik a figyelemfelkeltés, a megelőzésre nevelés, összességében a felkészítés feladatrendszere. Tekintettel azonban a KI-k szerteágazó típusára, az általuk nyújtott szolgáltatások széleskörű igénybevételi lehetőségeire, kétirányú felkészítést látok megvalósíthatónak. Szükséges egy általános, a lakosság lehető legszélesebb körét elérő felkészítési rendszer, amelyet jelenleg a hivatásos katasztrófavédelmi szerv klasszikus lakosságfelkészítési tevékenységében látok megvalósíthatónak. Emellett azonban célszerű egy ágazatokra jellemző speciális – ágazati rendeletekben szabályozott módszertan szerinti – felkészítési metódus, amely az egyes KI elemeket kötelezi az általuk közvetlenül érintett lakosság információkkal történő ellátására.

Ez a gyakorlat jelenleg teljesen kiforratlan. A hazai és a külföldi jogforrások, vagy szakirodalmak gyakorlatilag egyáltalán nem foglalkoznak mélységében ezzel a kérdéskörrel. A KIV európai programjának 2011-ben kezdődött felülvizsgálata valójában jelenleg is tart, eredményei között számos új megközelítés található, de a KIV célkitűzéseként azonosított felkészülés lakosság szemszögéből történő célirányos vizsgálatára még nem került sor.

A felülvizsgálattal kapcsolatban, 2012 nyarán kiadott munkadokumentum rávilágított arra, hogy a legfőbb célkitűzés a jelenlegi KIV folyamatok hiányosságainak azonosítása és a kockázatbecslési módszertan közösségi szintű alkalmazására való felkészülés, amely az Európai Tanács 2011. áprilisi következtetésével (az EU-n belüli katasztrófa-elhárítással kapcsolatos kockázatértékelések fejlesztésével) párhuzamosan valósítható meg. A tervezett kockázatbecslések és kockázatértékelések folyamatának szerves része az egyes KI működési zavarok, kiesések lakosságra gyakorolt hatásainak vizsgálata, de jelen célok alapján mindebbe

nem tartozik bele a potenciálisan kialakuló veszélyhelyzetekre történő lakossági felkészítés [12].

A kritikus energetikai infrastruktúrák védelmének hálózatával kapcsolatban egy 2012-ben kiadott EU Bizottsági állásfoglalás hangsúlyozza például a határon átnyúló hatások létfontosságú stratégiai jellegét és felismeri a lakosság részéről is potenciálisan fennálló veszélyeztető tényezőket (pl.: vezetéklopás, vandalizmus), de továbbra is az állam és az üzemeltető/tulajdonos közötti információáramlás biztosítását helyezi előtérbe. Az állásfoglalás már külön foglalkozik a fogyasztók ellátására gyakorolt hatások jelentőségével és következményeivel, de a kockázat alapú megközelítés nem tartalmazza a lakosság felkészítésének ide kapcsolható szegmenseit [13].

A montreáli műszaki egyetem kutatói, a KIV lehetséges dominó-hatásának és a védelmi folyamatok rugalmasságának vizsgálata során összehasonlításokat végeztek a KI-k esetében rendelkezésre álló tudás, valamint számítási és tervezési folyamatok vonatkozásában. Ennek keretében a felkészülés (scenario alapú gyakorlatok) célcsoportjaiként a kritikus infrastruktúra elem üzemeltetőit/tulajdonosait és alkalmazottaikat, valamint ún. „kulcsfontosságú érintetteket" azonosították. Az elemzés – és így az eredmény – nem tartalmaz az egyes infrastruktúrákban bekövetkező veszélyhelyzetekkel kapcsolatos olyan megállapításokat, amelyek kifejezetten a működési problémák által érintett lakosságra gyakorolt hatással, vagy a kiváltott reakciókkal lehetnek kapcsolatosak [14].

Nemzetközi tekintetben Fadi A. Karaa, a New Jersey Technológiai Intézet egyetemi docense egyik előadásában fejtette ki oly módon a KI rendszerek célkitűzéseit, hogy konklúziójában a KI-val kapcsolatos veszélyhelyzet-kezelés egyik alapvető feladataként azonosította az operatív reagálás mellett a lakosságvédelmi feladatokat. A gazdasági fejlődés, az életminőség biztosítása, a fenntarthatóság és a megfelelő erőforrás gazdálkodás mellett ugyanis kimondta, hogy a lakosságvédelemnek, mint célkitűzésnek része kell legyen a sebezhetőség megértetése, a dominó-hatás és a nem kívánt események megismertetése, valamint a védelmi lehetőségek meghatározása egyaránt. Módszertant, eljárásrendet, célcsoportokat és tartalmi elemeket azonban nem nevesített [15].

3. 2. Lakosságfelkészítés és lakosságtájékoztatás

A 2012. január 1-jén hatályba lépett, a katasztrófák elleni védekezés nemzeti rendszerét meghatározó jogszabálycsomag a jogszabályi hierarchia minden szintjén, a megfelelő részletességgel tér ki a katasztrófákkal kapcsolatos megelőző időszaki lakosságfelkészítési tevékenység alapvető követelményeire, módszereire, valamint a katasztrófa bekövetkezését követő riasztási és veszélyhelyzeti tájékoztatási feladatokra egyaránt.

Figyelemmel a korábbiakban már feltárt tényre, hogy a lakosságnak is kötelezettsége és egyben joga, hogy a közvetlen környezetét és az abban jelentkező veszélyforrásokat megismerje, a túléléshez és a meneküléshez megfelelő ismeretekkel és információkkal rendelkezzen, valamint az Aarhusi Egyezmény vívmányaira, a szabályozók egyik legfontosabb része a riasztás és a veszélyhelyzeti tájékoztatás, amelyet a lakosságfelkészítéssel együttesen szükséges értelmezni és alkalmazni. A rendelkezések alapján a felkészítésnek két alapvető módja van:

<table>
<tr><th>Aktív lakosságtájékoztatás</th><td></td><th>Passzív lakosságtájékoztatás</th></tr>
<tr><td>tájékoztató kiadványok</td><td rowspan="4">ESZKÖZ</td><td rowspan="2">kiadványok elérhetővé tétele</td></tr>
<tr><td>közlemények a helyi sajtóban (írott, elektronikus, képi)</td></tr>
<tr><td>lakosság fórumok</td><td rowspan="2">katasztrófavédelmi kirendeltségi nyílt nap</td></tr>
<tr><td>nyilvános rendezvények</td></tr>
<tr><td colspan="3">TARTALOM</td></tr>
<tr><td colspan="3">riasztási módszerek és jelek
magatartási szabályok
segítségnyújtás formái
helyi kockázatok
veszélyelhárítás módjai</td></tr>
</table>

6. ábra. A felkészítés módjai (Szerk.: szerző)

Fentiek alapján lakosságfelkészítési eszköznek tekinthető minden olyan tájékoztató kiadvány, helyi sajtó közreműködésével kialakított információs fórum és nyilvános rendezvény, amely az aktív módszer alkalmazásával, a korosztályi sajátosságok figyelembe vételével kialakított tartalommal jut el a lakossághoz. Mindemellett lehetőség van a passzív módszerek által történő folyamatos felkészítésre is. Ez alatt főként az interneten közzétett és állandóan elérhető információs kiadványokat és az eseti jelleggel rendezett nyílt napokat értjük.

A tájékoztatás tartalma – mindkét módszer esetében – elsősorban a riasztási jelek felismerésére, a helyi sajátosságokon alapuló veszélyeztető tényezők megismerésére és az ezekhez kapcsolható magatartási szabályok elsajátítására irányul. A hatékony és eredményes felkészítés kulcsa mindezeken túlmenően a célcsoportok szerinti információ átadás, amely lehetővé teszi, hogy széles körben, az életkori sajátosságok elsődleges figyelembe vételével biztosítsuk a lehető leghasznosabb tudást a lakosság részére. A katasztrófavédelmi célú lakosságfelkészítés keretében a következő célcsoportok elkülönítésére került sor:

<table>
<tr><td>polgári védelmi szervezetek</td><td>polgári védelmi szervezetbe beosztott személyek
kijelölt vezetői állomány</td></tr>
<tr><td>közigazgatási szereplők</td><td>központi államigazgatási szervek vezetői által kijelölt személyek
megyei védelmi bizottság elnökei és tagjai
helyi védelmi bizottság elnökei
főpolgármester, a polgármesterek és a jegyzők
közbiztonsági referensek</td></tr>
<tr><td colspan="2">katasztrófavédelmi feladatok ellátásában részt vevők és közreműködők</td></tr>
<tr><td>köznevelésben részt vevők</td><td>óvodai, alap- és középfokú nevelésben részt vevők
felsőoktatásban részt vevők
sajátos nevelési igényűek
pedagógusok (óvodapedagógus, általános és középiskolai pedagógus)</td></tr>
<tr><td colspan="2">egyéb lakosság</td></tr>
</table>

7. ábra. A felkészítés célcsoportjai (Szerk.: szerző)

Általánosságban igaz, hogy az új alapokra helyezett szabályozás kiforrott, megalapozott rendszerbe helyezi a katasztrófavédelmi célú lakosságfelkészítést [16].

4. AZ ÁLTALÁNOS LAKOSSÁGFELKÉSZÍTÉS LEHETSÉGES MÓDSZERTANA KIV SZEMPONTBÓL

A létfontosságú rendszerek és létesítmények vonatkozásában az információk érzékenysége elsődleges és meghatározó. Rendkívül fontos, hogy egy-egy létfontosságúként kijelölt rendszer működésével kapcsolatos információhalmaz elsősorban támadási, károkozásra alkalmas lehetőséget biztosít az ártó szándékú cselekményekre. Emiatt – figyelembe véve a titokvédelem alapelvét – a lakosságfelkészítés és a lakosságtájékoztatás során különös figyelmet kell szentelni arra, hogy a szükséges és elégséges tudás, amely lehetővé teszi a KI elemek sérülését követően a megfelelő magatartásformák alkalmazását, ne tartalmazzon olyan információt, amely fentiekre irányul.

A lakosságfelkészítési tevékenység módszertanát tekintve a KIV vonatkozásában is szükséges meghatározni a felkészítés célcsoportjait. A definiálás során – az életkori sajátosságokon túl – tekintettel kell lenni a XXI. századi társadalomra jellemző „informatizáltságra", a korosztályok közötti egyre mélyülő különbségekre, és a demográfiai eltérésekre. Mindezek alapján az általános, a létfontosságú rendszerek és létesítmények által hordozott veszélyeztetettségre való lakosságfelkészítés fő célcsoportjait a következők szerint javasolom meghatározni:

- közigazgatási szereplők;
- KIV védelmének biztosításában részt vevők;
- egyéb lakosság.

E célcsoportok részére az általános felkészítés célkitűzéseként nem a KI megismerését, hanem annak zavarai, esetleges kiesése miatti következmények bemutatását és a válaszul adandó magatartási formák elsajátítását szükséges meghatározni. Hasonlóan a katasztrófavédelmi felkészítés céljához a KIV célú felkészítésnek is a bekövetkezhető események során jelentkező feladatok ellátására, a káros következmények lehető legkisebbre csökkentésére, valamint a megfelelő és elvárható lakossági reagálás biztosítására kell irányulnia. Ennek keretében az irányadó reagálási szabályok és a tudatos biztonságra nevelés jegyében a felkészítés az állampolgári felelősségérzet és az elővigyázatosság kialakítását, az alternatívák egyén szintjén történő biztosításának alapjait hivatott garantálni.

A felkészítés módszertanát tekintve alkalmazható az aktív és a passzív tájékoztatás egyaránt. A létfontosságú rendszerek védelmét biztosító szervezetek és felelősök felkészítése során főként az aktív, közvetlen és célirányos képzéseket célszerű alkalmazni, míg a lakosság vonatkozásában – célcsoporttól függően – az aktív és a passzív módszer egyaránt eredményes lehet. Vizsgálataim alapján a következő módszertant tartom a leginkább végrehajthatónak:

CÉLCSOPORT		MÓDSZER
közigazgatási szereplők	ágazati államigazgatási szervek vezetői által kijelölt személyek megyei védelmi bizottság elnökei és tagjai helyi védelmi bizottság elnökei főpolgármester, a polgármesterek és a jegyzők közbiztonsági referensek	**aktív**: tantermi, e-learning, konzultációs, tréning jellegű képzés
KIV védelmének biztosításában részt vevők	üzemeltető, tulajdonos szolgáltatók állománya élet- és vagyonbiztonság garantálásáért felelős hatóságok állománya	
egyéb lakosság	köznevelésben részt vevők (életkori sajátosság szerint) felsőoktatásban részt vevők sajátos nevelési igényűek pedagógusok	**aktív:** tantermi, tananyagba integrált képzés
	lakóközösségek (városi és vidéki) civil egyesületek "social media" közösségek	**aktív & passzív:** fórumok, rendezvények, kiadványok, kampányok,

8. ábra. A felkészítés célcsoportokhoz köthető, javasolt módszerei (Szerk.: szerző)

Fentiek figyelembe vételével szükséges meghatározni az általános felkészítés tartalmát, amelynél főként az energia és az infokommunikációs ágazat sérülése vagy kiesése miatti következmények játszhatnak meghatározó szerepet. A lakosság az e rendszerekből fakadó hibák, tartós szolgáltatás kimaradások, illetve akadozások hatásainak van leginkább kitéve. A következő ábra fontossági sorrend szerint szemlélteti a lakosság szempontjából elsődleges ágazatok működési zavaraihoz köthető lehetséges hatásokat. Az ábrán szerepelnek továbbá azok a szektorok is, amelyek egy-egy ágazat infrastruktúráival szoros kapcsolatban állnak, így az interdependencia és a dominó-elv alapján ok vagy okozat formájában kapcsolhatóak az adott ágazat működési zavarához.

ÁGAZAT	SÉRÜLÉS/KIESÉS HATÁSA	LEHETSÉGES KAPCSOLÓDÁSI PONTOK
ENERGIA	áramszünet, gázszolgáltatás szünetelése, fűtési/hűtési problémák, kommunikációs kihívások, közlekedési nehézségek	**infokommunikáció,** közlekedés víz, egészségügy, ipar, pénzügy
INFOKOMMUNIKÁCIÓ	információs rendszerek leállása, információhiány, tájékoztatás nehézségei, kormányzati rendszerek akadozása, mentésirányítás problémái	**energia,** közlekedés, víz, egészségügy, pénzügy, ipar
VÍZ	ivó-vízszolgáltatás hiánya, minőségromlás, szennyvíz-elvezetési problémák, ár- és belvízi helyzet	**energia,** egészségügy, **infokommunikáció,** ipar
KÖZLEKEDÉS	lezárt utak, torlódások, vasúti közlekedés akadozása, leállása, balesetveszélyes körülmények	**energia, infokommunikáció**
EGÉSZSÉGÜGY	mentésirányítás akadozása, kórházi ellátás kiesése, járványok kialakulásának veszélye	**energia, infokommunikáció,** víz
IPAR	veszélyes anyagok környezetbe kerülése, ipari termelés kiesése	**energia, infokommunikáció,** közlekedés, pénzügy, egészségügy, víz
PÉNZÜGY	bankrendszer akadozása, jövedelemhez és tartalékokhoz való hozzáférés szünetelése	**energia, infokommunikáció**

9. ábra. Ágazatok működési zavarainak hatása és kölcsönös függősége (Szerk.: szerző)

Nemzetközi szinten széleskörű, főként tapasztalati úton kialakított lakosságfelkészítési módszertanokat figyelhetünk meg, amelyeknek – hazánkhoz hasonlóan – nem része még a kritikus infrastruktúrák védelmével kapcsolatban szükséges információ átadás. Az alapelvek és megközelítések azonban további alapot adhatnak a hazai KIV célú felkészítésnek.

Az Amerikai Szövetségi Veszélyhelyzet-kezelési Ügynökség (Federal Emergency Management Agency – FEMA) rendkívül nagy jelentőséget tulajdonít a megfelelő szintű és tartalmú lakosságfelkészítésnek, így megalapozott és tapasztalati úton fejlesztett módszertanokat alkalmaz a szükséges és elégséges információk elsajátíttatására. A FEMA a *„whole community approach”*[11] elvének megfelelően a lehető legszélesebb körű tájékoztatás megvalósítására törekszik, amelyet tematizáltan, több módon elérhető információk folyamatos biztosításával hajt végre [17].

A nyugati társadalmak többségénél kiemelt szerepet kap a lakosságfelkészítés és tájékoztatás rendszerében a *„social media”*, vagyis az infokommunikációs eszközök és a világháló által létrehozott „eszközrendszer”. Hazánkban még nincs kiforrott módja az ilyen úton történő felkészítésnek, de az elmúlt időszak tapasztalatai alapján jelenleg zajlik a katasztrófavédelmi célú felkészítés és tájékoztatás ilyen irányú fejlesztése. A BM OKF 2013. május 30-án elindította Facebook-oldalát, amely módszert például a Magyar Honvédség egy

[11] Jelentése: teljes közösség szempontjából történő megközelítés.

ideje már alkalmaz. A következő hetek során kerül pontosításra, hogy ez a módszertan, amely a fiatalok körében oly kedvelt közösségi oldalon tehet elérhetővé alapvető ismereteket, valamint bekövetkezett katasztrófahelyzetek során szükséges információkat, pontosan milyen tartalommal, milyen rendszerben fog működni.

Mindemellett rendelkezésünkre áll a SEVESO II. irányelv által bevezetett, a lakosság aktív tájékoztatásáról szóló kötelezettség módszertana, amely a veszélyes anyagokkal foglalkozó üzemek által veszélyeztetett területen élők rendszeres és kérés nélküli tájékoztatását írja elő [18]. Ennek megvalósítása hazánkban a felső küszöbértékű üzem külső védelmi tervével egyidejűleg készített lakossági tájékoztató kiadvány összeállításában nyilvánul meg. Tekintettel arra, hogy az ilyen típusú kiadványok célirányosan az adott veszélyes üzem sajátosságai által hordozott veszélyeztetettséggel kapcsolatos információkat tartalmazzák, módszertanilag különösen alkalmasak lehetnek a mind a KIV célú általános, mind pedig az ágazati felkészítés során.

Szorosan ide kapcsolható az a hazai törekvés, amelyet a 2012 októberében létrejött Országos Tűzmegelőzési Bizottság (a továbbiakban: OTB) végez. A bizottság kifejezetten tűzmegelőzési feladatok támogatására létrehozott tanácsadó és kommunikációt folytató szerveződés, amely a Nemzeti Fejlesztési Minisztérium, a Vidékfejlesztési Minisztérium és a BM OKF együttműködésének eredménye és megnyilvánulási formája. Az OTB által eddig végrehajtott projektek a CO mérgezések veszélyeire való figyelemfelhívásra, valamint a szabadtéri tüzek megelőzésének fontosságára irányultak. A módszertant figyelembe véve megállapítható, hogy kifejezetten alkalmas széleskörű felkészítésre, információ átadásra, így meggyőződésem, hogy a KIV célú felkészítés keretében is megfelelően alkalmazható lehet.

A fenti áttekintés alapján megállapítható, hogy a jelenlegi katasztrófavédelmi célú felkészítés rendszerében van helye az általános KIV felkészítésnek, mert célcsoport és módszertan szempontjából is integrálható. További kutatást és tervezést igényel azonban az ágazatokra jellemző, speciális felkészítési folyamat, amely az egyes szektorok különbözősége miatt várhatóan markáns eltéréseket fog mutatni.

ÖSSZEFOGLALÁS

Vinton Gray Cerf [12] szerint nem az információ a hatalom, hanem az információ megosztása. Meggyőződése, hogy „az emberiség történelme során rendszeresen beigazolódott, hogy az *információ*, a tudás megosztása egyre nagyobb hatalommal jár, és hogy azok a társadalmak, amelyek visszatartják az *információ*t, óriási károkat okoznak saját maguknak”. Az információ jelentőségének bemutatása alapján egyetértésemet fejezem ki a fenti gondolattal, amelyet tovább gördítve hangsúlyozni kívánom a kommunikációs folyamatok jelentőségét, az információ megosztásának hasznosságát. Mindezek aktív és célirányos alkalmazásával a lakosságfelkészítés rendszerében biztosítható minden olyan ismeret és információ, amelyek az egyén biztonságkultúrájának, reagáló és túlélő képességének fejlődését biztosíthatják.

A katasztrófavédelmi célú felkészítési folyamatok jelenlegi végrehajtását tekintve meggyőződésem, hogy szükséges és lehetséges a létfontosságú rendszerek és létesítmények vonatkozásában alapvető információk átadása, amennyiben az általános felkészítés tartalma meghatározásra kerül. Ehhez természetesen mélyebb és kifejezetten a lakosság információ-szükségletét célzó kutatásokra van szükség, amely elképzelhetetlen az ágazatok közreműködése nélkül. Az általam általános felkészítésnek nevezett folyamat nem létezhet a szektorok sajátosságait magába foglaló, ágazati felkészítési rendszer kidolgozása nélkül, amely pedig kifejezetten egy-egy ágazat által hordozott, a lakosság mindennapi életének folyamatossága szempontjából meghatározó tájékoztatást biztosíthatja.

[12] Amerikai matematikus és informatikus, akire általában az Internet egyik alapító atyjaként hivatkoznak.

Az Aarhusi Egyezmény egyik alapelve, hogy az információk biztosítása során a *„közérdeket szükséges előtérbe helyezni”*, így az állami feladatba – a katasztrófavédelmi felkészítésbe – történő integráció, a már működő rendszer kiegészítésével rövid idő alatt, kis ráfordítással megvalósítható.

Felhasznált irodalom

[1] Denis McQuail: A tömegkommunikáció elmélete; Osiris kiadó, Budapest 2003.

[2] http://www.bokorportal.hu/bokke/3e/egyens/04egyens.php (letöltés ideje: 2013. 05. 09.)

[3] http://infoter.blog.hu/2012/01/25/jogos_e_a_jog_az_informaciohoz (letöltés ideje: 2013. 05. 09.)

[4] http://www.katasztrofak.abbcenter.com/?cim=1&id=39103# (letöltés ideje: 2012. 04. 02.)

[5] Mógor Judit: A lakossági tájékoztatás és a nyilvánosság biztosításának kutatása a súlyos ipari balesetek elleni védekezésben. PhD értekezés, Budapest 2011.

[6] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

[7] Magyarország Alaptörvénye (2011. április 25.)

[8] A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény

[9] COM (2005) 576 final – Zöld Könyv az európai kritikus infrastruktúrák védelmének európai programjáról

[10] Bonnyai Tünde: A kritikus infrastruktúra védelem fogalmi rendszere, hazai és nemzetközi szabályozása. Pályamunka a Katasztrófavédelmi Tudományos Tanács pályázatán. Budapest, 2011. (http://www.vedelem.hu/letoltes/tanulmany/tan382.pdf)

[11] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) kormányrendelet

[12] Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP) – SWD(2012) 190 final

[13] Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection (November 2012)

[14] B. Robert, L. Morabito, I. Cloutier, Y. Hémond: Interdependent Critical Infrastructures: from protecion towards resilience – 2013. (http://www.tisp.org/index.cfm?cdid=13144&pid=10261, letöltés ideje: 2013. 05. 02.)

[15] *„Critical Infrastructure Symposium 2013: The Infrastructure Security Partnership”* – 2013. április 16., New York

[16] a katasztrófák elleni védekezés egyes szabályairól szóló 62/2011. (XII. 29.) BM rendelet

[17] http://www.fema.gov/national-preparedness/whole-community (letöltés ideje: 2013. 05. 20.)

[18] A veszélyes anyagokkal kapcsolatos súlyos baleseti veszélyek ellenőrzéséről szóló 96/82/EK Irányelv 13. cikk.

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Lucas Grégory – Halász László – Solymosi József
gregory.luc4s@gmail.com - halasz.laszlo@uni-nke.hu - solymosi.jozsef@uni-nke.hu

EXPLORING THE CAPACITIES OF AIRBORNE TECHNOLOGY FOR THE DISASTER ASSESSMENT

Abstract

This article reviews the existing airborne technologies and explores their capacities for the disaster assessment.
The first part of this article aims at providing comprehensive information about disaster assessment and the existing airborne technology. First, some definitions and general introductory information are given about disaster and airborne technology. It is followed by an inventory about the different types of disasters, the associated relevant information to be gathered for the situation assessment, and last by a review of the airborne technology (different platforms, sensors and associated capacities).
The second half of this article aims at assessing the capacities of airborne techniques for disaster assessment putting into relation a type of disaster with a method on how to perform the assessment work. This part is completed by the presentation of a set of strategically chosen case studies in order to cover diverse types of disasters and the aerial reconnaissance solutions employed.

A cikk bemutatja a katasztrófa helyzetértékelésben alkalmazható légi felderítő eljárások lehetőségeinek áttekitését. A közlemény első felében jellemzésre kerülnek a katasztrófa típusok, valamint a helyzetértékeléshez szükséges információk. A publikáció második részében a légi felderítésben használt módszerek és alkalmazhatóságuk kerül elemzésre illetve az egyes légi felderítő eljrások hatékonyságának bemutatása gyakorlati példák segítségével.

Keywords: *airborne, reconnaissance, disaster, catastrophe, remote sensing, sensors ~ légierő, felderítés katasztrófa, távérzékelés, érzékelők*

INTRODUCTION

An airborne disaster *assessment* is a preliminary survey made by airborne means in order to collect information about the situation on an area affected by a disaster. Information collect can be oriented towards several goals at the same time, for example the estimation of the damages done, or easing the orientation of the first emergency responses (first help to people), or supporting situation analysis for protective measures (in case of a dynamic disaster which can endanger a larger area).

This study considers all existing types of disasters which are commonly divided in two groups: natural (meteorological, hydrological, biological, etc.) and man-made (sociological and technological hazards).

Airborne techniques are usually chosen for their ability to cover large areas within a short time. Airborne remote sensing also offers some advantage compared to field survey in case a road network infrastructure is not usable or if the level of contamination on the ground is unknown or could threaten health.

The evolution of sensors and processing capabilities has widened the spectrum of applications where aerial reconnaissance can be utilized. Classical imagery has been completed with a couple of new technologies like LiDAR, hyperpectral imagery, thermal imagery which already has or could find some applications in disaster management. The recent trend with the use of UAV platform and UAV sensor technology is also considered in this study.

DISASTER TYPOLOGY AND RELEVANT SITUATION INFORMATION TO COLLECT

This part takes as an input the different types of disasters and provides an inventory of the information potentially relevant in the different assessment processes. Generally three types of assessment are used:

Situation (Disaster) Assessment. This assessment gathers information on the magnitude of the disaster and the extent of its impact on the population and the physical infrastructure, as well as the environment.

*Needs Assessment***.** The initial needs assessment identifies resources and services for immediate emergency measures to save and sustain the lives and livelihoods of the affected population. Conduct this assessment at the site of a disaster or at the location(s) of displaced population(s).

Environmental Impact Assessment. The need to consider environmental issues during disaster operations rests on four considerations:

- Environmental degradation often causes natural disasters and aggravates their effects.
- Competition over natural resources frequently provokes armed conflicts.
- Disasters can result in significant environmental damage.
- Relief assistance can result in negative environmental impacts, leading to a need for additional assistance to solve problems that could have been avoided or at least mitigated if they had been anticipated in the disaster response planning stages.

The airborne assessment is very important in the situation and environment impact assessment.

The different types of disaster are listed in tab.1. Disasters can be divided in two groups: natural disaster and man-made disasters. The first column of tab.1. summarizes the information gathered from different sources dealing with disaster classifications. [1], [2], [3]

The table was filled considering a disaster and information potentially available from aerial means which could be relevant to disaster management. For all the types of disaster it is relevant to know:

- the extent of the impacted area
- the intensity of the damages
- if there are difference with the intensity of damaged inside an impacted area (zonation)
- if there are other areas are potentially endangered
- the location of the victims for their assistance.

As this information is common for all the disasters, to avoid repetition, they are not written in tab.1.

Type of disaster	Relevant information to be gathered by aerial reconnaissance means
Natural disasters	
Geophysical	
Earthquakes	* Damage to infrastructure and critical facilities * Damage to homes and commercial buildings.
Tsunami	***Number of people to evacuate. * Damage to infrastructure and critical facilities * Damage to homes and commercial buildings. *Distinguishing the areas that dried for first help.
Volcanic eruption	*** Number of people to evacuate. **Detection of active areas though the thermal activity, gas emission or through the changes in elevation. **Gathering information about speed and direction of the lava, lahars, etc flows as well as terrain elevation, POI on the trajectory.
Mass movement (avalanche, land slide, rock fall)	***Existence of unstable snow layer, rocks, soil layer. */**Direction of the movement. Speed. POI on the trajectory. *Info about critical infrastructure status
Hydrological	
Floods	*** Number of people to evacuate. **Volumetric data. */**/***Elevation data. Precise surface model. **Evolution of the situation
Mass movement (land slide, rock fall)	*** Number of people to evacuate. ***Existence of unstable snow layer, rocks, soil layer. */**Direction of the movement. Speed. POI on the trajectory. *Info about critical infrastructure status
Meteorological	*Short term small scale*
Blizzards	*Info about road network obstruction
Storms/Cyclone	*** Number of people to evacuate. *Info about critical infrastructure status (bridges, main roads, hospital, etc.)
Climatological	*Medium to long term, large scale*
Wildfires	*** Number of people to evacuate. **Hot spots detection. **Live evolution of the situation (direction of the fire).
Droughts	
Extreme temperature	
Biological	**Spread of diseases in vegetation, spread of invasive species, blooms (algae).
Extraterrestrial	
Human-made disasters	
Sociological	
Civil disorder, terrorism and war	Impacted area, impacted infrastructure, victims, intensity of damages. Refer to fire, industrial, nuclear, CBRN.
Technological	
Industrial	*Location, thickness, concentration of contamination.
Fire	**/*Localization of hot spots. **Information about efficiency of firefight (for adapting the fight).
Transportation	*chemical identification *identification of POI/AOI to protect (water catchments, rivers, etc)
Nuclear	*chemical identification *dose rate quantification *concentration and dissemination.
CBRN	**chemical identification **quantification (concentration, spread, dissemination) of CBRN agent. **identification of POI/AOI to protect (water catchments, rivers, etc)

1. table. Relevant information to be collected by aerial means for each type of disaster *post-,**during, ***pre-disaster.

Depending on the type of disaster assessment activities can be oriented on the pre-disaster phase (when disaster protection is possible), during the disaster (if conditions are favorable for flying), and post-disaster phase (first help guidance). Almost all the types of disaster listed found some potential application of aerial reconnaissance. Some disasters like CBRN, nuclear, industrial requires the collect of measurable physical values (concentration, dose rate, etc) whereas other disaster rather requires environmental and geographical characteristics (flooding) and a third category rather requires infrastructure status information (cyclone, earthquake).

This part has answered to the question "which information should be gathered". The next question to be logically answered is "how to gather the information?"

OVERVIEW OF THE TECHNICAL CAPACITIES OF AIRBORNE TECHNOLOGY

This part introduces and categorizes the different types of sensors and their detection and implementation capacities.

Different platform for very different aims and operational context

Airborne reconnaissance employs different types of platforms with different associated capacities. Tab. 2 summarizes the main advantages and disadvantages between the different platforms. Aircraft reconnaissance is privileged to cover large areas within short time at relatively high altitude. Helicopters are utilized when flight characteristics require low altitude, low speed or following a corridor trajectory. UAV are limited to the survey of small areas; their main limitation is the carriage load.

Platform	Advantage	Disadvantage
Aircraft	Faster flight speed and higher altitude allow larger area coverage per unit of time.	Cannot perform acquisition at low speed. Can not follow curves and corridors. Minimal AAG required for safety.
Helicopter	No minimal speed. Possibility to fly at low AAG[1] and to follow terrain elevation. Possibility to fly curves and corridors.	The most costly. Lower coverage capacity per unit of time.
small UAV	Flexibility, maneuverability. Adapted to small areas. The less costly.	Limitation with the carriage load. Limitation with the coverage capacity. Technology still under development for certain censors.

2. table. Advantages and disadvantages associated to different types of holding platforms

To be noticed platform and sensors cannot be chosen independently. Sensor influences the selection of a platform by its requirements regarding the AAG it should be operated at (which mainly depends on the required accuracy) and the requirement regarding the flight characteristics (ground speed). The nature and size of the target object of the reconnaissance also influence the selection of the platform.

Sensors presentation

Each sensor is characterized by the physical detection principle it is based on (wavelength reflection, absorption, measurement of light travelling time, etc), its capacities (accuracy, detection range, field of view, etc) and the characteristics of the product for the end user. The following paragraphs provide detailed information about a couple of very common sensors used in disaster surveys. Thus completion about aerial sensors is given into a synthetic table (tab.3.).

[1] Altitude Above Ground

Aerial imaging

Nowadays aerial imaging is performed with digital cameras (medium, large and ultra large format). [8], [9] Red, Green, Blue and Near Infra Red channels (RGBN) are the most commonly used. GSD[2] is governed by the flight altitude (AAG). The smaller the GSD is, the most detailed the pictures are. From a given GSD the required AAG is calculated. Based on the AAG, the FOV of the sensor (determined by the pixel size and number of pixel of the CDD array) and the requirement for the overlay between the frames it possible to determine the position of the flights lines, the frame footprints and to calculate the flight time (tab.7. provide a good example). Maximal flight speed is determined by the maximal frame rate of the sensor (1 frame per second in the case of Leica RCD30 camera for example). All these operations are done and assisted by flight planning software. Camera control system is coupled with GPS/IMU system to store the external orientation parameters which are used during the post-processing of the images for their geometric correction and correct positioning into a block (photogrammetry). Aerial imaging is the most versatile reconnaissance mean for mapping the status over an area. In term of time, 5h roughly covers 260 km^2 with a medium format camera at 1200m AAG. Post processing overall requires 24 to 30h to make the radiometric image enhancement, to calculate trajectories, to determine image external orientation and to mosaic images. As a general rule an ortho-image product can be available within 24-72h after the beginning of mobilization of the aircraft (depending on the size of the AOI and final accuracy required). Oblique imagery

Imagery is useful in the entire situation where photo interpretation provides relevant information about the situation (status of roads, buildings, areas flooded or not, impacted or not, etc).

Aerial laser scanning

LiDAR is the modern mean to establish terrain models (DTM) and surface models (DSM). The sensor measures the travelling time between the source point and the ground and derivate a distance between the sensor and the target. Laser scanner is operated coupled with a GPS/IMU system. The orientation of the laser beam is known every time a shot is sent. Knowing the position of the aircraft and the orientation and the beam, each point hit on the ground can be positioned in a x,y,z digital model. The main characteristic of the LiDAR system are the pulse rate (partly determine point density) and the scanning pattern. The overlay between the strip, the flight speed, flight AAG and the pulse rate determine the average point density of the final product. Hydrologic model requires 5 pt/m^2 average densities. The systems can produce clouds of point from 0,5 pt/m^2 to 42 pt/m^2 in general condition of use. Scanning patterns influence the point repartition on the ground (raster, sinusoid, triangular) and at the NADIR in particular. The flight speed is similar to the one for imaging.

DSM and DTM derivates from the cloud of points (after geometric correction, error correction and classification). They can be used for 3D modeling (infrastructure), flood modeling, volumetric calculation, and also in combination with other data (data fusion) for automatic classification (the elevation is a useful input in object oriented classification). [4]

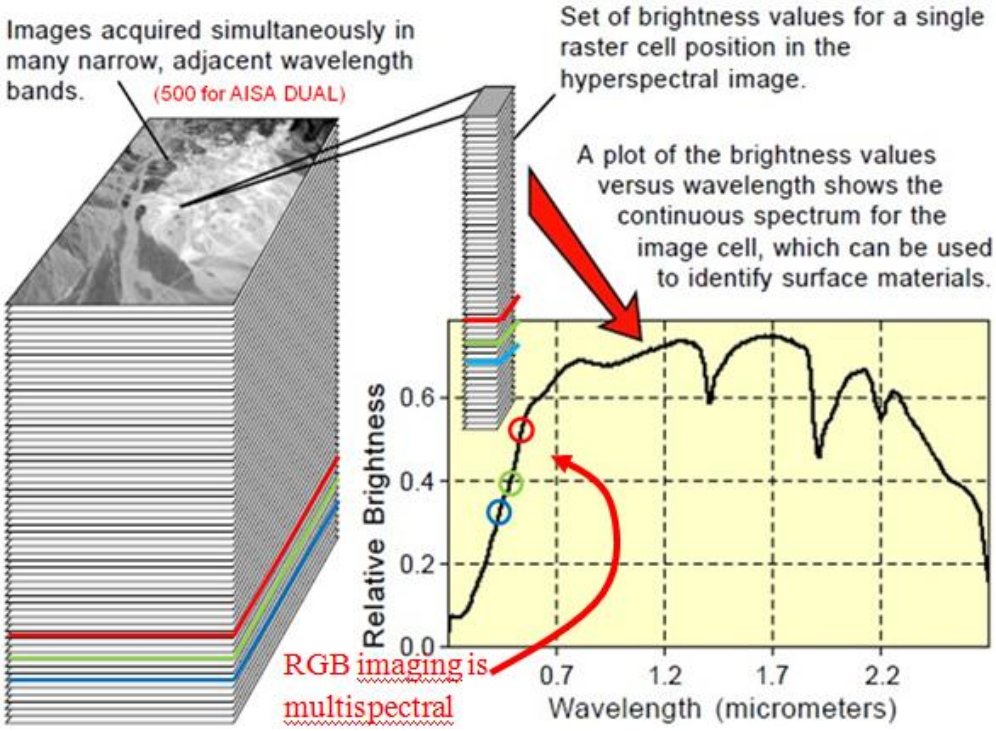
Another application of laser scanning exists, it is called differential laser scanning and it is based on the measurement of the absorbance of the laser beam by the target at variable emission wavelength. [5] The technique is relevant to measure gas concentration in the air, chemical and contamination in the atmosphere. [6], [7]

[2] Ground sampling distance

Hyperspectral imaging

Hyperspectral imaging extends the capacities of imaging with providing spectral data about ground surface objects (different from multi spectral imaging where data is provided for a limited number of and non contiguous spectral values). Hyperspectral spectrometer exists in the VNIR, SWIR, LWIR and FIR regions. Technically they are characterized with their spectral resolution, spectral range and spatial accuracy.

Thematic maps are the products associated to hyperspectral imaging. The huge amount of information from the spectral data about objects on the ground can be derivate to classify the images with higher accuracy. Thus it is possible to classify objects that other methods do not "see" or to make more sharp distinctions. Recent application of hyperspectral imaging was done for oil mapping, contamination mapping, and gas detection in the atmosphere.



1. figure. General principle of hyperspectral imaging and differentiation from multi spectral imaging (RGB)

Aerial spectrometers with more accurate spectral resolution covering several spectral regions are under development (at present they only cover a really narrow part of one spectral region), this will open the era of ultra spectral imaging and they are expected to push forward the limits with air composition detection. [8], [9]

Sensor	Physical detection principle	Capacities	End product
RGBN. Medium, large and ultra-large format digital camera [10], [11]	Measurement of light reflectance by physical objects on the ground at 3+ different wavelength at "NADIR"	Medium format camera (RCD30): 47 km^2/h at 1300m AAG, FOV 60°, 12cm GSD, 51 m/s. Large format camera (ASD80): 170 km^2/h with 15 cm GSD, 65m/s.	RGBN ortho-images, mosaics.
RGB oblique imagery [12], [13]	5 RGB cameras are disposed at 45° in forward backward, right and left directions + NADIR	10-50 cm GSD. Similar to medium format camera.	true-ortho, 2,5D city models. Measurement in enhanced 2,5D view. View around buildings.
Laser scanner (LiDAR) [14], [15]	Active. Distance sensor-target by light travelling time + orientation of the laser beam.	Max. 5cm vertical accuracy, 0-75 degree FOV. 250 kHz. 1-42 point/m^2. First pulse, last pulse, full wave form. Average coverage 50 km^2/h.	Elevation models (DSM, DTM).
Differential absorption LiDAR (DIAL) [6], [7]	Active. Absorption of lights energy by particles or gas in the atmosphere	Water vapor, CO2, aerosol, ozone and gas detection with concentration estimation.	Air composition and element concentration maps.
Hyperspectral imaging	Measurement of light reflectance by physical object of the ground, atmospheric gas at more than 400 wavelengths.	AISA Dual (400-2500 nm (VNIR&SWIR)): 3,3-12nm spectral resolution. 65 cm GSD at 1000m AAG, FOV 24° [16] AVIRIS: 224 contiguous bands for AVIRIS from 400 to 2500 nm [17].	ortho images. Classified images, thematic maps.
Thermal imaging	Measurement of heat emission (and reflection).	Digitherm system: 0,05K thermal resolution for the sensor = +/-1,5K for temp. measurement. [18]	Maps of thermal radiance.
Gamma spectrometry [19], [20], [21], [22]	Gamma photon captured by ionization chamber or by crystals.	Require helicopter at 70km/h, altitude 100m. GM tube, Nai(TI) crystal. Coverage 18-20 km^2/h. Dose rate over 2-5 mGy/h. Count rate over 10-20 µGy/h.	Maps of dose rate at 1m for extended contamination. Localisation of ponctual sources and count rate maps.
Air sampling method [23]	capture of particles in the atmosphere	Volume filtered per unit of time, threshold of concentration detected.	Qualitative and quantitative information about air composition, punctual measurement or average value on a transect.

3. table. Summary about the sensors, detection principle, main capacities and end product

Disaster	Information	Technology and/or product
Earthquake	Building status (standing, collapsed, unstable) Road network status Research of survival	Oblique imagery. Classical RGB imagery. Thermal.
Tsunami	Building status (standing, collapsed, unstable) Road network status Research of survival Area dried ready for first response	Oblique imagery. Imagery, video. Thermal. Imagery, video.
Volcanic eruption	Detection of person to evacuate. Detection of active areas though the thermal activity, gas emission or through the changes in elevation. Gathering information about speed and direction of the lava, lahars, etc flows as well as terrain elevation, POI on the trajectory.	Imaging Thermal imaging, DIAL, LiDAR Imaging, LiDAR.
Avalanches	Location of buried persons. Zonation of impacted area. Zonation of infrastructure impacted. Endangered areas or persons, existence of unstable snow layer.	Thermal imaging (if victim close to surface). LiDAR, RGB imaging. LiDAR.
Floods	Impacted area. Volumetric data. Elevation data. Modeling	Ortho-images LiDAR (DSM, DTM)
Wildfires	Hot spots localization. Firefight efficiency assessment and guidance Change in fire direction, evolution of the situation	Thermal imaging Thermal imaging Thermal and imaging
Blizzards	Impacted infrastructure (road network to be cleaned).	RGB imaging or LiDAR
Cyclonic storms	Detection of person to evacuate. Building status (standing, collapsed, unstable) Road network status Research of survival	RGB imagery or thermal imaging Oblique imagery. Classical RGB imagery. Thermal.
Hailstorm	Impacted area. Impacted infrastructure. Intensity of damages.	RGB imagery
Heat waves	Temperature on the ground.	Thermal imaging.
Health disaster	Spread of diseases in vegetation, spread of invasive species, blooms (algae).	Hyperspectral (vegetation, algae).
Space disasters	Extent of impact Spread of radioactive substance Spread of toxic substance	RGB imaging. Aerial gamma spectrometry Hyperspectral
Civil disorder, terrorism and war	Impacted area, impacted infrastructure, victims, intensity of damages. Refer to fire, industrial, nuclear, CBRN.	Oblique imagery.
Industrial	Information about the localization, concentration of the contamination	Hyperspectral* Hyperspectral*, DIAL*. Hyperspectral* LiDAR (for elevation model in case of flooding risk).
Fire	Localization of hot spots, firefight work assistance	Thermal imaging.
Transportation	Pollution extent (oil spill, water contamination, air contamination)	LiDAR (for elevation data in case of flooding risk). Hyperspectral.
Nuclear	Intensity of contamination, type, location	Aerial gamma spectrometry.
CBRN	Type of contamination, extent.	DIAL [18] Hyperspectral imaging Air sampling.

4. table. with full relation catastrophe, information, technology/measurement method

CONSIDERING TIME OVER THE FULL WORK FLOW FOR THE ASSESSMENT OF AIRBORNE CAPACITIES

The previous part put into relation a type of disaster, the information relevant for its management and the associated airborne technology to mobilize to gather this information. Adequate information and appropriated means for the collection is not sufficient as regards to the catastrophe management situation. The second priority is the management of the time. As only a final product can be exploited in the management of disaster (3D model for LiDAR, thematic maps and ortho-photos for imagery) all the work flow (and associated cumulated time) leading to the delivery of the final product should be considered[3].

The following part introduces the workflow and all the aspects influencing time in an ortho-image production process. The choice is oriented towards ortho-imagery production as it is the most common and versatile reconnaissance product.

GSD depends on AAG

In the aerial data acquisition process, first a decision is made regarding the area to be flown. Secondly the project manager has to make a choice as regards to the quality of the data which in imagery means the size of pixels on the ground (GSD or spatial resolution). The GSD is governed by fixed sensors characteristics (FOV (related to the optics), number of pixels on the CCD array, size of the pixels) and the altitude of flight (the only adaptable entry).

AAG and FOV determine strip width which affects the flight time

Once AAG is fixed it is possible to position the flight lines over the AOI, making additional decision about the required overlay between frame footprints. The number of flight lines conditions the total flight time. All this work is assisted by software and a digital flight plan is issued at the end of this process.

In practice, and in particular in the case of disaster reconnaissance, rush data are targeted which result in a lower spatial resolution but favor production time with higher AAG.

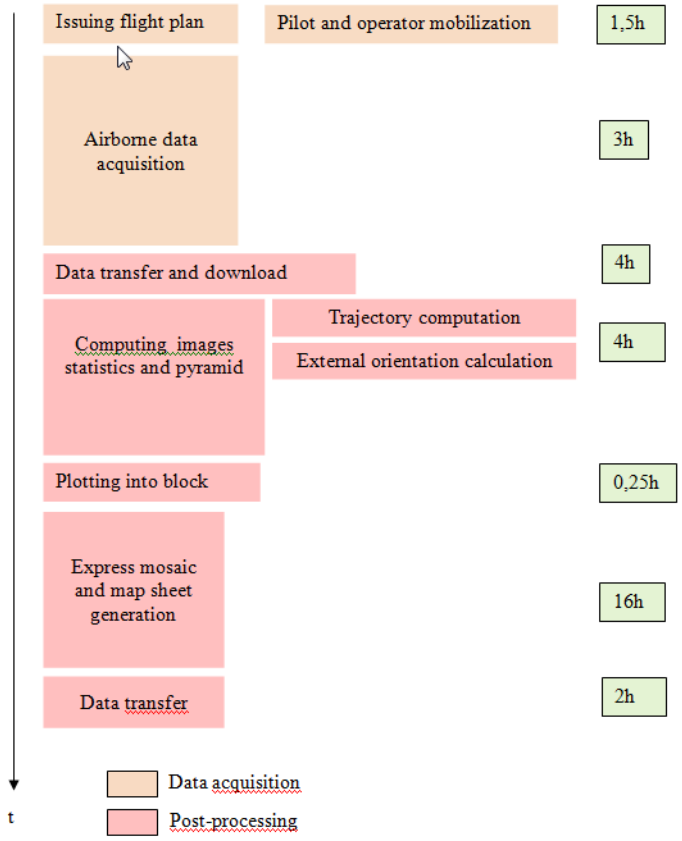
AAG affects file size which affects post-processing time.

The number of frames made over an area depends on the AAG and the associated number of flight lines. The size of the data is proportional to the number of frame for the image and to the time of flight for the trajectory data. The time of post-processing is directly related to the size of the dataset.

General ortho-image production workflow and timeline

The following scenario corresponds to the production of an express mosaic for the 776 frames of the Zala AOI presented in fig.2. The complete ortho-rectification with automatic point matching, bundle adjustments and the use of corrected DSM for ortho-rectification would require much more time. From the project planning to the delivery of the product a minimum time of 30h is required.

[3] The data generated by the sensor is usually in a raw format and it is not classified nor geocorrected, so it is not exploitable.



Advisory to produce table for each sensors or combination of sensors about operating time, spatial accuracy and post-processing time.

New solution that allow following the disaster in real time and mapping the POI on touch screen during the flight. [24] Those solutions are efficient for small areas.

SELECTION OF RELEVANT CASE STUDIES

The part aims at providing concrete and developed examples about the use of aerial reconnaissance means for a diverse selection of disasters.

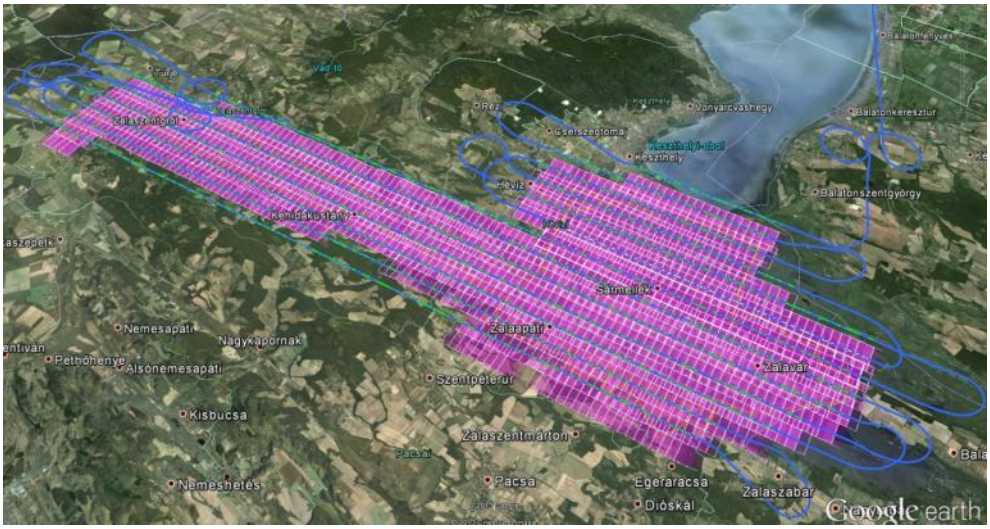
RGB imagery and LiDAR data for flooding reconnaissance (natural disaster)

This case study aims first at introducing aerial imagery, the reconnaissance mean the most versatile and the most generally used. Our second belief is to present information about flooding, a natural disaster that frequently happens. Because of its geophysical characteristic (flat land, rivers draining much extended surface abroad) Hungary is particularly exposed to flooding. Our team performed two aerial reconnaissance surveys on April the 16th over Zala and Kapos rivers right after the flooding event. The data acquisition was performed with a Cesna C-206 aircraft equipped with a Leica dual system for ortho-imagery and LiDAR (RCD30 medium format camera and ALS70 laser scanner). RGBN ortho-imagery with 15cm GSD was produced in combination with a 4-5 pt/m^2 density cloud of points.

Number of flight lines	**32**	**Average point density at NADIR**	**4 pt/m^2**
AOI total area	270 km^2	Expected vertical accuracy (LIDAR)	0,09 m
Length of flight	820 km	Expected accuracy (Ortho)	15 cm
Taxi time from base to AOI	0,25 h	Max flight altitude above ground	1300 m
Time to fly	5,7 h	FOV	54°
Number of frame	1833	Overlay between footprint	30%
Ortho GSD	15 cm	strip width	1325 m
Average point density	5 pt/m^2	Flight speed	185 km/h

5. table. Main characteristics of the flight for Zala and Kapos AIO

Fig.2. show the flight report over the Zala AOI. The airplane trajectory is represented with a blue line. The footprint of each frame is figured with a purple square. A total of 776 frames were taken in 3 hour (including taxi).



2. figure. Flight report over the Zala AOI

Fig. 3 shows a sample of territory affected by the flooding. Flooded areas can easily be identified visually on the picture (a) and (b). With the use of a dual system, the visual interpretation and digitalization of flooded areas can be replaced by an automatic classification using the low reflectance of laser beam by the water. This fusion is of high interest for the production of rush data on the extent of flood area. Additionally LiDAR elevation data is used as an input for hydrological model.

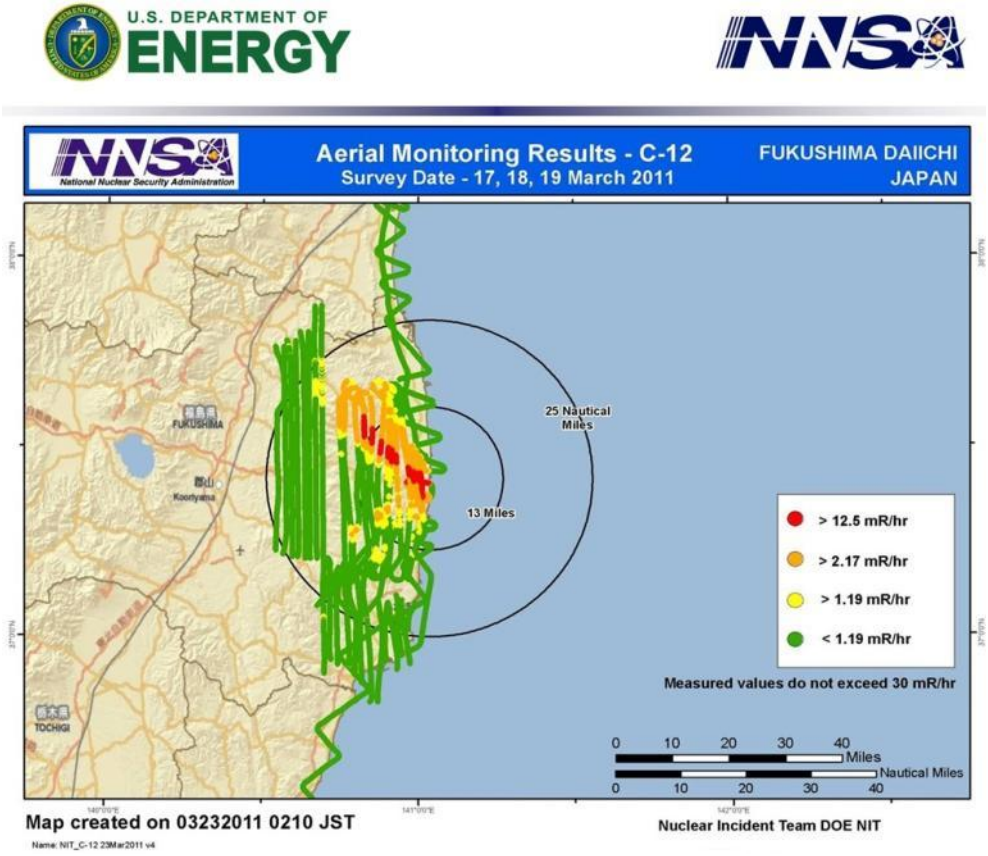
3. figure. Ortho image over a flooded area

Almost immediate gamma reconnaissance over an extended area after the Fukushima disaster (March 11, 2011)

With one nuclear power plant in Páks, several ones in the neighbor countries (a) and radiologic materials with long range travel capacities in the case of a serious accident, nuclear risk should be considered and associated reconnaissance capacities developed[4]. The catastrophe of Fukushima demonstrated how important the airborne capacity is.

On March 14, 2011 the US department of Energy (DOE) deployed a tailored Management Response Team (CMTR) and Arial Measuring System (AMS) capability using military airlift to Yokota Air Base. By March 17, the AMS had acquired a general picture of the level of contamination on the ground. [25] The flight operations were curtailed on March 22-23 due to weather conditions. On March 25, 2011the first radiological assessment report was issued.

The radiation data was collected with a fixed-wing aircraft (C-12), with an array of large thallium activated sodium iodide (NaI(T)) crystals and associated readout electronics to produce time and location referenced measurements. AMS data represented as exposure rate 1 meter from the ground at the time the measurement occurred. [26], [27] The map issued helped to affine the contour of the most impacted area, to guide the protection measures and to guide the next surveys for the monitoring of the radiological assessment.



4. figure. A map from March 25, 2011 report

The approach provided precise results within a short time over an extended area (mobilization on the 14th, and first results on the 17th). The delay which might be caused by the weather condition is an important point to consider for all the aerial survey.

[4] Hungarian defense force has equipped a helicopter with an aerial reconnaissance system (LABV)

Complementary use of multiple sensing aerial capacities on the red mud disaster (industrial disaster, October 4, 2010)

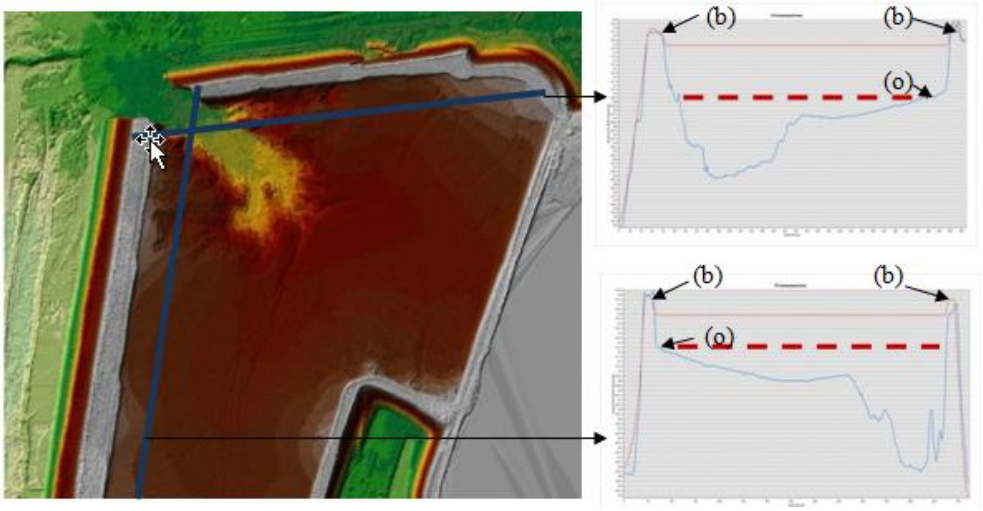
On October 2010, the embankments of an industrial reservoir located in Kolontár, Hungary failed and released a mixture of 1.1 million cubic meters of bi-product red sludge which flooded the settlements of Kolontár, Devecser and Somlóvásárhely. An interdisciplinary approach was necessary to tackle all the challenges lain by this totally unexpected event. Five different remote sensing systems were used. [28] Three of them are detailed below.

Aerial LiDAR survey was performed with a Leica ALS60 at 800m AGL in order to issue a final model with 4 pt/m^2 with a vertical accuracy of 10 cm. The objective of the survey was threefold:

- Collecting elevation data as input for hydrological modeling of the flooding,
- Collecting data for the 3D modeling of the reservoir
- Estimating the spilled volume (fig.5).

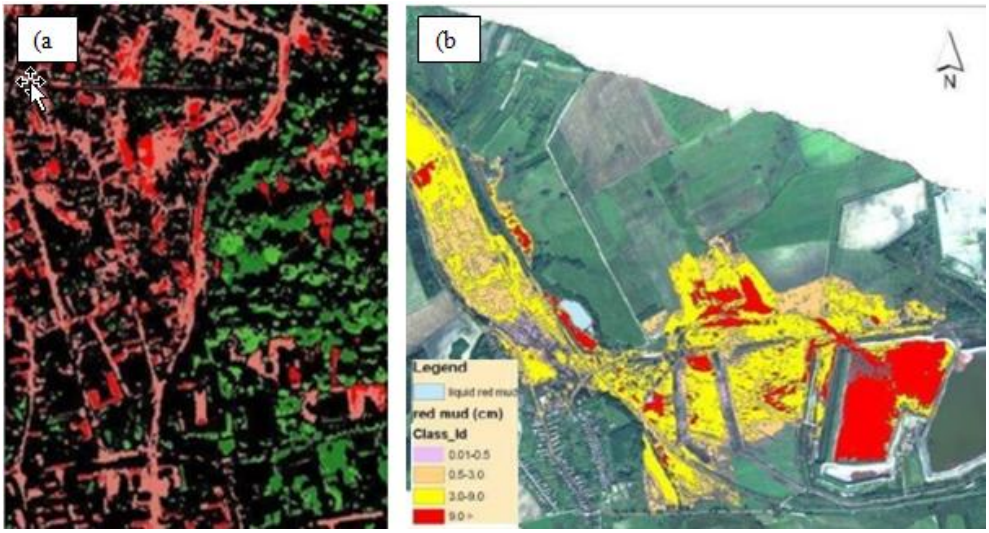
The calculation of the missing volume in the reservoir was done using LiDAR data in combination with stereoscopic measurement with aerial photography pairs. [28]

Fig.5. shows a 3D model (top view) and cross-sections where elevation data was plotted and analyzed. On the two graphs corresponding to the cross-sections, the borders (b) of the dam can easily be identified. The original level of decanted red mud originally stored in the reservoir can be estimated (o), last the level of red mud not decanted (red curve) was plotted. By issuing two DTM (before and after event) and calculating the volumic different it was possible to calculate the missing volume in the reservoir. Calculations gave a total volume of leaking approaching the 1,1 million of cube meters.



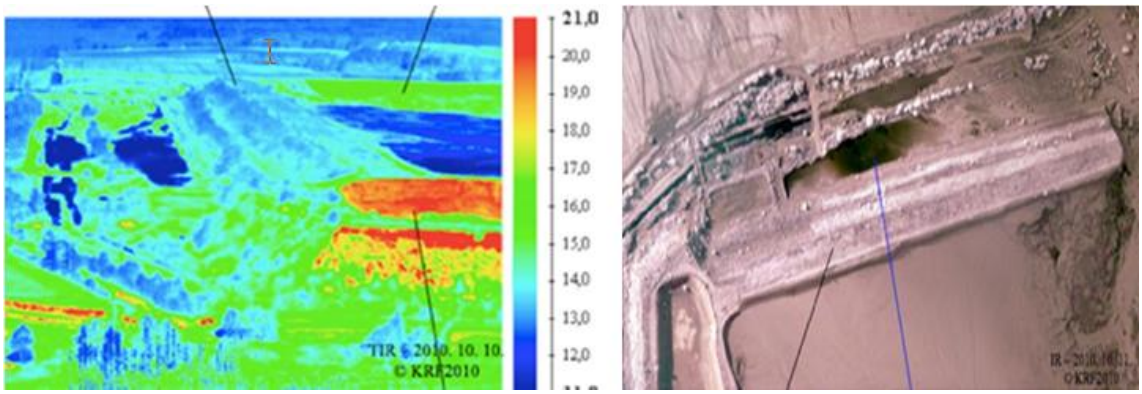
5. figure. 3D model of the reservoir from LiDAR data post-processing and profile lines for estimating the leaked volume

Hyperspectral flight was performed with an AISA Eagle imaging system at 1655m AGL with a corresponding GSD of 1,1m. 253 bands were collected in the 400-970nm region. After geometrical and radiometrical correction and pixel classification, the maps bellow were issued (fig.6.). [29] Those maps were used to guide and prioritize the cleanup work.



6. figure. Thematic maps about contamination zonation
(a) and red mud pollution thickness (b) from hyperspectral imaging

Thermal imaging (NIR, FIR) was applied in order to track invisible breaks and breach in the banks of the dam. Wet leaking areas were identified in the shot near the reservoir (fig.7.). Those clues allude to hidden cracks and leaks. The detailed examination of the whole dam was an important issue for the security of the post-damage work and ground work examinations. The thermal measurements made over a period of seven days allow determining which parts were intact and can be used for moving or could be approached safely. [30]



7. figure. Thermal images (FIR and IR) showing leaks and humid patches

Conclusion

The diverse aerial reconnaissance done on the red mud disaster demonstrated how rich and diverse the field of application of aerial surveying technology can be. Two facts are very important to mention. First, it demonstrated the advantage to use different sensors to provide complementary information on different thematic areas related to the same disaster (status of the dams: detection of hidden cracks, detection of water infiltration, calculation of the volume of the leak; environmental status: extent of the flooded area, thickness of the red sludge layer, wetness status). As a second important fact - considering this event was unique in the history and the research teams who carried out the reconnaissance had neither prepared nor methods ready beforehand - they demonstrated they were able to adapt quickly and produce within a short time new methods for the use of the technology and to produce adequate rush data. This also shows that the technologies are flexible enough to measure phenomena in new fields of application (hyperspectral, LiDAR).

Composite UAV/UAS case study built from diverse technological solutions

Presently UAV and UAS applications are increasing all over the world. The unmanned solution presents several advantages for disaster management, whether for their flight flexibility (approach, change of direction) or with the limitation of the risk for operators in extreme situations (catastrophe undergoing, health hazards, too important contamination, unknown contamination level). The following paragraphs derivate from the work of Adams (2012), summarizing the most recent application of UAV in disaster situation. [31]

Collecting information when physical access is compromised by the damages - damage survey of road network with UAV imagery and video

Several applications of UAV were done after earthquake (Haiti) and cyclone (Ike, Wilma, Katrina) to survey the damage on infrastructure and in particular on the road network. [32] UAV appeared as one of the most adapted solutions when site access is compromised. The survey was done using a helicopter UAV with digital camera system able to perform both imagery and video. The UAV was equipped with GPS in order to be able to guide it to an AOI and let it hover in place when the operator wanted more detailed analysis on a place.

Another case reported the use of Helicopter UAV after the typhoon Morakot in Taiwan. Imagery was captured; calibration, photogrammetric techniques and triangulation were applied to produce quality digital elevation DEM that helped in the disaster restoration and reconstruction work. [33]

Collecting information when physical access is compromised by contamination level – survey at Fukushima

In March 2011 the Fukushima-Daiichi nuclear facility was damaged after Japan was hit by an earthquake followed by a tsunami. Because of the high level of radiation after the melting of 3 reactors and because workers had to be as few exposed as possible exposed to the radiations, aerial monitoring with UAV was employed. A Air Force Global Hawk UAV was mobilized on the area. It was equipped with IR sensors and guided the operator in their attempts to cool the reactors. A T-Hawk Micro Aerial Vehicle equipped with radiation sensors completed the reconnaissance and help the operator to localize the nuclear fuel debris. The T-Hawk UAV could acquire video and imagery at lower altitude. [35], [36], [37], [38]

Similarly to the T-Hawk, three French helicopter UAVs were equipped with camera and radiation sensors to support the monitoring operations. The fleet of UAV employed in this situation demonstrates one more time the necessity to gather complementary information (IR, video, imagery and gamma spectrometry) and shows how the limitations inherent to UAV was tackled (flying time limited to one hour in average).

Rapid aerial mapping response with semi-automated or fully automated maps creation.

The last trend we would like to introduce is the fully automated or semi-automated map production. Several companies and research introduced the present capacity with live mosaicking from aerial images or videos. [39], [40], [24] POI can also the marked during the reconnaissance. With the use information system which transfer the information in real time from the UAV to processing center and from the centre to operators in the field, is it possible to guide almost immediately the field operators to the priority target.

CONCLUSION

The study demonstrated that starting from the exhaustive list of the types of disaster and looking for each which information is relevant to collect by aerial means; it is possible to find application or airborne remote sensing for almost all the types of disaster.

The choice of the technology is technically driven, starting from the information to be collected (one or several sources), defining the accuracy required and setting the operational parameters (AAG, ground speed). The study also showed that a couple of technologies (LiDAR, RGB imaging, thermal, and hyperspectral imaging) can be successfully employed to cover almost all types of disaster. This has a strategic importance for disaster reconnaissance capacity building. A body responsible for disaster management and equipped with such technologies can handle reconnaissance for most of the situations.

Progress not only with the acquisition technology but also with processing capacities should be mentioned. The information support process should be considered as a whole because no deficiency (and delay) can be accepted in the case of catastrophe management. The apparition of live mosaicking and live transfer of information allow more flexibility and immediate response.

The case studies - selected to shows the most up to date trends - demonstrated that the combination of sensors for multi disciplinary approach is a key for a successful reconnaissance of disasters. Data fusion, dual sensors are becoming common. Another trend with the use of UAV/UAS allows more flexibility (with weather and with flight) and reduces the risks for the operator on extreme or risky disaster operation theatre. Real time information transfer, algorithm for real time geo-correction and the adaptation of the sensors to UAV platform will definitely reshape the reconnaissance approach in the coming years.

References:

[1] Regina Below, Angelika Witz, Debarati Guha-Sapir. Disaster Category Classification and peril Terminology for Operational Purposes. Université Catholique de Louvain. 20 p.

[2] Damienne Provitolo. A new classification of catastrophes based on “Complexity Criteria”. From System Complexity to Emergent Properties , Understanding Complex Systems 2009, pp 179-194.

[3] Halász L., Pellérdi R. Katasztrófavédelem, Zrínyi, 2010.

[4] J. Ramos, L. Marrufo, F.J. Gonzlez: Use of Lidar Data in Floodplain Risk Management Planning: The Experience of Tabasco 2007 Flood. "Advances in Geoscience and Remote Sensing", Gary Jedlovec, ISBN 978-953-307-005-6, Published: October 1, 2009.

[5] Halasz Laszlo, Pinter Istvan, Andrea Solymar Szocs: Remote sensing in the biological and chemical reconnaissance. AARMS, vol 1. Issue 1 (2002), 39-56.

[6] Development of a novel Airborne Differential Absorption Lidar System for the UK FAAM aircraft: http://www.npl.co.uk/environmental-measurement/research/airborne-differential-absorption-lidar

[7] NASA fact sheet about DIAL: http://www.nasa.gov/centers/langley/news/factsheets/DIAL.html

[8] H., Holma, A. J., Mattila, & T., Hyvärinen: New thermal infrared hyperspectral imagers. NATO Technical report, RTO-SET-151, 2009.

[9] R. Richter: Hyperspectral Sensors for Military Applications. Emerging EO Microsoft Phenomenology, 2005.

[10] ultracam imaging offer: http://www.microsoft.com/ultracam/en-us/ultracamproducts.aspx

[11] Leica aerial imaging products http://www.leica-geosystems.com/en/Airborne-Imaging_86816.htm

[12] Pictometry oblique imagery system: http://www.pictometry.com/index.php?option=com_content&view=article&id=76&Itemid=85

[13] Advantages of oblique imagery for disaster management http://geodatapoint.com/articles/view/what_makes_oblique_imagery_so_effective_for_disaster_response

[14] Airborne laser scanner devices by Leica: http://www.leica-geosystems.com/en/Leica-ALS70-Airborne-Laser-Scanner_94516.htm

[15] Airborne laser scanner devices by optech: http://www.optech.ca/prodaltm.htm

[16] Hyperspectral airborne imagers by SPECIM: http://www.specim.fi/index.php/products/airborne

[17] Hyperspectral AVIRIS system: http://aviris.jpl.nasa.gov/

[18] Thermography system by igi: http://www.igi.eu/digitherm.html

[19] IAEA: Guidelines for radioelement mapping using gamma ray spectrometry data, 2003.

[20] J. Zelenák, J. Csurgai: Analysis of the applicability of the airborne radiological reconnaissance in case of searching lost or stolen radioactive sources. Hadmérnök, (2009) 46-62.

[21] Gamma Zrt LABV - Airborne Nuclear Reconnaissance System. http://www.gammatech.hu/?module=products&site=main&group=teruletszerint_katasztrofavedelem&menupath=-teruletszerint_katasztrofavedelem&product=labv&lang=hun

[22] K. Kurvinen, P. Smolander, R. Pöllänen, S. Kuukankorpi, M. Kettunen and J. Lyytinen: Design of a radiation surveillance unit for an unmanned aerial vehicle. Journal of Environmental Radioactivity, 81(1) (2005) 1-10.

[23] R. Pöllänena, H. Toivonen, K. Peräjärvia, T. Karhunen, T. Ilander, J. Lehtinen, K. Rintala, T. Katajainen, J. Niemeläc, M. Juusela: Radiation surveillance using an unmanned aerial vehicle. Applied Radiation and Isotopes, 67(2) (2009) 340 – 344.

[24] Real time image mosaic solution: htt p://www.cloudcaptech.com/solutions/commercial_disaster_reconnaissance.shtm

[25] Paul Guss. DOE response to the Radiological Release from the Fukushima Dai-ichi Nuclear Power Plant. NEI RETS/REMP workshop. 2011

[26] Radiological assessment – March 25, 2011.

[27] US DOE/NNSA Response to 2011 Fukushima Incident- Raw Aerial Data and Extracted Ground Exposure Rates and Cesium Deposition https://explore.data.gov/Geography-and-Environment/US-DOE-NNSA-Response-to-2011-Fukushima-Incident-Ra/prrn-6s35

[28] J. Berke, V. Kozma-Bognár, L.D. Kováts, P. Burai, T. TOmor, T. Nagy, T. Németh: Applied information technology on remote sensing data investigation of red mud catastrophe. Informatika. Vol XIV. No. 2. p. 24-28.

[29] Cs. Lenart, P. Burai, A. Smailbegovic, T. Biro, Zs. Katona, R. Andricevic: Multi-sensor integration and mapping strategies for the detection and remediation of the red mud spill in Kolontar, Hungary: Estimating the thickness of the spill layer using hyperspectral imaging and Lidar, Hyperspectral Image and Signal Processing. Evolution in Remote Sensing (WHISPERS). 3rd Workshop, Lisbon, Portugal. (2011).

[30] Péter Burai, Smailbegovic, A., Lénárt Csaba, József Berke, Gábor Milics and Tibor Bíró, Preliminary analysis of red mud spill based on aerial imagery. AGD Landscape and Environment, 2011. 5(1): p. 10.

[31] J. C. Trinder, M. Salah: Aerial images and LiDAR data fusion for disaster change detection. ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume I-4, 2012.

[32] S. M. Adams, C. J. Friedland: A survey of unmanned aerial vehicle (UAV) usage for imagery collection in disaster research and management.

[33] Ji Ping Hu, Wen Bin Wu, Qu Lin Tan: Application of Unmanned Aerial Vehicle Remote Sensing for Geological Disaster Reconnaissance along Transportation Lines: A Case Study

[34] T. Chou, M. L. Yeh: Disaster Monitoring and Management by the Unmanned Aerial Vehicle Technology. ISPRS Technical Commission VII Symposium. W. Wagner and B. Szekely. Vienna, Austria, IAPRS. XXXVIII: 6 (2010).

[35] Erico Guizzo. Robotic Aerial Vehicle Captures Dramatic Footage of Fukushima Reactors. Posted 20 Apr 2011

[36] E. Ackerman: Japan Earthquake: Global Hawk UAV May Be Able to Peek Inside Damaged Reactors. Spectrum. IEEE (2011).

[37] B. Reavis, B. Hem: Honeywell T-Hawk Aids Fukusima Daiichi Recovery: Unmanned Micro Air Vehicle Provides Video Feed to Remote Monitors. Honeywell Aerospace Media Center. Honeywell International Inc. (2011).

[38] UAV helicopter send by HELIPSE: http://news.cnet.com/8301-17938_105-20051499-1.html

[39] C. Kyoungah, L. Impyeong: A UAV based close-range rapid aerial monitoring system for emergency responses. International Archives of the Photogrammetry, Remote Sensing and Spatial Information Science, Vol XXXVIII-1/C22 (2011).

[40] T. Suzuki, D. Miyoshi: Real time hazard map generation using small unmanned aerial vehicle. SICE Annula Conference (2008).

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Meglécz Katalin
meglecz.katalin@hm.gov.hu

BIOLÓGIAI BIZTONSÁG, KOCKÁZATKEZELÉS

Absztrakt

A biológiai biztonság napjainkban az orvostudomány eredményei ellenére is kiemelt kérdés. A biológiai védelem eszközrendszerét a kockázatokkal szembeni felkészültséget és reagáló képességet erősítő tevékenységek alkotják, a kockázatok azonosításától, azok elemzésén át a kockázatkezelésig, az Európai Unióban és globális szinten is.

The biosafety today is a matter of priority despite the results of medicine. Preparedness and response capabilities constitute the reinforcement of the equipment of biological protection against the risks from the identification of risks, through their analysis, to the risk management in the European Union and globally too.

Kulcsszavak: *biológiai fenyegetés, surveillance, bioterrorizmus, kockázatbecslés, kockázatkezelés ~ biological threat, surveillance, bioterrorism, risk evaluation, risk management*

BEVEZETÉS

A biológiai fenyegetettség jelentős kihívást jelent bármely ország számára. Ha a biológiai veszélyről beszélünk, három forrásból származó fenyegetéssel kell a biológiai védelemnek szembenéznie – ezek a természetes fertőzések és járványok, a bioterrorizmus, és más államok fenyegetése, a biológiai fegyver alkalmazásának lehetősége.

BIOLÓGIAI FENYEGETÉS

Az emberiséget történelme során mindig sújtották a járványok, fertőző megbetegedések. A XX. század végére úgy tűnt a fejlett világ legyőzheti ezeket. Az orvostudomány fejlődésével, a betegségek hatékony megelőzési stratégiáinak, a közegészségügyi-járványügyi intézményrendszernek és rendszabályoknak világméretű elterjedésével, a védőoltások bevezetésével csökkent a fertőző megbetegedések szerepe a fejlett világban.

Mindezek ellenére a fertőzések okozta mikrobiológiai veszély ma is valós fenyegetés. Napjainkban, Európában az összes megbetegedés 10 %-át még mindig a fertőző megbetegedések adják, melyek fokozott kihívást jelentenek az egészségügy és az államok számára. [1] A humán kórokozók jelentős számú megbetegedést okoznak, és ennek következtében kiemelt gazdasági terhet jelentenek globálisan. Ide sorolhatók a személyről-személyre terjedő akut fertőzések, az egészségügyi ellátással összefüggő fertőzések, az élelmiszerrel terjedő fertőzések, a vektorral terjedő fertőzések, a krónikus fertőzések, és a fertőzés által indukált daganatos megbetegedések. [2] Súlyos problémát okoznak az egyre sokoldalúbb formában jelentkező antibiotikum-rezisztenciák, valamint az újra és újonnan felbukkanó fertőzések fenyegetése (az emerging infections), a globalizáció és az utazások, a tömegrendezvények biztonsága. Ezek a tényezők a mai helyzetben egy sajátos járványügyi helyzetet teremtettek, ahol a fertőző ágensek rövid idő alatt nagy számú fogékony egyedet találhatnak, akár egymástól nagy távolságra is és ezáltal robbanásszerű terjedésük is bekövetkezhet. Az ilyen megbetegedések, járványok példái lehetnek a SARS megbetegedések 2003-ban, a németországi EHEC járvány 2011-ben, vagy a malária, dengue megbetegedések újra előretörése.

A biológiai terrorizmus - amikor a terrorcselekményt betegséget okozó biológiai organizmusok felhasználásával hajtják végre - sem új keletű jelenség. A Monterey Nemzetközi Tanulmányok Intézetének Tömegpusztító Fegyverek Elterjedését Megakadályozó Tanulmányok Központja (US, Kalifornia) 1999-ben és 2003-ban megjelent jelentéseinek megfelelően a XX. században regisztrált terrorcselekmények (417 esemény) közül 1999-ig 130 ABV, ebből 65 biológiai, 2000-ben 26, 2001-ben 607 bioterror eseményt regisztráltak a riasztásokkal együtt [3, 4].

Ágens	**esetek száma/riasztás**		
	1909-1999	**2000**	**2001**
biológiai	95	26/22	607/600
vegyi	65	24/0	12/1
nukleáris	5	2/0	4/2
radiológiai	5	17/3	2/0
kombinált	0	0	3/0
ismeretlen	5	4/0	0

1. ábra. Monterey report I-II. 1999-2003

Az Amerikai Egyesült Államokban 2001. szeptember 11-én bekövetkezett terrortámadás és az azt követő anthrax-tartalmú levelek, valamint az Irak megszállását követő terrorhullám arra

késztette a politikai vezetőket és elemzőket, hogy értékeljék újra egy tömeges áldozatokat szedő biológiai terrortámadás valószínűségét és veszélyeit. Hírszerzői információk alapján mára egyértelművé vált, hogy reális egy biológiai terrortámadás veszélye.

Természetesen a veszély mértéke országonként változik. Elsődleges célponttá vált az USA és a terrorellenes harcban résztvevő főbb szövetségesei, például Nagy-Britannia és Izrael. Azok az ázsiai országok, ahol nagyszámú muzulmán kisebbség küzd önálló államiságért – például Malajzia – szintén nagyobb mértékben veszélyeztetettek. A NATO-tagállamok, mint az USA stratégiai partnerei szintén elsődleges célpontokká váltak. Elég csak a Madridban és Londonban elkövetett, nagy számú sérültet és halálos áldozatokat követelő merényletekre gondolni.

Annak ellenére, hogy a támadásoknak csak csekély százalékában használtak biológiai hatóanyagot, az utóbbi időben riasztó tendencia mutatkozik a biológiai terrorfenyegetés három fontos dimenziójában, a motiváció, a szervezeti kérdések és a technikai képességek területén egyaránt [4]

A hagyományosnak tekintett biológiai fegyver alkalmazásának veszélye a legalacsonyabb annak ellenére, hogy a biológiai fegyverek alkalmazására évszázadokra visszamenőleg találhatunk utalásokat a történelmi dokumentumokban. A biológiai hadviselés már a középkorban megkezdődött, és napjainkig nyomon követhető [3, 4]. A tudományok fejlődésével azonban a XX. században került előtérbe a tömegpusztító fegyverek másik két nagy csoportja, a nukleáris és a vegyi fegyverek, majd ehhez csatlakoztak a radiológiai fegyverek is. A CBRN körből a „B”, biológiai fegyverek háttérbe szorultak. Ez annak ellenére következett be, hogy a biológiai fegyver viszonylagosan egyszerű a vegyi, nukleáris és radiológiai fegyverek komplexitásához, speciális szakértelmet és jelentős anyagi ráfordítást követelő előállításához képest.

Ennek a háttérbe szorulásnak több oka is lehetséges, egyfelől az Amerikai Egyesült Államok és Nixon elnök nyomására megszületett a Biológiai és Toxinfegyver Tilalmi Egyezmény (BTWC, 1972), és a nemzetközi diplomáciában a nukleáris és vegyi fegyverek betiltását előkészítő egyezmények kerültek előtérbe. Másfelől a keleti blokkban egy kifelé mutatott viszonylagos érdektelenség látszott a biológiai fegyverek vonatkozásában, ami a mai ismereteink szerint egy igen intenzív kutatási és fegyverkezési program leplezésére szolgált. Harmadik lehetséges okként vetődik fel a biológiai fegyver elleni védekezés komplex és költséges volta, amely nem áll arányban az előállítás költségeivel és a komplexitás – interdiszciplinalitás jelentősen megnehezíti ezt a feladatot. További okként említik a biológiai fegyverek sajátosságait, mint a késleltetett hatást, a környezeti tényezőktől való függőséget, amelyek katonai szemmel nehezen meghatározható hatásfokúvá teszik ezeket a fegyvereket. Felmerül még a humanitás kérdése, a visszatartó erő a pusztítás lehetséges mértéke miatt [3].

Véleményem szerint még egy lehetséges magyarázata van a biológiai fegyverek háttérbe szorulásának, amely a reguláris haderők jellemzőjéből fakad. Az ABV, majd a CBRN védelemre kiképzett erők állományának összetételéből, szemléletéből, kiképzéséből, feladatrendszeréből adódóan marginálisan kezeli a biológiai fegyverek elleni védelmet. A vegyivédelmi alakulatok állományában mérnökök és technikusok, vegyész és radiológus szakemberek teljesítenek szolgálatot, orvos, biológus csak külső szakértőként, esetenként kerül a feladatok ellátásába bevonásra. Ennek megfelelően a NATO-n belül is, biológiai fegyverrel szemben megfogalmazódnak olyan elvárások, mint a könnyű detektálhatóság, azonnali felismerés, detektálás („biológiai doziméter”), amelyek a biológiai fegyver jellegéből fakadóan a kor mai ismeretei szerint szinte lehetetlen teljesíteni. A 2002. évi prágai NATO csúcstalálkozón került megfogalmazásra a komplex, laboratóriumi háttérrel támogatott CBRN védelem szükségessége, amely az egészségügyi szolgálatokkal való szoros együttműködést és egyre erőteljesebb szemléletváltást eredményezett.

BIOLÓGIAI ÁGENSEK

A természetben előforduló mikrobiológiai ágensek veszélyességük szerint 4 BSL (Bio Safety Level) csoportba – BSL1-BSL4 – vannak besorolva. A BSL szint mutatja meg bármely a kórokozóval kapcsolatos tevékenység kockázatát. A BLS1 osztályú kórokozók nem humán kórokozók, rendkívül alacsony kockázattal. A BSL2 kórokozók a humán patogének, melyek közepes vagy alacsony közösségi kockázatot okoznak és közepesen súlyos betegségekért felelnek. A BSL3 kórokozók súlyos, vagy halálos humán megbetegedést okoznak közepes társadalmi kockázat mellett. A BSL4 szintű kórokozók az emberi kórokozók azon kategóriája, melyek súlyos vagy halálos megbetegedéseket okoznak magas közösségi kockázat mellett. [5] A különösen veszélyes fertőző megbetegedéseket okozó élő ágensekkel csak a megfelelő biztonsági besorolású, különleges védelemmel rendelkező laboratóriumokban végezhető diagnosztikai valamint kutatási tevékenység.

A kiemelt jelentőségű biológiai fenyegetések potenciális kórokozói a BSL 3-4 szintű kórokozók közül kerülnek ki, ezért ezek az elsődleges célpontjai a megelőzésnek és a közegészségügyi szakpolitikának országos, EU és nemzetközi szinten. A járványügyi potenciállal bíró betegségek gyors és nagyarányú növekedést okozhatnak a morbiditásban[1] és mortalitásban[2], valamint társadalmi és gazdasági zavarokat generálhatnak, és ezért jelentős nemzetközi aggodalomra adnak okot. [2]

A BIOLÓGIAI VÉDELEM ESZKÖZEI

A hatékony biológiai védelem megköveteli az egészségügyi tevékenység pontos, időben történő végrehajtását, ideértve az egészségügyi felderítést a tervezést, megfelelő surveillance[3] rendszer működtetését, az irányítást, szükség esetén egészségügyi kiürítést, a betegek irányítását és követését, az egészségügyi anyagellátást. A biovédelem gyakorlati eszköztárába tartoznak a kockázatokkal szembeni felkészültséget és reagáló képességet erősítő tevékenységek, amelyek – különösen az EU-n belül – magukban foglalják a válságkezelésre vonatkozó intézkedések és stratégiák kidolgozását, a globális kommunikációs rendszerek létrehozását, a megelőzésre, kezelésre és a károk enyhítésére vonatkozó szaktanácsadás nyújtását, egészségügyi kockázatfelmérések készítését, és a vegyi, biológiai, radiológiai és nukleáris kockázatokkal kapcsolatos kutatások támogatását.[5]

A válságkezelésre vonatkozó intézkedések sorában a legjelentősebb a WHO/Egészségügyi Világszervezet által 2005-ben elfogadott Nemzetközi Egészségügyi Rendszabályok (International Health Regulations). Célja egy esetleges nemzetközi horderejű közegészségügyi szükséghelyzetben a védekezés a betegségek nemzetközi terjedésével szemben olyan módszerekkel, amelyek arányosak a veszélyekkel, és nem okoznak szükségtelen zavarokat a nemzetközi kereskedelemben és a közlekedésben.

A WHO 1951-ben fogadta el az első Nemzetközi Egészségügyi Rendszabályokat (*International Sanitary Regulations*), amit azóta átneveztek (*International Health Regulations*) és többször módosítottak, legutóbb és legátfogóbban 2005-ben.

A NER alkalmazási köre kiterjed biológiai kórokozók, vegyi és radionukleáris ágensek által előidézett, továbbá ismeretlen eredetű eseményekre. Hatálya alá tartoznak: a nemzetközi

[1] Az egyes betegségeknek egy adott populációban megfigyelhető gyakoriságára vonatkozó adat (100 000 főre / év)

[2] Az egyes betegségek okozta halálozás egy adott populációban megfigyelhető gyakoriságára vonatkozó adat (100 000 főre / év)

[3] Olyan folyamatosan működő egészségügyi információs rendszer, amely standardizált definíciók és módszertan alapján validált kritériumok szerinti adatgyűjtést, elemzést, értelmezést, visszacsatolást és intervenciót tesz lehetővé

forgalomban részt vevő személyek, poggyász, rakomány, konténer, szállítóeszköz, áru, postacsomagok, emberi maradványok akik/amelyek fertőzöttek vagy szennyezettek, vagy a fertőzés vagy szennyezés forrását hordozzák, és ezáltal közegészségügyi kockázatot jelentenek. Egységesíti a nemzetközi reptereken, kikötőkben és egyes szárazföldi átkelőhelyeken alkalmazott közegészségügyi rutineljárásokat is. A NER megbízza az egyes országokat, hogy alakítsanak ki képességet az ilyen veszélyek detektálására és elszigetelésére. Az átfogó és jól integrált epidemiológiai és mikrobiológiai surveillance és riasztórendszerek kulcsfontosságú elemei az ilyen veszélyekre történő felkészülésnek [2]

A NER minden részes államra nézve kötelező erejű nemzetközi jogi eszköz. A NER szabályait hazánkban az Egészségügyi Világszervezet Nemzetközi Egészségügyi Rendszabályainak kihirdetéséről szóló 2009. évi XCI. törvény léptette hatályba.

JÁRVÁNYÜGYI KOCKÁZATELEMZÉS

A biológiai veszélyek és különösen a kiemelten veszélyes kórokozók elleni védekezés és felkészülés meghatározott intézkedések sorozatát kívánja meg. Az intézkedéseknek – a veszélyhez képest, amelyet minimalizálni kívánnak, illetve amelyre válaszul születnek – arányosnak, megfizethetőnek, fenntarthatónak és megbízhatónak kell lenniük. [6] A megfelelő intézkedések kidolgozásában játszik szerepet a kockázatok becslése, elemzése és értékelése. Ennek érdekében elengedhetetlenül szükséges lépések a veszély azonosítása, a hatás és expozíció összefüggésének elemzése, a várható expozíció becslése, majd ezek figyelembe vételével a kockázatok jellemzése.

A járványügyi kockázatelemzés egyesíti a járványtan ismereteit, a kockázatelemzés metodikáját és a bizonyítékokon alapuló orvoslás eredményeit. A járványok esetében az előre történő tervezés és felkészülés időt takarít meg a védekezés időszakában, mellyel a járványfolyamat lefolyása jelentősen befolyásolható. Ezért kulcsfontosságú a gyors kockázatbecslés az adott helyzetben.

A járványügyi kockázatbecslés már a krízishelyzetre való felkészülés időszakában megkezdődik az információk, adatok gyűjtésével, elemzésével a releváns szakirodalom tanulmányozásával, a járványügyi surveillance adatok elemzésével és értékelésével. A releváns járványügyi helyzetértékeléséhez ellenőrzött rész-, és háttér információk beszerzése szükséges, amely a járványügyi vizsgálat és adatgyűjtés révén szakértők által valósul meg. [7]

Az Európai Unióban a tagállamok működtetik az egészségügyi ellátó, közegészségügyi és nemzeti surveillance rendszereket, amelyek különböznek a jogi alapot, szervezeti modellt, finanszírozási forrást és a regionális hatósági jogköröket illetően. Hasonlóan, az elsődleges diagnosztikai és a másodlagos referencialaboratóriumi szolgáltatások jelentősen eltérnek a tagállamokban, szervezeti modelljeikben, az alkalmazott diagnosztikai vizsgálati módszereikben, a fejlett jellemzés érdekében, a másodlagos szintre utalt minták arányában, a referencia vizsgálati módszerek alkalmazásában, valamint a nemzeti és a nemzetközi surveillance hálózatokban való részvételt illetően. [2]

Hazánkban a járványügyi surveillance rendszer részeként mintegy 80 fertőző betegséget kell kötelezően jelenteni, míg ez a szám más uniós országokban átlagosan 45. A fertőző betegségekre vonatkozó adatok gyűjtése online adatbázisban történik. A ritka betegségeket az Országos Epidemiológiai Központban diagnosztizálják. Az egészségügyi ellátó rendszer orvosai – az ún. észlelő orvos – a halmozódó esetekről, jogszabályban[4] külön megjelölt megbetegedésekről telefonon is jelentést tesznek.

Az EU a Fertőző Betegségek Hálózata[5] révén, 1999-ben összekapcsolta az EU tagállamok egészségügyi hatóságait, az Európai Bizottságot és a nemzetközi partnereket, koordinálva az

[4] 63/1997. (XII. 21.) NM rendelet a fertőző betegségek jelentésének rendjéről
[5] 2119/98/EK határozat

EU surveillance-t és kialakította a korai riasztó és reagáló rendszert (EWRS) [6]. A rendszer 49 fertőző betegséget, az egészségügyi ellátással összefüggő fertőzéseket és az antimikrobiális rezisztenciát foglalja magában, amelyek listáját rendszeresen aktualizálják amint új betegségek jelennek meg[7].

Az Európai Unió biovédelmi stratégiája részeként 2005-ben megalakításra került az Európai Betegségmegelőzési és Járványügyi Központ, az ECDC[8], amely előírt feladatának megfelelően, azonosítja és értékeli a fertőző betegségek által az emberi egészségre jelentett fennálló és újonnan megjelenő veszélyeket, valamint tájékoztat ezekről. Az ECDC hosszú távú[9] surveillance stratégiát dolgozott ki az egységes, központosított, integrált európai surveillance rendszer kiépítésének érdekében, az ECDC és a tagállamok epidemiológiai és mikrobiológiai szakemberei szoros együttműködésében, a betegség-hálózatok és azok koordinációs csoportjainak megszervezésével. Ez az eredmény jelentős mértékben fokozza a surveillance adatok hatékonyságát, hozzáférhetőségét és összehasonlíthatóságát, és biztosítja az európai surveillance rendszer fenntarthatóságát. [2]

A megfelelő, közel valós idejű surveillance rendszer adja az alapját a biológiai kockázatok becslésének. A fertőző megbetegedések monitorozásával kialakul egy, az adott területre, országra vagy régióra jellemző járványügyi adatbázis, amely az adott területen előforduló és endémiás[10] betegségekről azok szintjéről, típusáról, szezonális előfordulásáról tájékoztat. Természetesen nem csak az egészségügyi ellátó hálózat alapvető működéséhez, fertőző megbetegedések és járványok megelőzéséhez szükséges intézkedések kidolgozásához, a kötelező és ajánlott védőoltások bevezetéséhez szolgáltat alapot a rendszer, hanem az alapszintet meghaladó, a szokásostól eltérő fertőző megbetegedések felbukkanásáról, azok halmozódásáról is tájékoztat, megalapozva ezzel az időben bevezetendő intézkedéseket a tömeges megbetegedések elkerülése érdekében.

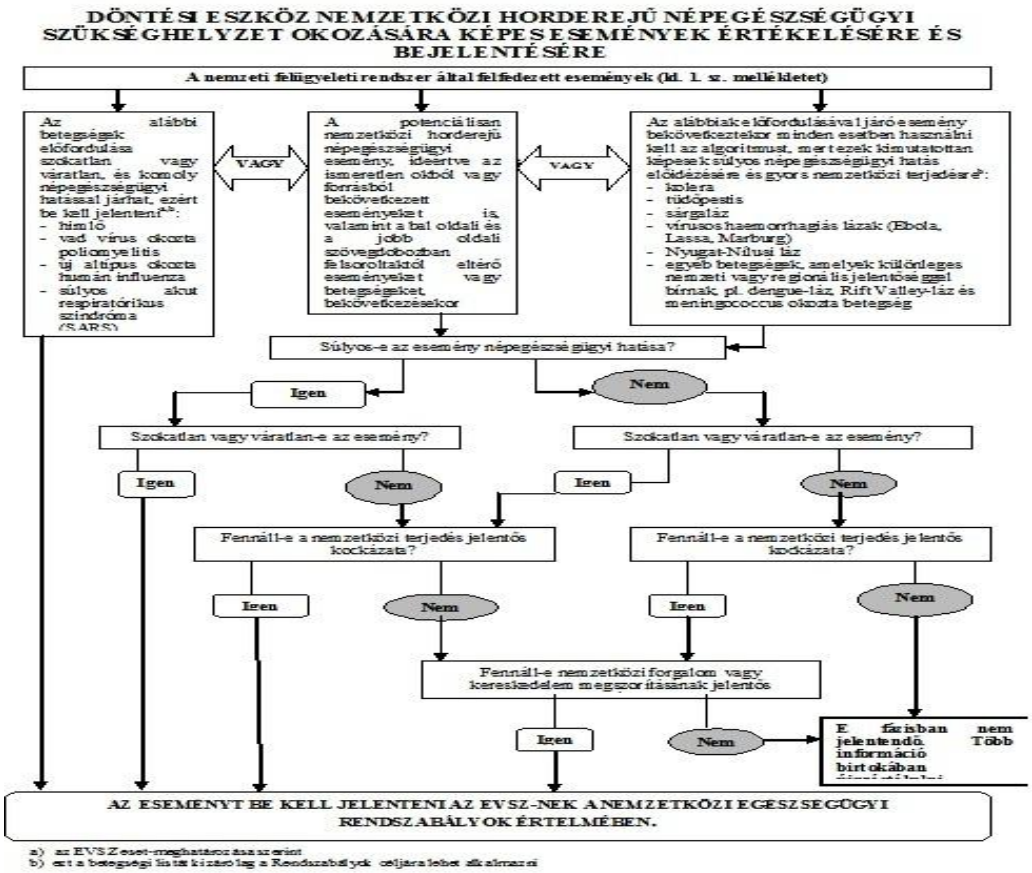
Az közel valós idejű surveillance rendszer fontosságát szemlélteti pl. anthrax az expozíciót követően a lappangási időben biotechnológiai módszerekkel kimutatva a kórokozót a megbetegedések közel 100 %-a, szindróma alapú korai riasztási rendszerekkel mintegy 70%-a, hagyományos surveillance rendszer, mintegy 30 %-a, klinikai diagnózist követően mintegy 12 %- a kerülhető el az eseteknek. [8]

A veszély, biológiai kockázat beazonosítását, detektálását követően lehetségessé válik a kockázatok értékelése. A kockázatbecslés és értékelés módszertana WHO NER 2005 dokumentumában is megjelenik. Az új szabályzat értelmében a tagállamok kötelesek jelenteni, ellenőrizni és reagálni bármilyen eseményre, amely nemzetközi szempontból potenciálisan népegészségügyi vészhelyzet jelenthet. A változás az újfajta nemzetközi egészségügyi veszélyekkel szembeni aggodalmakat tükrözi, és annak tényszerűségét, hogy az új betegségek éves gyakorisággal jelentkeznek. Az új nemzetközi egészségügyi szabályzat kiterjeszti a tagállamok szerepét és felelősségét, és négy fő kötelező feladatot szab meg. Országos NER tájékoztató központ (focal point)[11] létrehozását, amely az év 365 napjában rendelkezésre áll hivatalos információk cseréjére a világszervezettel, országos tervezet kidolgozását a felügyelet és válaszadás terén történő kapacitásépítésre, a laboratóriumi kapacitás megújítását a veszélyes kórokozók azonosítására és végül kapacitás fejlesztését a terepszemle, a társadalmi mozgósítás és az esetmenedzsment terén.

[6] Early Warning and Response System; 2000/57/EK határozat
[7] 2000/96/EK határozat
[8] European Centre of Disease Prevention and Controll
[9] 2007-2013
[10] Bizonyos földrajzi helyhez kötött állandó járványos megbetegedés rendszeres és tömeges előfordulása.
[11] A Részes Államok által kijelölt nemzeti központ, amely folyamatosan hozzáférhető a Rendszabályok előírásai szerinti EVSZ NER kapcsolattartó központokkal való kommunikáció céljából. Hazánkban az ÁNTSZ OTH Gyorsreagálású Főosztály.

Az új nemzetközi egészségügyi szabályzat tartalmaz egy döntéstámogató eszközt is, amely segítségével az országok meghatározhatják, hogy egy esemény nemzetközi szempontból népegészségügyi veszélyt/kockázatot jelent-e.

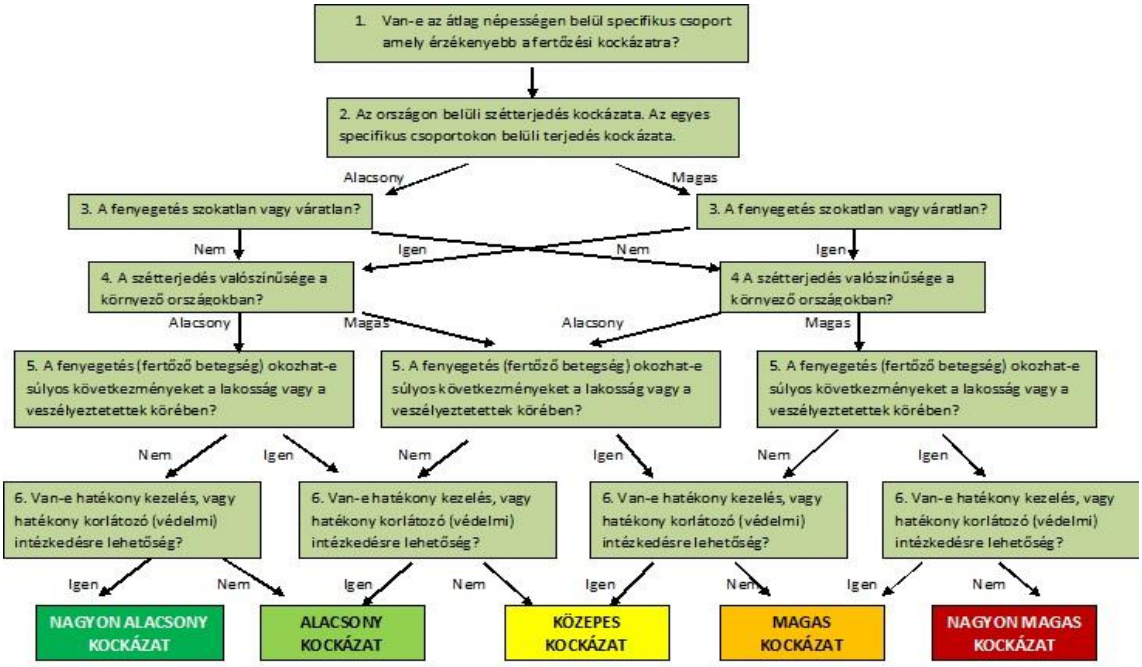
A NER szerinti népegészségügyi kockázat az emberi populációk egészségére károsan ható esemény valószínűsége, különös hangsúllyal azon az eseményen, amely nemzetközileg terjedhet, vagy amely súlyos és közvetlen veszélyt okozhat. A jelentésre kötelezett esemény kapcsán a WHO főigazgató dönti el a kapott — elsősorban attól a Részes Államtól, amelynek felségterületén az esemény bekövetkezett —információk alapján, hogy egy esemény nemzetközi horderejű népegészségügyi szükséghelyzetet jelent-e a Rendszabályokban megállapított követelmények és eljárás szerint. Annak eldöntéséhez, hogy egy esemény nemzetközi horderejű népegészségügyi szükséghelyzetet jelent-e, a főigazgató figyelembe veszi a Részes Állam által közölt információkat; a NER a 2. sz. mellékletében található döntési eszközt; a szükséghelyzeti bizottság szakvéleményét; tudományos elveket, továbbá a rendelkezésre álló tudományos bizonyítékokat és egyéb vonatkozó információkat; valamint az emberi egészségre jelentett kockázat, a betegség nemzetközi terjedésének kockázata és a nemzetközi forgalom megzavarásának kockázata kiértékelését. Ezen döntési mátrix szerint kerültek meghatározásra és kihirdetésre 2009-ben az influenza világjárvány fokozatai a megfelelő intézkedések meghozatala érdekében. [9]



2. ábra. IHR 2. sz. melléklet

2010-ben az EWRS kiegészítése céljából kockázatkezelési kérdésekkel foglalkozó, új kockázatértékelési platform kezdte meg működését az ECDC-ben. 2011-ben kidolgoztak egy gyors és hatékony kockázatbecslési módszert. A gyors kockázatelemzési módszer a szakmai bizonyítékra alapozva, kérdőívek és döntési algoritmusok használatával alapozza meg az egyes járványhelyzetek kezelését, és lehetővé teszi a szükséges intézkedések bevezetését a

járványfolyamat kezelése érdekében. A döntési mátrix nem csak az EU-n belüli eseményekre használható, hanem hatékony egyéb, nemzetközi jelentőségű események értékelésében is. [7]



1. sz. ábra ECDC gyors kockázatelemzési mátrix

A bemutatott döntési mátrixok használatának segítségével a járványügyi riasztási rendszereken keresztül beérkező adatok azonosításával történik meg a veszély felismerése. A releváns járványügyi helyzetértékeléséhez ellenőrzött rész-, és háttér információk beszerzése szükséges, amely a járványügyi vizsgálat és adatgyűjtés révén szakértők által valósul meg. A beérkező adatok függvényében a kockázatelemzés újra és újra lefuttatásra kerül, eredményének megfelelően módosíthatók a szükséges intézkedések, így elérhető, hogy csak a az elengedhetetlen, de szükséges intézkedések kerüljenek bevezetésre és elrendelésre, ugyanakkor elérhető legyen a kirobbanó, vagy készülőjárványok társadalmi-gazdasági hatásának mérséklése.

ÖSSZEFOGLALÁS

A fertőző megbetegedések által kiváltott hatás, a társadalom biztonságának fenyegetettsége ma is jelentős és fennáll. A biológiai védelem érdekében hatékony intézkedések és döntések rendszerének szükségességét felismerve került aktualizálásra 2005-ben a WHO Nemzetközi Egészségügyi Rendszabályok. Az Európai Betegségmegelőzési és Járványvédelmi Központot 2005-ben azzal a céllal hozták lére, hogy megerősítsék Európa fertőző betegségekkel szembeni védelmét. Célja az EU intézményeivel és a tagállamokkal együttműködve a tudományos bizonyítékokon alapuló, a fertőző betegségekkel szemben a lehető leghatékonyabb védelemben, a legújabb megelőző és ellenőrző intézkedések által. Az Európai Unió tudományos intézményeként működő központ kockázatértékeléseket végez, és tudományos bizonyítékokat szolgáltat az EU és a tagállamok politikai döntéshozói számára. Ugyanakkor közvetlen, tevékeny szerepet is játszik Európa betegségek elleni védelmében. Az európai szakértők az egészségügyi rendszereket kulcsfontosságú komponensnek tartják az egészségügyi káros események és lehetséges egészségbiztonsági vészhelyzetek esetén. Egy gyenge, felkészületlen egészségügyi rendszer problémát jelenthet a válaszadási láncban ez által gátolva a hatékony és gyors válaszreakciót. Egy erős, jól felkészült és jól működő egészségügyi rendszer meggátolhatja, hogy egy egészségügyi káros esemény globális krízis

helyzetet okozzon. A járványok elleni védekezés, a tervezés és a felkészülés és a járványhelyetek kezelésére, végül felszámolására, kiemelt szerepet kap a járványtani alapokon nyugvó kockázatbecslés és elemzés, amelyen alapuló intézkedések a kirobbanó járványok társadalmi-gazdasági hatását jelentősen csökkenthetik.

Felhasznált irodalom

[1] What Europe should be doing about infectious diseases, European Academies Science Advisory Council, EASAC közlemény, 2011. 04. 06.
http://www.easac.eu/home/press-releases/detail-view/article/what-europe.html
Letöltés ideje: 2012. 09. 10.

[2] ECDC – Updated Public Health Microbiology Strategy & Work Plan 2012-2016 Annex I: Background and milestones in EU public health microbiology, 2007-2011

[3] Dr. Faludi Gábor: A biológiai fegyver és az ellene való védelem – biovédelem (orvosi) kérdései, Doktori értekezés, ZMNE Katonai Műszaki Doktori Iskola, 2011. 11. 28.
http://193.224.76.4/download/konyvtar/digitgy/phd/2011/faludi_gabor.pdf
Letöltés ideje: 2011. 11. 10.

[4] Török Ervin: A bioterrorizmus, mint biztonságpolitikai kockázat in Szakmai Szemle, a Katonai Biztonsági Hivatal Tudományos Tanácsának kiadványa,
2005. 3. szám pp.: 42-66.
http://www.kbh.gov.hu/publ/szakmai_szemle/2005_3_szam.pdf
Letöltés ideje: 2011. 10. 24.

[5] http://ec.europa.eu/health/preparedness_response/cbrn_threats/index_hu.htm
Letöltés ideje: 2013. 01. 10.

[6] Zöld Könyv a Biológiai Veszélyekre Való Felkészültségről, Az Európai Közösségek Bizottsága, Zöld könyv, Brüsszel, 11.7.2007 COM(2007) 399

[7] European Centre for Disease Prevention and Control. Operational guidance on rapid riskassessment methodology. Stockholm: ECDC; 2011. ISBN 978-92-9193-306-8.

[8] Dr. Kopcsó István: A katona-egészségügyi szolgálat XXI. századi kihívásai, különös tekintettel a NATO egészségügyi transzformációs folyamatának támogatására, 2009
http://193.224.76.2/downloads/konyvtar/digitgy/phd/2010/kopcso_istvan.pdf
Letöltés ideje: 2010. 01. 23.

[9] Egészségügyi Világszervezet Nemzetközi Egészségügyi Rendszabályainak kihirdetéséről szóló 2009. évi XCI. törvény

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Mórocza Árpád - Pellérdi Rezső
arpad.morocza@gmail.com - pellerdi.rezso@uni-nke.hu

A METRÓ, MINT KRITIKUS INFRASTRUKTÚRA

Absztrakt

A főváros legfontosabb tömegközlekedési létesítménye a metró. Egyelőre három metróvonalat találunk Budapesten, azonban a negyedik átadása a közeljövőben várható. A metró az új jogszabályi háttér alapján kritikus infrastruktúrának lett minősítve. A cikkben bemutatjuk a metrót fenyegető természeti és civilizációs veszélyeket, illetve vázoljuk, hogy milyen lehetőségek mutatkoznak a rendszer biztonságának fokozására. A metró K-Ny-i és É-D-i vonalain kettős rendeltetésű életvédelmi létesítményeket találhatunk. Nem titkolt célunk volt, hogy a meglévő óvóhelyi struktúrának az új kritikus infrastruktúra védelmi feladatrendszerben helyet találjak, azaz a 20. század hidegháborús fenyegetettsége miatt kiépült rendszer a 21. század biztonsági kihívásaira is megoldást nyújthasson.

The capital's most important public transport facility is the metro. For now, we can find three metro lines in Budapest, but the fourth one's transfer is expected in the near future. The metro under the new legislative framework classified as critical infrastructure. In this article the authors present the metro's threat of natural and man-made emergency, and outline what opportunities are there, to improve the security of the system. On the metro's east-west and north-south lines, dual-purpose life saving facilities can be found. Our goal was not a secret that we tried to find a place for the existing structure of the shelter, in the protection of critical infrastructure system. So the system that was built in the 20th century, against the Cold War threat, also can give solution for the security challenges in the 21st century.

Kulcsszavak: *óvóhelyi védelem, biztonság, veszélyhelyzet, életvédelmi létesítmények, metró ~ shelter protection, security, emergency, life protection establishments, metro*

BEVEZETÉS

A kritikus infrastruktúra védelem szorosan kapcsolódik a biztonság fogalmához. A biztonság régi meghatározása szerint ez egy olyan állapot, melyben minket semmiféle –ránk nézve- káros hatás nem érhet. Ha jól belegondolunk, ilyen állapot gyakorlatilag nincs, így a biztonság fogalmának új megközelítését tudom elfogadni, mely szerint a biztonság egy olyan állapot, melyben képesek vagyunk reagálni a minket veszélyeztető esetleges hatásokra.

A kritikus infrastruktúra védelem is e képesség megvalósítása érdekében alakult ki. Fontos tisztázni a kritikus infrastruktúra védelem fogalmát. Az infrastruktúra fogalma a gazdaságtudományban jelent meg. Olyan feltételek gyűjtőneve, melyek közvetlenül nem vesznek részt a termelési folyamatokban, azonban a termelésnek és a termelés fejlesztésének lehetőségét közvetve befolyásolják.

A társadalmi értelemben vett infrastruktúra ebből következtetve mindazon szervezetek, létesítmények, létesítményrendszerek, hálózatok összessége, amelyek egy országon belül a lakosság szellemi és tárgyi életfeltételeit megteremtik, a gazdaság működését elősegítik, illetve lehetővé teszik. Kritikusnak nevezhetünk minden olyan dolgot, feltételt, melynek megsemmisülés, rongálódása, csökkenése az általa támogatott létesítményre, rendszerre egyértelműen negatív hatást gyakorol.

A kritikus infrastruktúra védelem fogalmának definícióját a katasztrófavédelmi törvény végrehajtásáról szóló 234/2011-es kormányrendelet adja, mely szerint kritikus infrastruktúra a Magyarországon található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése, e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.

A metrónak, mint tömegközlekedési infrastruktúrának a működése, illetve a működés biztonságosságának javítása, különös tekintettel lévén arra, hogy a K-Ny-i és az É-D-i metróvonalak duplán kritikus infrastruktúrának számítanak, mivel egyrészt tömegközlekedési létesítmények, másrészt pedig a bennük kialakított óvóhelyi struktúrának köszönhetően védett létesítmények is kiemelt feladat.

A PREVENTÍV BIZTONSÁG

Barry Buzan szerint a biztonság egy komplex rendszerként értelmezhető, melynek öt dimenziója van: környezeti, gazdasági, politikai, katonai és társadalmi. A bipoláris világrend megszűnése megnövelte a biztonság nem katonai tényezőinek jelentőségét. A társadalmi biztonság meghatározza és garantálja a társadalmi cselekvés feltételrendszerét.[1] Ám ahhoz, hogy a társadalmi biztonság megvalósuljon, biztosítani kell a környezeti, gazdasági, politikai és a katonai biztonsági tényezők feltételeit is, vagyis az egyes elemek közt szoros kölcsönhatás érvényesül.

A társadalmi biztonságot számtalan esemény, folyamat fenyegetheti, mint például az ún. új típusú kihívások (intenzív globalizáció, alacsony intenzitású konfliktusok, helyi háborúk, információs korszak, a kritikus infrastruktúrák elleni támadások), melyek a közelmúltban jelentek megjelentek meg, kerültek felszínre. Ilyen fenyegetéseket jelentenek még a társadalmi biztonság gazdasági veszélyforrásai (a mélyszegénység, a társadalmon belüli nagy anyagi különbségek, melyek konfliktusok kialakulásához vezethetnek) vagy a környezeti problémákból fakadó veszélyek, környezeti katasztrófák. Az ilyen fenyegetések

[1] Gondolatok és vélemények a biztonságunkról – A biztonságkultúra kérdései, TIT HABE, Budapest 2008., Dr. Vámosi Zoltán: A biztonság, biztonságpolitika és biztonságkultúra összefüggései, 11. oldal

veszélyeztetik a polgárok testi épségét, környezetét, illetve vagyonát, tehát polgári veszélyhelyzetet idézhetnek elő.

1907-ben, 105 éve született Barényi Béla[2], aki a gépjármű iparban maradandót alkotott, ugyanis megalkotta a preventív biztonság fogalmát. Manapság már az összes autót úgy tervezik meg, hogy egy esetleges ütközés esetén az utasokat magába foglaló egység viszonylag sértetlen maradjon, míg a többi rész az ütközés során energia elnyelő funkcióval bírjon, így védve az utasokat a túlzott és veszélyes erőhatásoktól. Bár maga az autó totálkárosra törik, a benne ülők jó esélyekkel élhetnek túl egy nagyobb sebességű ütközést is. Ezen túl természetesen a balesetek elkerülését is fontos célnak tűzte ki az autóipar, ezért javítják a gépjárművek menettulajdonságait, stb. Gyakorlatilag a tervezők előre gondolkoznak, próbálnak felkészülni minden lehetséges esetre, azaz ténylegesen javítják a közlekedésben résztvevők biztonságát.

A prevenció (lat. praeventio) megelőzést, megakadályozást, meghiúsítást jelent.[3] Esetünkben valamely, a kritikus infrastruktúrát károsító lehetséges hatások bekövetkezésük előtti megakadályozását, elhárítását jelenti.

Ha a fenti autós példát tágabban kívánjuk értelmezni, szükséges a biztonság fogalmával is foglalkoznunk. Mi az, hogy biztonság?

„1. A dolgoknak, életviszonyoknak olyan rendje, olyan állapot, amelyben kellemetlen meglepetésnek, zavarnak, veszélynek nincs vagy alig van lehetősége, amelyben ilyentől nem kell félni.

a.) Valakinek, valaminek (veszélytől, kártól, jogtalan beavatkozástól, bántástól való) védett állapota, helyzete.

b.) Védelem, oltalom.

Ehhez a fogalomkörhöz tartozik az ún. biztonságérzet: a valakinek azzal a tudattal járó érzése, hogy biztonságban van; az az érzés, amely lehetővé teszi, hogy elfogultság nélkül, kellő határozottsággal, öntudattal cselekedjék az ember; magabiztosság."[4]

Fenti fogalom meghatározás meglehetősen elavultnak tekinthető, ugyanis gyakorlatilag egy olyan állapotot vetít elénk, amelyben minket semmiféle –ránk nézve- negatív hatás nem érhet. Ha jobban belegondolunk, ilyen állapot nincs. Testi épségünk, egészségünk, anyagi-materiális, szellemi, kollektív biztonságunk folyamatos kihívásoknak van kitéve, azaz akkor lehetünk biztonságban –ha egyáltalán biztonságnak lehet nevezni ezt az állapotot-, ha képesek vagyunk kezelni ezeket a helyzeteket. Ennek megfelelően az alábbi, a biztonság fogalmának komplex értelmezését tudom elfogadni:

„A biztonság ma komplex fogalom és állapot; a politikai, gazdasági, katonai, szociális, humanitárius, környezetvédelmi szférákra, valamint a katasztrófaelhárításra egyaránt kiterjed. […] olyan reális képességeken nyugvó helyzet és állapot, amely magában foglalja: az ország lakosságának, területének, állami érdekeinek, nemzeti értékeinek megóvását és védelmét minden olyan külső és belső potenciális veszélytől, fenyegetéstől, amely az emberi és nemzeti (nemzetiségi, etnikai, vallási) létet, az egyén boldogulását, a progresszív irányú fejlődét hátráltatja és akadályozza."[5]

Összekötve a metrót, mint tömegközlekedési infrastruktúrát a prevencióval és a biztonsággal megállapíthatjuk, hogy a metró biztonságának javításához a prevenciót és a rendelkezésünkre álló eszközök alkalmazását elsődleges fontosságú eszközöknek kell tekintenünk.

---

[2] http://www.veteran-mercedes.hu/barenyi.html letöltve: 2012-10-10

[3] Tudományos és Köznyelvi Szavak Magyar Értelmező Szótára, letöltve: 2012-10-08

[4] A magyar nyelv értelmező szótára. I. kötet A–D, Akadémiai Kiadó, Budapest, 1959. 643. old.

[5] Hadtudományi Lexikon A–L. Főszerkesztő: Szabó József, MHTT, Budapest, 1995. 144. old.

2. KRITIKUS INFRASTRUKTÚRA VÉDELEM

Az infrastruktúra a termeléshez kapcsolódó eszközök, intézmények és módszerek összessége, amelyek közvetlenül nem részei a termelési folyamatnak, azonban annak nélkülözhetetlen feltételeit adják. Infrastruktúrák nélkül nincs termelés; a termelés nélkül pedig nincs létjogosultságuk az infrastruktúráknak.

Az infrastruktúrák nagy méretük, közhasznúságuk és tömeges igénybevételük miatt a világ államaiban általában állami kézben vannak. Privatizálásuk éppen ezért szigorúbb feltételekhez kötött, mint egy termelő vállalat esetében. További jellemzőjük, hogy előállítási költségük mellett jelentős fenntartási költségük is van.

A karbantartások és felújítások elmaradása a termelés drágulását eredményezheti, ezen túlmenően csökken az adott infrastruktúra által kiszolgált ágaz biztonsága, amely mind balesetveszélyt, mind pedig anyagi károkat okozhat. A 3-as metró állapota tipikus példa erre a fenti állításra. Az évek során elhasználódott, a teljes körű felújítás hiánya csökkenti a rendszer biztonságát; idővel elodázhatatlan lesz az infrastruktúra felújítása, mivel a rendszer működésének biztonsága alapjaiban válik megkérdőjelezhetővé.

Az infrastruktúrák fontos jellemzője a kapacitás, amely az időegységre levetített szolgáltatási teljesítményt jelenti. A metrók esetében ez az utasforgalom mértékét jelenti. Az infrastruktúrák önmagukban nem termelnek hasznot, azonban hiányuk a termelés alapvető lehetőségét kizárják. Ezért van az, hogy az infrastrukturális beruházások haszna más ágazatokban jelentkezik, így a fejlesztésre, illetve fenntartásra fordított költségeket is más ágazatok profitjának megadóztatásából kell biztosítani.

A különféle infrastruktúrák üzemzavaraira a társadalom érzékenyen reagál. Elég, ha arra gondolunk, hogy a 2012. első félévében gyakori, metrót érintő füstölések miatti üzemzavarok milyen fennakadásokat jelentettek a főváros tömegközlekedésében. A fennakadásokon túl többletköltségeket is jelentett, mivel a metró kieséséből származó utas-szállítási kapacitást más módon –pótló buszok forgalomba állításával- kellett megoldani. Értelemszerűen a pótló buszok is hiányoztak valahol, ez –a dominó elvhez hasonlóan- további többletköltségeket, fennakadásokat eredményezhetett. A példa jó szemléltető eszköz arra, hogy mennyire lényeges a különféle infrastruktúrák szünetmentes, üzemszerű működésének biztosítása.

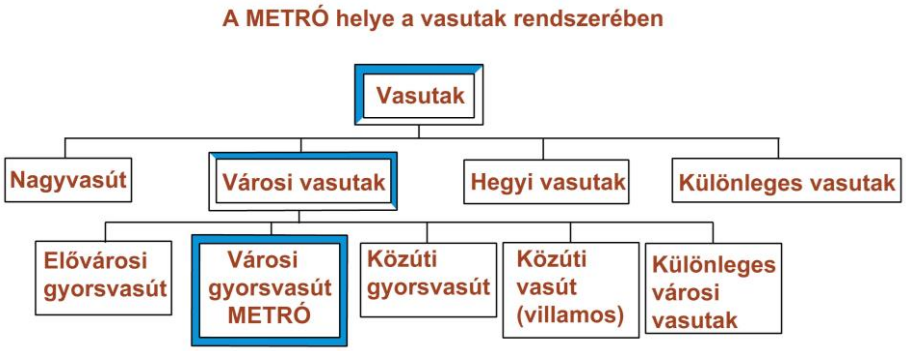
3. TÖMEGKÖZLEKEDÉS, MINT KRITIKUS INFRASTRUKTÚRA

Napjaink felgyorsult világában a megtett út és az eltelt idő hányadosával meghatározott mennyiség, azaz a sebesség kiemelten fontos. Egyre gyorsabb és biztonságosabb közlekedési eszközöket terveznek, gyártanak, melyek végül ismét csak rohanást szülnek. A sebesség mellett azonban a költséghatékonyság és a környezeti terhelés minimalizálása is fontos szempont lett.

Különösen a nagyvárosokban nem célszerű az egyéni közlekedést erősíteni, mivel így a környezeti terhelés sokkal nagyobb lesz, a forgalmi torlódások kialakulásával a közlekedés megbénulhat, a tömegközlekedéshez (újabb kifejezéssel: *közösségi közlekedés*[6]) viszonyítva kevésbé biztonságos, és drágább; nem mellékesen a parkolás lehetőségeinek biztosítása meglehetősen költséges és nagy volumenű beruházásokat (informatikai rendszerek, mélygarázsok, stb.) igényel.

Szerkezetéből adódóan kettős rendeltetésű életvédelmi létesítmények kialakítására is lehetőség van a metrókban. Ezek az életvédelmi létesítmények a világ több metrójában – Budapest, Moszkva, Prága, London, stb.- kialakításra kerültek.

[6] A kifejezés a „*public transport”* fordításából következik.



1. ábra. A METRÓ helye a vasutak rendszerében

3.1. Óvóhely a metróban

Az helyi védelem története egyidősnek tekinthető az emberiség történetével, ugyanis a konfliktusok során mindig felmerült az igény arra, hogy a civil lakosság életét megóvják a pusztításoktól.

A helyi védelem a repülés megjelenése kapcsán igen nagy szerephez jutott. Elég, ha a második világháború szőnyegbombázásaira gondolunk, amikor a lakosság a pályaudvarok, üzemek közelében kialakított lakossági életvédelmi létesítményekben vészelte át a bombázásokat.

A második világháborút követően a nukleáris fegyverek megjelenése ösztökélte a tervezőket arra, hogy a lakosságvédelem e formáját továbbra is fent tartsák. Az óvóhelyek lakosságvédelmi rendszerben történő elhelyezkedését a következő ábra szemlélteti.

A K-Ny-i metró tervezése során –hasonlóan a példaként szolgáló moszkvai metróhoz- e létesítmény kettős funkciót kapott; azaz fő célja békeidőszakban a tömegközlekedés, míg egy esetleges minősített időszakban óvóhely biztosítása. Az É-D-i metrót szintén így alakították ki; azonban a DBR metrót már *nem*.

A fővárosban mintegy 3 300 életvédelmi létesítmény található, ezekben hozzávetőlegesen 495 000 főt lehetne elhelyezni. Ezek a létesítmények azonban nagyrészt csak romteher ellen védő szükségóvóhelyek (légópincék), melyek nem rendelkeznek saját energia, vízhálózattal, szűrt szellőzőkkel, és vizesblokkokkal.

A metró kettős funkcióval rendelkező szakaszaiban 220 000 főt lehetne elhelyezni. Ezek a kettős rendeltetésű létesítmények III. és IV. osztályba sorolt minősített óvóhelyek. Látnunk kell azt, hogy a fővárosban található életvédelmi létesítmények állapotához és védőképességéhez képest a metró folyamatosan karbantartott, minősített óvóhelyei nagy kontrasztot mutatnak, éppen ezért nem szabad hagyni, hogy egy ilyen védőképességű és állapotú lakosságvédelmi létesítmény további fenntartása, állagmegóvása –ne adj Isten: fejlesztése- ne valósulhasson meg.

A K-Ny-i vonalon 3, az É-D-i vonalon 9 szektor került kialakításra. A szektorokra osztás célja az, hogy egy szektor esetleges rongálódása, megsemmisülése esetén a többi ettől függetlenül működőképes marad. A szektorok 4 üzemmódban üzemelhetnek: betelepüléses, léglökésvédett, gáz-és sugárvédett, teljes elzárkózásos.

A metró óvóhelyek kialakításának szemléltetéshez egy ábrát készítettem, mely egy *nem valós* példán keresztül mutatja be a létesítmény funkcionális kialakítását.

2. ábra. Metró óvóhely
Forrás: saját ábra

3.2. A metrót veszélyeztető hatások

Jelen cikkben mindössze a legfontosabb veszélyeztető hatások bemutatására nyílik lehetőség; elegendőnek mutatkozik, ha rá tudjuk irányítani a figyelmet e hatások sokféleségére - ezáltal reflektálva a védekezés komplexitására és szükségességére-.

A metrót veszélyeztető hatásokat alapvetően két nagy részre oszthatjuk fel:

Természeti és c*ivilizációs* eredetű hatásokra.

3.2.1. Természeti eredetű veszélyek

1. *Árvíz:* A fővárosi metrórendszer árvíz veszélyeztetettsége valós fogalom. A K-Ny-i vonalon a Batthyány tér és a Kossuth tér állomások vannak kitéve az esetleges árvizek hatásainak. A 2006. áprilisi árvíznél a Duna rekord vízállása[7] miatt szükségessé vált a felkészülés a Batthyány téren lévő lejtakna kapu (polgári védelmi műtárgy) bezárására, mivel számítani lehetett arra, hogy a lejtaknát egy esetleges gátszakadás miatt elárasztathatja a víz. Ez a lépés -hogy az 50 tonna/m^2 túlterhelésre méretezett léglökésvédelmet és hermetizációt megvalósító kapu[8] bezárásának lehetőségét megteremtették- teljes egészében *infrastruktúra védelmi intézkedés* volt. A kapu zárt állapotában az utasforgalom az állomáson nem lett volna megvalósítható, azonban a szerelvények az állomáson történő megállás nélkül továbbhaladhattak volna, így a létesítmény fő célja, azaz az utasforgalom biztosítása megvalósítható lett volna.A 2010-es árvíznél szintén kilátásba helyezték az állomás lezárását.[9] Az árvizet követően a veszélyeztetett állomásokra árvízvédelmi szivattyúkat telepítettek egy esetleges vízbetörés gyors kezelésének lehetősége érdekében. Az árvizek veszélyeztető hatását semmiképpen sem szabad figyelmen kívül hagynunk, elég ha arra gondolunk, hogy a prágai metró a 2002-es árvíz során gyakorlatilag megsemmisült, amikor 25 állomásából 17 víz alá került.[10]

[7] http://www.index.hu/bulvar/rvzbp3423/ „Homokzsákok mindenfelé" letöltve: 2012-10-21

[8] A méretezés a metró III. osztályú, minősített óvóhelyének paramétere. Az alagút szerkezetek és az elzáróberendezések is e túlterhelésnek állnak ellen.

[9] http://www.index.hu/belfold/2010/06/01/megint_a_viz_azur/valtozasok_lesznek_a_budapesti_tomegkozlekedesben/ letöltve: 2012-10-21

[10] http://www.nol.hu/archivum/archiv-81603 letöltve: 2012-10-22

3. ábra. A prágai metró a 2002-es árvíz után
Forrás: http://www.nol.hu/archivum/archiv-81603 (2012-10-22)

2. *Viharok:* A viharok elsősorban a felszíni közlekedést veszélyeztetik. A kidőlt fák, leszakadt elektromos vezetékek megbéníthatják a busz, trolibusz, villamos és vasúti közlekedést. Ezen túlmenően a felszínen tartózkodókra is veszélyt jelent. Példaként a 2006. augusztus 20-i tűzijátékon négyen haltak meg, és 300-an sebesültek meg a viharban[11]. Ilyen esetben a metró biztonságos és tömegtartózkodásra alkalmas létesítményeit könnyen a lakosság rendelkezésére lehetne bocsátani, vagy szükségóvóhelyként, vagy –ami nagyobb szervezést igényel, de hatásosabb- védett útvonal biztosítása mellett kitelepítési útvonalként. Ehhez azonban a döntéshozó szervek gyors és határozott reagálása lenne szükséges. A katasztrófát követően a felelősség megállapítására irányuló időszakban Takács Albert, az akkori állampolgári jogok országgyűlési biztosának általános helyettese jelentette ki, hogy „Ha a vasárnapi tűzijáték alatt kitört viharban feleannyi ember intézkedett volna, mint ahányan hétfőn vizsgálatot kezdeményezett az ügyben, akkor valószínűleg megelőzhető lett volna a tragédia.”[12] A vihar idején egyébként rengetegen az Alagútba menekültek a Lánchíd környékéről.

3.2.2. Civilizációs eredetű veszélyek

1. *Terrorizmus:* A tömegközlekedés egyértelműen nagyon kitett a terrorizmus veszélyének. A repülőtereken kiépített komoly biztonsági rendszerek telepítése – anyagi és forgalmi okokból- a metróban lehetetlen lenne. Nincs lehetőség arra, hogy a napi milliós utas számmal rendelkező metrókban az összes utast átvizsgálják, felügyeljék a mozgásukat, esetleges gyanús egyéneket kiemeljenek. Az utasforgalom ellenőrzésének lehetőségét a telepített ipari kamera hálózat, a forgalmi szolgálattevők és a biztonsági szolgálat munkatársainak jelenléte adja. A metró nagyon sok terrortámadásnak volt a célpontja; ezt az Aktualitások részben taglaltam. A kamera rendszerekkel kapcsolatosan érdemes kiemelni, hogy a 2005-ös londoni metrót is érintő terrortámadások elkövetőit a városban és az összes tömegközlekedési eszközön kiépített, arcfelismerő rendszerrel összekötött kamerarendszerek segítségével sikerült azonosítani. A budapesti metróban szintén érdemes lenne egy ilyen, visszakövethető, pontos arcfelismerést lehetővé tevő rendszert kiépíteni. A védekezés nehézségét –a nagy utasforgalom mellett- a kis terek adják. Gyakorlatilag egy jól előkészített támadást megakadályozni nehezen vagy egyáltalán nem lehet. A védekezés eszköze jelen esetben is a *prevenció*, mely egyrészt az *adatbiztonság garantálásából* másrészt a *felkészítésből*, harmadrészt

[11] http://index.hu/bulvar/vhrkrnlg8174 letöltve: 2012-10-22
[12] http://www.inforadio.hu/hir/belfold/hir-65860 letöltve: 2012-10-22

pedig a *felderítésből és elhárításból* áll. A *felkészítés* alatt a forgalmi szolgálattevők, az állomási műszaki ügyeletesek, a vonalközpontokban a vonal műszaki működéséért felelős műszaki diszpécserek, a vonalközpontokban a vonal forgalmi működéséért felelős központi forgalmi menetirányítók, a vonalközpontokban a vonal energiaellátásért felelős energia diszpécserek és a rendvédelmi szervek beavatkozó állományának (katasztrófavédelem, rendőrség, terrorelhárítás) megfelelő kiképzését és gyakoroltatását értem. Lényeges lenne az adott helyszínen szolgálatot teljesítők ilyen irányú kiképzése, mivel a gyorsan és szakszerűen hozott jó döntések a további műveletek sikerét nagyban elősegítik. Ez nem csak a terrortámadásokra, hanem például a tűzesetekre vagy egyéb üzemzavarokra is érvényes.

2. *Tűzesetek:* A metró tűzvédelmének kiemelten fontosnak kell lennie a biztonság javításában. A tűzvédelem részei a következők: tűzmegelőzés, tűzoltás-műszakimentés és a tűzvizsgálat[13]. A legnagyobb eredményeket a tűzbiztonság javításában itt is a megelőzéssel lehet elérni. Ez passzív és aktív tűzvédelmi rendszerek, szabályok életbeléptetését kívánja meg, különös tekintettel lévén arra, hogy a metróban keletkező tüzek oltása kifejezetten nehéz és veszélyes feladat az állomások megközelíthetősége (nagy mélységek, nagy távolságok), a nagyfeszültség esetleges jelenléte (825V, egyenáram), a nagy embertömegek jelenléte, a pánikjelenség esélye, illetve a tűzoltók által alkalmazott nyitott rendszerű, túlnyomásos légzőkészülékek által biztosított korlátozott bevetési idő miatt. A K-Ny-i metróvonalon a 2000-es évek elején végrehajtott rekonstrukció során nagy figyelmet kapott a létesítmény tűzbiztonságának fokozása. Ekkor kerültek telepítésre az állomási vágányszakaszokra; a mozgólépcső gépházakba; a lejtaknákba; a kábelcsatornákba; illetve egyéb üzemi terekbe a nagynyomású (120 bar üzemi nyomású) *FOGTEC vízköddel oltó* berendezések, melyek oltási teljesítménye illetve a minimális vízkár egyaránt mellette szólnak. A vízköddel oltó további előnye, hogy a menekülési útvonal füstmentesítésére is alkalmas és csökkenti a hőterhelést. Feszültség alatti elektromos berendezések oltására is alkalmas, ezt a metró esetében is kipróbálták. A vízköddel oltó rendszerek mellett a füstmentes menekülési útvonal biztosítására a lejtaknákban párosan telepített, axiális átömlésű *JET ventillátorokat* helyeztek el. A *főszellőző ventillátorok* tűzvédelmi funkciót is kaptak: az alagút szakaszok irányított füstmentesítését lehet végrehajtani velük, ez a forgásirányuk és fordulatszámuk szabályozhatóságának köszönhető. Új BMZ-Integral *tűzjelző* központot és érzékelőket telepítettek, végrehajtották a *tűzszakaszolást* illetve a födémáttörések tűzgátló anyaggal történő lezárását. Az É-D-i metrón bekövetkezett füstölések[14] és tűzesetek[15] miatt nyilvánvalóvá vált, hogy a vonal –K-Ny-i vonalához hasonló- teljes felújítása és a futásteljesítményük végén járó metrószerelvények cseréje elodázhatatlan feladat. Mindezen lépések elengedhetetlenek a metró tűzbiztonságának – ezáltal a tömegközlekedési infrastruktúra védelmének-javításához. A BKK 2012. október 8-i közleménye alapján a metró szerelvények tűzbiztonságának javításával kapcsolatos, hogy a BKV 2012 májusában Tarlós István főpolgármester és a BKK kezdeményezésére kérte fel a TÜV Rheinland műszaki szakértő intézetet a vonatokon található elektromos berendezések átvizsgálásával, valamint kockázatkészítéssel. A jelentés eredményei szigorúbb ellenőrzési protokollt javasoltak a karbantartás és üzemeltetés során, melyet a BKV elfogadott.[16]

[13] 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról

[14] http://www.iho.hu/hur/fustolo-metro-a-3-as-vonalon-120502 letöltve: 2012-10-22

[15] http://www.index.hu/bulvar/2011/04/19/kiuritettek_az_arpad_hidi_metroallomast/ letöltve: 2012-10-22

[16] http://www.bkk.hu/2012/10/kozlemany-a-3-as-metro-muszaki-rendszereirol-keszult-vizsgalati-jelentes-kapcsan/ letöltve: 2012-10-22

3. *Üzemzavarok:* A metró biztonságos üzemét nem csak külső, hanem belső tényezők is nagyban befolyásolhatják. 1991. február 1-én az Astoria állomásnál eltörött egy főnyomócső, amelyből nagymennyiségű víz került az állomásterekbe. Jellemző a csőtörés hatásaira, hogy az alagútban rekedt vonat utasait a magasabban fekvő Blaha Lujza tér állomás felé a feszültség és forgalommentes pályán kellett átkísérni; a víz pedig a Deák Ferenc tér felé folyt, ahol a két vonal között vasúti összeköttetést biztosító üzemi összekötő alagútban nagyjából 40 cm mélységben állt.

4. KÖVETKEZTETÉSEK, JAVASLATOK

A cikkben átfogó képet alakítottunk ki a metró helyzetéről felvázoltuk, hogy a metrót veszélyeztető hatásokat. Fontos ismételten megjegyezni, hogy a budapesti metrót hivatalosan is kritikus infrastruktúrának, vagy, ahogy a törvény fogalmaz: létfontosságú elemnek lett nyilvánítva. Nem titkolt célunk volt az sem, hogy a régi veszélyekre kialakított óvóhelyi struktúrát összekössük egy teljesen *új feladatrendszerrel*, azaz a kritikus infrastruktúra védelemmel. A metró óvóhelyi rendszerének a tömegközlekedési infrastruktúra kritikus infrastruktúra védelemével kapcsolatban nem csak lehetséges eszközként kell jelen lennie, hanem önmagában, mint tömegtartózkodásra alkalmas lakossági óvóhelynek is helyet kell kapnia a kritikus infrastruktúra védelem fogalomkörében. Az már gyakorlatilag csak egy plusz, hogy egyben a tömegközlekedési infrastruktúra védelmére is lehet alkalmazni magát az óvóhelyet!

A katasztrófa fogalma komplex fogalom; ennek megfelelően a katasztrófák elleni védekezés szintén szerteágazó tevékenységet kíván meg. Manapság a lakosságvédelemben a fő szerepet a távolságvédelem elve adja, azaz a kitelepítés és a kimenekítés alkalmazása. A helyi védelem, azon belül is az óvóhelyi védelem egyfajta mostohagyerekként van kezelve a lakosságvédelemben, mivel mindenki úgy tekint rá, mint egy régmúlt időszak szülöttére, amely teljesen más biztonsági kihívásokra adott válaszul jött létre –gyakorlatilag a hidegháború nukleáris fegyverei elleni védekezésre lett kialakítva-. A metró óvóhely az összes többi életvédelmi létesítmény között kiemelt helyet foglal el. Állításra bizonyítékul szolgál, hogy folyamatosan kiképzett személyi állománnyal rendelkezik a Metró Polgári védelmi Szakalegység. Ezen túlmenően az óvóhelyi berendezéseket folyamatosan hadrafogható állapotban tartják, köszönhetően a 12 éves ciklikussági rendben megvalósított nagyjavításoknak. Az alagútszerkezetek védőképessége alapból kiemelkedő, a telepített szükségenergia és szükségvíz hálózatok pedig a városi hálózatoktól való független működést biztosítják. A kor biztonsági kihívásai teljesen megváltoztak, gyakorlatilag már senki sem készül atomháborúra. Azonban a veszélyek ismertetésénél láthattuk, hogy sok más, új veszély jelent meg, amelyek elleni védekezés szintén kötelességünk. E védekezés módja vagy a lakosság elhelyezése védett körülmények között; védett útvonal biztosítása a távolságvédelmi manőverek végrehajtásához; vagy magának a metrónak, mint tömegközlekedési rendszernek a védelme.

Javaslatként megfogalmazható, hogy érdemes lenne készíteni egy tanulmányt, a főváros közlekedési helyzetéről, ha a metró néhány napra leállna. Nem véletlen, hogy a metró dolgozóinak sztrájkjoga nem engedi meg a teljes forgalmi üzem leállítását! Akármilyen sztrájk lenne, a metrónak a minimális szolgáltatást biztosítania kéne. Nem szabad figyelmen kívül hagynunk azt a tényt sem, hogy a metró szerelvényeket bizonyos időnél nagyobb követési idővel nem lehet közlekedtetni, mivel így az állomásterekben, és a peronokon feltorlódó tömeg balesetveszélyes helyzeteket okozna. Gyakorlatilag vagy közlekedik a metró üzemszerűen, vagy sehogy. Kutatómunkám során nem találtam egyetlen tanulmányt sem arra vonatkozóan, hogy a főváros tömegközlekedésében, illetve egyáltalán a főváros életében milyen problémákat (dugók, légszennyezezettség, gazdasági következmények) okozna a

metró közlekedésének hiánya, abban azonban biztos vagyok, hogy „forintosíthatóak” lennének ezek a problémák, zavarok.

Véleményünk szerint a metró óvóhely berendezései csak eszközök egy lehetséges infrastruktúra védelemben. A valódi értelmét a rendszernek a *tervezés*, és a *gyakorlatok* végrehajtása adná. Például célszerű lenne tervezni egy 900 cm-es dunai árvíz elleni védekezést a metró árvíz-veszélyeztetett állomásain. Jó együttműködési alapot jelentene a katasztrófavédelem és a BKV Zrt. szakemberei között a védekezés részletes megtervezése; szivattyúk telepítési helyének-körülményének tisztázása stb.

Más gyakorlatok alkalmával a BKV Zrt. munkavállalói részt vehetnének például tűzvédelmi továbbképzéseken, tanfolyamokon, mialatt a tűzoltói beavatkozó állomány a metró területén helyismereti foglalkozásokon venne részt, mentési és oltási gyakorlatokkal összekötve. Ez a fajta együttműködés jelen van most is a katasztrófavédelem és a BKV Zrt. között. Úgy gondoljuk, a Metró óvóhelyeken évente kétszer megtartott szektorpróbák, vagy polgári védelmi gyakorlatok is alkalmasak arra, hogy akár egy komplex kitelepítési gyakorlatban kerüljenek végrehajtásra, adott kerület, kerületek bevonásával.

Mindez végső soron a metró biztonságának színvonalas fejlődését; a beavatkozó állomány ismereteinek bővülését; a BKV munkavállalóinak biztonságra nevelését; és végső soron a metrót, mint tömegközlekedési létesítményt használó személyek biztonságérzetének növekedését eredményezné.

Felhasznált irodalom

[1] Közlekedik a főváros Írta és szerkesztette: Legát Tibor. Jószöveg Műhely Kiadó, Budapest, 2008

[2] MILLFAV és METRÓ A.1. Alagútfenntartási Utasítás és műszaki adatok, előírások BKV Rt., Budapest, 2002

[3] A magyar nyelv értelmező szótára. I. kötet A–D, Akadémiai Kiadó, Budapest, 1959.

[4] Hadtudományi Lexikon A–L. Főszerkesztő: Szabó József, MHTT, Budapest, 1995.

[5] Révai új lexikona, 12. (Klc-Ky), Babits Kiadó, Szekszárd, 2003.

[6] Jávorka Géza: Polgári védelem, főiskolai jegyzet, Eötvös József Főiskola

[7] Pellérdi Rezső-Mórocza Árpád: Az óvóhelyi védelem aktualitásának vizsgálata, Hadmérnök, ZMNE, 2010. 1. sz. 12. o. http://www.hadmernok.hu/2010_1_morocza_pellerdi.pdf letöltve: 2012-10-22

[8] Magyarország Alaptörvénye

[9] 2011. évi CXXVIII. törvény

[10] 2011. évi CXIII. Törvény

[11] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

[12] 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

[13] 2012.évi CLXVI. törvény

[14] A metró, mint a jövő kritkis infrastruktúrája, XXXI. OTDK 1. helyezett dolgozat. Írta Mórocza Árpád, konzulens: Dr. Pellérdi Rezső ny. alez. egyetemi docens

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Schüller Attila
schuller.a@gmail.com

COMPARATIVE ANALYSIS OF PATENTS FOR VISUAL FIRE ALARMS

Abstract

Tűzeset miatti épületkiürítéskor fontos szerepe van annak, hogy a menekülők gyorsan felismerjék a helyes menekülési útvonalat. Ennek elősegítésére léteznek szabályozások, de folyamatosan adnak be szabadalmakat az előírásokhoz képest hatékonyabb vizuális tűzjelző eszközökre. A szerző néhány amerikai szabadalomban szereplő megoldás előnyeit mutatja be, amelyek csökkenthetik a kiürítés során jelentkező negatív emberi tényezőket.

During evacuation due to fire it is important that the people who are trying to escape should quickly recognize the escape route. To facilitate this, there are regulations, but patents are being lodged continuously for visual fire alarm devices that are more efficient than the requirements. The author presents the advantages of some solutions offered by several U.S. patents.

Keywords: *vizuális tűzjelzés, szabadalom, emberi tényező, tűzriadó, evakuálás, épületkiürítés ~ visual fire alarm, patent, human factor, fire drill, fire alarm, evacuation*

INTRODUCTION

The types of alarm and signs laid down in the fire safety regulations only ensure a certain level of safety and rely on people's awareness, attention and discipline. However, experience has shown that many people act inappropriately in emergency situations even when they have been informed what to do in case of fire and have taken part in fire drills. Although this training reduces the occurrence of human errors, technical solutions could also be used to help the people fleeing to choose the right escape route.

In the 2/2012 issue of Hadmérnök I discussed the negative human factors that occur during a fire alarm. [1] I pointed out, among other things, that people do not pay attention to the routes during evacuation. A Swedish study shows that most people prefer to use the main entrance, even when an emergency exit is closer. This is especially true when the emergency exit door is closed. [2]. In many cases not only does finding the right escape route pose a problem but also people do not realise that they have to escape. [1]

Provided sufficient resources are available for the use of modern visual tools, people are able to recognize quickly that there is an emergency and to choose the right escape route.[1]

There are a lot of patents on the subject of this article and their number continues to grow. Due to lack of space, the list of the solutions I have presented is not exhaustive. I have tried to present the most interesting ones and those which are relatively easy to implement. In some cases, the patents describe a more complex system, but I have only dealt with the visual signalling part of the system.

REGULATIONS

The National Fire Protection Association (NFPA) defines the general requirements in the U.S. The escape route is designated by simple, easy to understand pictograms. Figure 1 allows the American pictograms to be compared with their Hungarian equivalents, the appearance of the latter is in accordance with the prescriptions contained in the decree 2/1998. (I. 16.) MüM.

Figure 1:U.S. (left) and Hungarian (right) escape route signs[2]

The fundamental imagery for symbols, as well as their background colour[3] and shape, are designated in Standard NFPA 170. However, although strobe lighting is commonly used to indicate the escape route, only these static symbols are used to provide information about the direction of escape, but experience shows, escaping people often do not pay attention to these pictograms.

[1] This article deals only with visual tools, but there are other tools such as directional sound, which was described in a previous issue of Hadmérnök. [3]

[2] This figure has been compiled by the author using sources [4] and [5].

[3] The colour of the symbol must meet the requirements of ANSI Z535.1, Safety Color Code.

With regard to lights, we should draw a distinction between emergency lighting that enhances the environment and the visibility of the emergency exits in the case of an emergency, and the visual cues that draw attention to the evacuation. From the standpoint of this article, regulation of visible signalling is more important than emergency lighting, so I have emphasized some factors that relate to the patents I have examined with regard to the fire safety regulations.

According to the Hungarian National Fire Protection Regulations (Országos Tűzvédelmi Szabályzat – OTSZ), visual signalling devices for fire alarms should not be used independently, only to supplement the audio alarm systems. The visual devices used for fire alarms should be clearly visible and should be clearly distinguishable from other lights used in the area. [6]

The parameters of strobe lights are regulated in detail by the NFPA. The flash rate shall not exceed two flashes per second (2 Hz) nor be less than one flash every second (1 Hz) throughout the listed voltage range of the appliance. The maximum pulse duration shall be 0.2 seconds with a maximum duty cycle of 40 percent. The pulse duration shall be defined as the time interval between initial and final points of 10 percent of the maximum signal. Lights used for fire alarm signalling only or to signal the intent to completely evacuate shall be clear or nominal white and shall not exceed 1000 cd (effective intensity). Lights used to signal to occupants that they should seek information or instructions shall be clear, nominal white or another colour as required by the emergency plan and the authority having jurisdiction for the area or building. [7] The regulations only refer to strobe lights. As I shall show, several patents propose sequential signal lights, for which there are currently no standards. However, the current rules can be regarded as providing a basic standard, so that in the case of sequential lights, I recommend that the parameters of the entire section should be adjusted to the characteristics of strobe lights. The OTSZ prescribes, among other things: the circuits of fire alarm systems shall be designed so that in the case of a single wire break or short circuit no more than 32 units may become inoperable and these devices must be in the same area and serve the same function.[6] So, in the case of sequential lights, the system should be divided into sections of 32 indicator lights. If more lights are required for a particular section of the route, they will have to be synchronised.

In the USA strobes used in combination systems where the same strobe is used for both mass notification and fire notification shall comply with the following:[7]

1. Be clear or nominal white, meeting the listing requirements of ANSI/UL 1971, Standard for Signalling Devices for the Hearing Impaired
2. Have no marking or be marked with the word ”ALERT” stamped or imprinted on the appliance
3. Be visible to the public

It is worth noting that the regulations permit the use of colour signals, the conditions for such use are described in a separate section.

Lights used for fire alarm signalling only or to signal the intent to completely evacuate shall not exceed 1000 cd (effective intensity). [7] This regulation is significant for those patents I have examined in which a laser beam is employed.

The OTSZ permits solutions to be employed that improve safety[4]: establishment of a fixed fire extinguishing and fire alarm device (design and construction), operation, inspection and maintenance shall comply with the law and the relevant technical requirements, or should at least ensure an equivalent safety level. [6]

[4] In this case, permission has to be obtained from the fire authority for installation and use.

SOLUTIONS OF PATENT

The title of the first patent that I examined is ”Dynamic Emergency Escape Indicator”. [8] The design of this device is similar to that of a normal exit sign, however, there are several silhouettes that flash sequentially. (Figure 2) Lighting devices located on the edge of the device increase its effectiveness in attracting people’s attention. Because the direction of these can be adjusted independently, this means that, according to the author of the patent, the device can be also used to help to designate the direction of escape by illuminating nearby objects one after the other.

Figure 2: dynamic emergency escape indicator [8]

The advantage of this device is that it attracts one’s attention to the figures flashing sequentially and the devices emitting flashing lights attract the eye. However there is a hidden danger in that the silhouettes flashing sequentially indicate a kind of a direction of escape, which may mislead the people escaping. For example the positioning in figure 2 may lead the person escaping to believe that he should turn left, rather than go out of the door (because the three human figures flash from right to left suggesting that you have to go left). The brightness of the lamps is not sufficient to illuminate distant objects, so these lights may only be a distraction. If the lighting devices are adjusted incorrectly, they may also shine in the eyes of people escaping, which may cause the direction of escape indicated by the sign to be more difficult to recognise. It should be noted that, in contrast to what is shown in figure 2, the smoke generated by the fire is not on the floor, but spreads almost to the ceiling.

The following patent helps for orientation in the dark with LED light strips built into the floor. [9] The lines shown in figure 3 indicate clearly and visibly the sections of the corridor, and the strip passes the doors that cannot be used for escape, it leads people escaping to the emergency exit with a clearly visible arc. The escape route is thereby easy to see, but the direction is not, therefore, the use of conventional supplements is absolute essential. (A similar solution is where the sign is also located in the middle of the corridor, but arrows indicate the direction and in some places texts provide information on the distance of the exit. [10]) This patent also includes an alternative solution for the case where mounting the LED strip in the middle of the corridor is not possible. In this case, the emergency exit would not be clearly marked, therefore the patent proposes a modification, as a result of which, the light signal can be seen only in one direction. Using this solution, apparently, the emergency exit door can be easily distinguished from the rest.

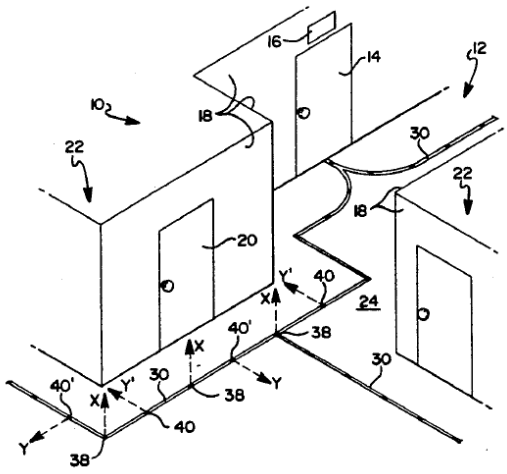


Figure 3: Emergency lighting strip [9]

Positioning the signs in the middle of the floor is preferable to prevent objects placed temporarily in the corridor (cupboards, flowers, boxes, etc.) from hiding the signs (in the case of a low positioning of the signs). However, the implementation is difficult and costly, especially where there is a carpeted floor. It should be noted that the material of the cover should be strong enough to avoid cracking and breaking, and such that transmission of the light is not reduced due to wear and tear, cleaning and other stress. The alternative solution of [9] makes the visual signal more difficult to see from a relatively narrow angle, making it difficult to interpret. In patent [10] the signal occupies a wide band and in many cases (e.g. the luxurious floor covering of hotels) can damage the overall effect of the design. This is offset by the easily recognizable arrows, which make the direction of evacuation absolutely clear and the distance marker inscriptions provide additional information for the people escaping. These information signals are shown in green and the red flashing "DONT USE!! GO TO EXIT" signal is to call attention to the predetermined danger-zones (the entrances to elevators).

The solution shown in figure 4 is different in that in facilitates the evacuation with photoluminescent signs. [11] Predetermined arrows, silhouettes or a series of geometric shapes (e.g. circles) of increasing or decreasing size designate the direction of escape (the arrow version is shown in the figure) and the EXIT signs show the exits. There are also patents in which arrows are also used, but in both directions, so in an emergency they light up, so that in a given situation – according to certain criteria – they mark out the optimal route. [12]

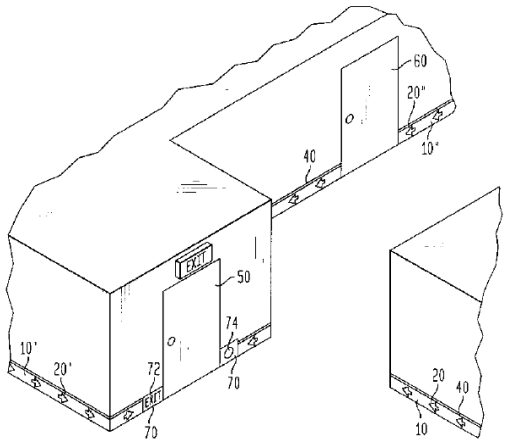


Figure 4: Evacuation route with photoluminescent indicators [11]

The arrows are easily recognizable from a distance, but different sized geometric symbols only provide information for those who know that the diameter of the signs increases or decreases towards the emergency exit.

A multifunctional signalling system is illustrated in figure 5. [13] The white or clear static lights provide ambient lighting, the coloured lights located among them indicate the direction of escape with sequential flashing. In one version of the invention, heat sensors located at each exit will trigger a reversal of the tracer lights to direct evacuees away from the exit in the event that the temperature at that exit reaches an unsafe level.

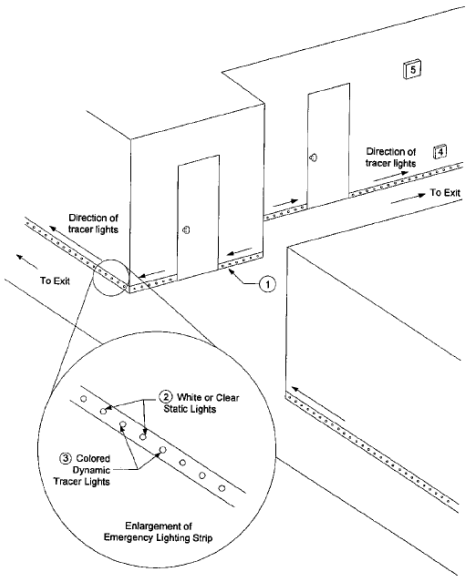


Figure 5: Emergency lighting system [13]

The ambient lighting feature is most effective close to the ground, so it is much easier to see things which might possibly prevent escape. The coloured lights flashing one after another clearly indicate the right direction of escape. The determination of the direction on the basis of the exit temperature may only be used if the direction of all route segments is defined by a main control circuit. The possibility of employing coloured lights in non-fire emergency situations (e.g. tornado, terrorist emergency) is also included in the patent, as well as for decorative purposes (e.g. pulsing lights controlled by music in a disco). According to the U.S. standards the fire alarm signal should be distinct from other types [7], the OTSZ states the following: the lights used for signalling fires should be clearly visible and should be clearly distinguishable from other light signals used in the area at risk. [6] The decorative use of the visual fire alarm and the fire alarm operation cannot be distinguished from one another, so in an emergency situation the people evacuating may think that the usual disco lighting is being operated. As a result they do not understand the meaning of the light strip, so do not pay any particular attention to it. In a previous part of this article (see Regulations) I pointed out that the NFPA allows the fire alarm to be used in other emergency situations, provided certain conditions are met. In this case, however, each mode of the system clearly draws attention to the danger.

The system in the following patent can only signal in one direction, but it is unique in that it provides information about how many doors there are to the exit. [14] This information can be recovered from the number of devices placed one above the other, and from the number of the contact points of these devices, as shown in figure 6. Another advantage is that because the devices stand out from the wall, their number can be counted and shape can be felt, which is very useful for the visually impaired.

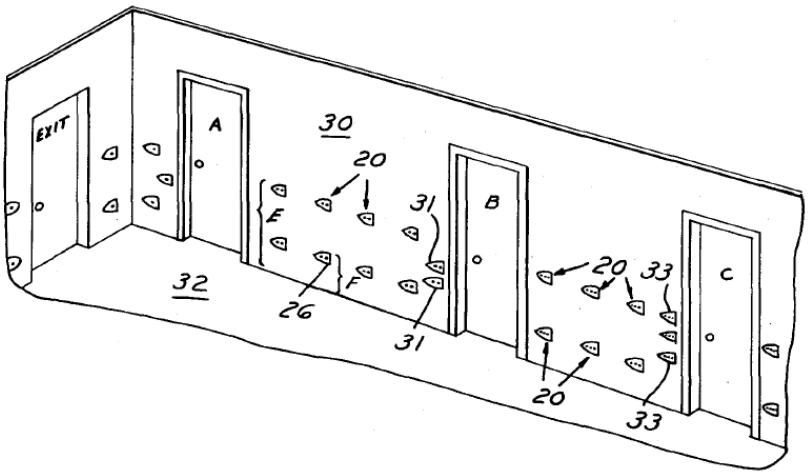


Figure 6: Escape/rescue system [14]

Although it is a good idea to provide information about the number of doors to the exit, this solution should only be used for short corridors. Otherwise, too many devices would have to be installed to indicate the distance of the exit. This would increase the construction cost and interpreting the information necessary for escape would be more difficult.

Finally, I introduce two solutions with lasers. Equipment that may be mounted to the wall is described in the patent [15], and which uses laser beams to project arrows, graphic or alphanumeric symbols onto the floor in the direction of escape. In the basic configuration there are three laser diodes adjusted at different angles, but the number of lasers may be more or less than this figure. The housing for the system can be moved horizontally and vertically to orient the projection within certain limits.

Although the position of the equipment is adjustable, it can only project signals over a short range. In a long corridor several devices should be used to ensure continuous projection of the escape route. To build a complete system would be very costly due to the many diodes that would be needed. One disturbing feature is that the size of the projected signals varies depending on the distance between the device and the point where the signal strikes the floor. A further problem could be if the equipment placed above the exit shines into the eyes of people escaping. As I have already pointed out, the NFPA allow 1000 mc maximum brightness, however, even a low-powered laser greatly exceeds this value and can dazzle a person. There has been a case when a laser used in a disco caused permanent damage to the eyes of the dancers. [16] The patent states that after the fire alarm has been activated the signs are projected continuously, but the signs flashing one after another would be more efficient. Implementing this, however, is difficult if the designation of a section of the escape route can only be achieved using several devices, because then they would have to be synchronised.

The last system employed is built into a false ceiling and can designate the escape route with vertical laser beams. [17] The patent describes three possible solutions. In the first case the laser beam is transmitted through a distribution unit to different glass fibres that transmit light to different points in the corridor. The second possibility is that the beam is transmitted through a mirror to additional mirrors sequentially; the latter direct the beams vertically. The third option is that each beam is created by independent laser diodes. For each option, the order in which the signs are indicated can be changed, so that the direction of escape can also be changed. In the systems contained in the patent the laser does not shine into the eyes (unless someone looks up at the ceiling), but the inventor recommends a very high-powered laser, which can cause damage to the eyes even if a person looks at it accidentally. The patent recommends using a 120 volt laser, which could also be dangerous if water is used to extinguish a fire, as it could cause electrocution.

All three solutions appearing in the above patent are imaginative, but their implementation is costly. In the first case the glass fibre distribution unit makes the system expensive, while in the second case positioning the mirrors exactly would be a costly process. In the third case the system would need a large number of laser diodes, which would demand a lot of financial resources. In the case of long corridors the solution with rotating mirrors would be very difficult to implement, because it would take too much space from the ceiling. Another disadvantage of this method is that coordination of the signs of separate sections of the escape route is difficult.

CONCLUSION

As the article has shown, there are several available solutions to designate and clarify the escape routes. In addition to the patents described several other options are available, but these must satisfy the regulations of the given country.

In choosing one of the many possible solutions, there are other important considerations, among which are the following:

- the material of the cover of the lights on the floor should be strong enough to avoid cracking and breaking, and such that transmission of the light is not reduced due to wear and tear, cleaning and other stress,
- care should be taken so that the light signs do not prevent people from seeing other signs when they are escaping,
- dynamic, not static lights attract peoples' attention more effectively,
- in the case of dynamic signs it is important to ensure that the direction of the light is the same as that of the escape route,
- if the indicator light is static, then arrows should indicate the direction of escape,
- when the direction of the light signs can be changed, this allows the escape route to be designated taking account of the location of the fire, but at present the legislation in force does not permit such a solution,
- the light signs must be synchronized with each other at the junction of the different sections so that the direction of the escape route is clear.

I have pointed out the problem of the compliance with existing standards and controls not being checked when the patent is accepted. This is supported by the fact that patent [13] recommends the decorative use of visual fire alarm devices.

The signalling of escape routes and directions is prescribed by the current regulations. By using visual warning devices that indicate the right direction of escape, it would be possible to determine an escape route which depends on the location of the danger, so it can be adjusted to the situation. The current technical level of development permits such a system to be implemented allowing people in danger to leave a building more easily and faster, where easily understandable light signals are used, which are able to designate the escape route taking into account the location of the fire. As I mentioned, the current law does not allow the implementation of such a system, but I am convinced that if the system I have described were implemented, it would be possible to demonstrate its superiority over the systems presently in operation, which would then require a change in the relevant legislation.

THIS ARTICLE IS SUPPORTED BY TENDER TÁMOP 4.2.2./B-10/1 (RISKS AND ANSWERS IN THE FIELD OF TALENT MAINTENANCE: "KOVÁSZ")

References

[1] Schüller, Attila: Az emberi tényező és a technikai megvalósítások vizsgálata tűzriadók során. In: Hadmérnök, 2/2012, p. 37-46.

[2] Benthorn, L., Frantzich, H.: Fire Alarm in a Public Building: How Do People Evaluate Information and Coose Evacuation Exit? Fire and Materials, 6/1999, p. 311-315.

[3] Miskey, Tamás: Az emberi tényezők és egy új kiürítéstámogató rendszer bemutatása. In: Hadmérnök, 2/2009, p. 57.66.

[4] NFPA 170: Standard for Fire Safety and Emergency Symbols, 2012 Edition. National Fire Protection Association, Quincy, Massachusetts, 2012.

[5] 2/1998. (I. 16.) MüM rendelet – a munkahelyen alkalmazandó biztonsági és egészségvédelmi jelzésekről

[6] 28/2011. (IX. 6.) BM rendelet – az Országos Tűzvédelmi Szabályzatról

[7] NFPA 72: National Fire Alarm and Signaling Code, 2013 Edition. National Fire Protection Association, Quincy, Massachusetts, 2012.

[8] Juei-Chao Chen: Dynamic Emergency Escape Indicator. U.S. Patent 2010/0013658 A1, Jan. 21, 2010.

[9] H. Gerald Gross: Emergency Lighting Strip. U.S. Patent 5 130 909, Jul. 14, 1992.

[10] Maurice Bligh: Color-coded Evacuation Signaling System. U.S. Patent 6 646 545 B2, Nov. 11, 2003.

[11] Daniel J. Tassey, Kenneth F. Newbold: Evacuation Route Having Photoluminescent Indicators. U.S. Patent 6 237 266 B1, May. 29, 2001.

[12] Steve B. LaCasse: Intelligent Directional Fire Alarm System. U.S. Patent 7 626 507 B2, Dec. 1, 2009.

[13] John W. Peterson: Emergency Lighting System and Method. U.S. Patent 7 255 454 B2, Aug. 14, 2007.

[14] Frederick G Schriever: Escape/Rescue System. U.S. Patent 4 385 586, May. 31, 1983.

[15] Mark R. Lehman, Dan Gechtman, Jerome Keith Fuller, Michael A. Hreha: Laser Director for Fire Evacuation Path. U.S. Patent 6 150 943, Nov. 21, 2000.

[16] Reuters and New Scientist staff: Party laser 'blinds' Russian ravers. New Scientist, 2008. http://www.newscientist.com/article/dn14310-party-laser-blinds-russian-ravers.html (18.05.2013)

[17] Gary L. Sweeney: Laser Light Fire Evacuation System. U.S. Patent 5 572 183, Nov. 5, 1996.

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Schweickhardt Gotthilf
schweickhardt.gotthilf@uni-nke.hu

A HIVATÁSOS KATASZTRÓFAVÉDELMI SZERVEK HATÓSÁGI TEVÉKENYSÉGÉNEK VÁLTOZÁSAI 2012. JANUÁR 01-ÉT KÖVETŐEN

Absztrakt

2012. január 01-ét megelőzően a tűzvédelem, polgári védelem és a veszélyes anyagokkal kapcsolatos hatósági tevékenységek, feladatok szervezetileg elkülönült szervezetek hatáskörébe tartoztak. A kialakított rendszer nem tette lehetővé az egyes résszakterületeken folyó hatósági tevékenységek összehangolását, az egységes követelménytámasztást. Az egyes önálló hatóságok saját részterületükön esetenként azonos feladatot eltérő módon hajtottak végre, és az azonos tényállást a hivatásos önkormányzati tűzoltóságok eltérően értelmeztek. 2012. január 01-ét követően a szakterület hatósági tevékenysége során jelentkező feladtok végrehajtása, jogszabályok értelmezése egységessé vált. A szerző a jelen cikkben igyekszik bemutatni a bekövetkezett változásokat, és a két időszak jogszabályi háttere alapján összehasonlítani a hatósági tevékenységet.

Before 1-st of January 2012 the authoritative activities and tasks related to fire protection, civil protection and dangerous substances had been belonged to the organically separated organisations. The established system did not make it possible the coordination of the partial authoritative activities, and the establishments of uniform requirements. The independent authorities from time to time implemented the same task in different way, and the professional municipal fire brigades interpreted differently the same statement of facts. After 1-st of January the implementation of the tasks and the interpretation of legal regulations raised up during the authoritative activities of the special professional fields became unified. The author of this article tries to introduce the occurred changes, and compare the authoritative activities of the two periods in accordance with their legal background.

Kulcsszavak: *hatósági tevékenység, közigazgatási eljárás, katasztrófavédelem ~ authoritative activities, public administration procedure, disaster management*

BEVEZETÉS

2012. január 01-ével egységes hivatásos katasztrófavédelmi szervezet kezdte meg a tevékenységét Magyarországon. A korábban több jogilag és szervezetileg elkülönült szervezet között megosztott tűzvédelmi, iparbiztonsági hatósági és szakhatósági feladatok egységes irányítás alatt lévő állami szervezet tevékenységeként jelennek meg.

Rendészeti, rendvédelmi tevékenységek körébe tartoznak a tűz,- és katasztrófavédelmi hatósági feladatok. A rendvédelmi szervek közé tartozó katasztrófavédelmi szervek is hatóságok, s így rendelkeznek hatósági jogkörrel, melyhez közhatalmi eszközök igénybevételére jogosultak. A hatósági jogkörbe tartozik a hatósági jogalkalmazás kérdése is. A jogalkalmazás során az adott ügyre vonatkozó általános jogszabályi rendelkezések alkalmazása történik. A hatósági tevékenység széles körű jogosultságokat tartalmaz, melyek szabályait jogszabályok határozzák meg. A közigazgatási szervek egyedi ügyekben hoznak döntéseket, melyek jogok és kötelezettségek megállapítása, szankciók alkalmazása és nem utolsó sorban jogviták eldöntését is magukba foglalják. Hatósági tevékenység körébe tartozik továbbá nyilvántartások vezetése, hatósági bizonyítványok és igazolványok kiállítása. A hatósági felügyeleti tevékenység végzése is kötelezettség a hatóságok számára. E feladat során ellenőrzési tevékenységet hajt végre a hatóság, mely során figyelemmel kíséri, hogy a jogosult, engedélyes, stb. a jogszabályok, illetve egyedi hatósági döntések előírásait betartja-e. Hiányosság esetén a hatóság a jogszabályokban meghatározott szankcionálási lehetőségével kényszerítheti ki az előírásoknak megfelelő tevékenység végrehajtását, vagy a tevékenységgel való felhagyást.

A hatósági jogalkalmazás tehát egyrészt közvetlen hatósági jogalkalmazást – jogok és kötelezettségek megállapítása, döntések kikényszerítése -, másrészt a hatósági felügyeletet – hatósági ellenőrzés, szankcionálás - jelent.

2012. JANUÁR 01. ELÖTTI ITŐSZAK HATÓSÁGI TEVÉKENYSÉGÉNEK ÁTTEKINTÉSE

2012. január 01-et megelőzően a katasztrófavédelemi szakterületi hatósági feladatokat – tűzvédelmi, iparbiztonsági, polgári védelmi - az államigazgatás különböző helyét elfoglaló szervezetek végezték. Hatósági feladatot látott el az önkormányzat, hivatásos önkormányzati tűzoltóság, a polgári védelmi szervezet, a katasztrófavédelem és a polgármester. Elkülönültek a tűzvédelmi és a polgári védelmi feladatokat végrehajtó szervezetek is. Önállóan az önkormányzatok részét képező hivatásos tűzoltóságok, a katasztrófavédelmi szervek területi és központi szervei láttak el hatósági feladatokat. A tűzvédelmi, polgári védelmi, katasztrófavédelmi és veszélyes anyagokkal kapcsolatos feladatok végrehajtását önálló törvények szabályozták.[1,2,3,4] Ugyanígy a szakhatósági feladatoknak is több szervezet volt a címzettje.

A tűzvédelem területén általánosságban első fokú hatósági jogkörrel rendelkeztek a hivatásos önkormányzati tűzoltóságok (a továbbiakban: tűzoltóság), s jogszabály határozta meg, hogy mely esetekben rendelkezett ilyen jogkörrel a területi, illetve központi katasztrófavédelmi szervezet. A tűzvédelmi hatósági jogkört általánosságban a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról szóló 1996. évi XXXI. törvény szabályozta,[1] s szabályozza, írja elő a hatósági feladatokat. A hatósági feladatokat ellátó szervezetek több alkalommal változtak. A tűzvédelmi hatósági jogkör egyes időszakokban az önkormányzati jegyzőhöz került telepítésre. Ebben az időszakban a tűzoltóság tűzmegelőzési feladatot ellátó szakemberei ellenőrzést és döntés előkészítést hajtottak végre. A másodfokú

[1] A törvény 11. § - 14. §. szabályozza a hatósági feladatokat. A törvény ezen belül önálló címként fogalmazta meg a tűzvizsgálati tevékenységet.

hatósági jogkört ennek megfelelően a területi, illetve központi katasztrófavédelmi szerv látta el. [5]

A hivatásos önkormányzati tűzoltóságok az alábbiak szerint rendelkeztek általános elsőfokú hatósági jogkörrel:

a) az épületek, építmények tűzvédelmi használati előírásai, valamint a tűzoltóságok beavatkozásával kapcsolatos előírások alól, - azonos biztonságot nyújtó előírások megtétele mellett - kérelemre eltérést engedélyezhettek,
b) a beépített tűzvédelmi berendezések létesítési és használatbavételi ügyeiben jártak el,
c) tűzvédelmi hatósági ellenőrzést tartottak,
d) jogszabályban meghatározott esetekben tűzvédelmi bírságot szabtak ki,
e) lefolytatatták a tűzvizsgálati eljárást,
f) hatósági bizonyítványt adtak ki,
g) a tűz- vagy robbanásveszélyes munkahelyen azt a munkavállalót, aki a munkakörével kapcsolatos tűzvédelmi előírásokat, illetőleg a tűzjelzésre vagy tűzoltásra szolgáló eszközök, felszerelések használatát nem ismerte, a szükséges ismeretek megszerzéséig az ott folytatott tevékenységtől eltilthatták,
h) a tűzvédelmi ellenőrzés, a tűzvizsgálati eljárás során feltárt hiányosságok, a tűzkárok megelőzése érdekében felhívhatták az ügyfél figyelmét a jogszabálysértések megszüntetésére, és szükség esetén tűzvédelmi hatósági intézkedést tettek,
i) az üzemeltetést, a tevékenység folytatását, az anyagok tárolását - amennyiben a rendeltetéstől eltérően közvetlen tűz- vagy robbanásveszélyt jelent - a tűzvédelmi követelmények érvényesítéséig szüneteltethették,
j) a jogszabályok keretei között megállapíthatták a tűzvédelmi kötelezettségeket.

Mind emellett különböző pl. építési hatósági tevékenységet meghatározó kormányrendelet ettől eltérő hatósági jogköröket is megállapíthatott. A másodfokú hatóság kijelölésében törés volt, tekintettel arra, hogy a főváros területén az Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: OKF) került megnevezésre másodfokú hatóságként.

Tűzmegelőzési területen a tűzoltóságok jogszabályok keretei között ellenőriztek, engedélyeztek, bírságoltak, s szakhatóságként jártak el. A tűzvédelmi bírságolás területén szintén megjelent az osztott hatáskör, mely jogszabályban meghatározottak szerint hatalmazta fel mind a tűzoltóságokat és a katasztrófavédelmi szerveket bírságolásra. A hatósági jogkörök alkalmazása során az egyes hivatásos önkormányzati tűzoltóságok jogértelmezésben eltérések voltak tapasztalhatók.

Tűzvédelmi bírságot többek között az alábbi esetekben lehetett kiszabni:

1. - a tűzvédelmi szabályt megszegték úgy, hogy az közvetlen tűz- vagy robbanásveszélyt, illetőleg tüzet idézett elő, vagy veszélyeztette a személyek biztonságát, akadályozta a mentésüket,
2. - ha elmulasztották a tűzjelzéshez és tűzoltáshoz szükséges eszköz, felszerelés, készülék, stb. karbantartását, vagy ellenőrzését, vagy rendeltetésétől eltérően használták ezeket,
3. - ha a munkáltató a törvényben előírt határidőre nem gondoskodott a munkavállalók tűzvédelmi oktatásáról,
4. - ha a kötelezettek nem készítették el a tűzvédelmi szabályzatot, illetve nem gondoskodtak annak megismertetéséről és betartatásáról,
5. - ha a tervező, illetőleg a kivitelező valótlan nyilatkozatot adott a tűzvédelmi szabályok, előírások érvényesítésére vonatkozóan,
6. - ha a tűzvédelmi szakvizsgához kötött tevékenységet szakvizsga nélkül végzték.

A bírság összegének nagyságának megállapításánál nem volt egységes a hiányosság mértékéhez igazodó követelményrendszer.

Az OKF 2012 előtti hatásköre nem adott lehetőséget a hatósági tevékenység országosan egységes értelmezésre. Az OKF és szervezeti egységei által kiadott tájékoztatók, szakmai állásfoglalások a hivatásos önkormányzati tűzoltóságok számára csak iránymutatásként voltak alkalmazhatók. Az első fokú tűzvédelmi hatóság döntése ellen az OKF, vagy területi szerve a jogorvoslati eljárás során egységes jogértelmezést alkalmazva döntött. Így a másodfokú eljárások egyfajta egységesítési szerepet is betöltöttek.

A tűzvédelmi szakvizsgáztatás hatósági feladatai megosztásra kerültek a tűzoltóság és a katasztrófavédelmi szervek között. Az OKF a tűzoltó és jelzőberendezések oktatása vonatkozásában végezte kizárólagosan a hatósági tevékenységet. Ez magába foglalta a nyilvántartást és a vizsgáztatási feladatokat. A szakvizsgáztatáshoz szükséges tananyag egységes követelménykeretét minden szakvizsgaágra az OKF adta meg.

A tűzoltósági hatósági feladatok között megjelent a tűzvizsgálati eljárás, melynek lezárásaként hatósági bizonyítvány kiadására kerülhetett sor.

A veszélyes áru szállításával és a veszélyes anyagot előállító, felhasználó és tároló ipari üzemekkel kapcsolatos hatósági engedélyezési és felügyeleti tevékenység is több szervezet feladatai között jelent meg. A tűzoltóság, a rendőrség, a közlekedési hatóság, a Magyar Kereskedelmi Ellenőrzési Hivatal, Vám és Pénzügyőrség és még számos szervezet vett részt hatóságként, vagy szakhatóságként a veszélyes anyagokkal és áruval kapcsolatos hatósági tevékenységben. Ebbe a körbe tartozott az egyes veszélyes anyagok előállítása, különböző szállítóeszközön történő szállítása, feldolgozása és tárolása. A veszélyes anyagokkal kapcsolatos feladatokat és tevékenységeket 2004. május 01-ét követően az Európai Unióhoz való csatlakozástól számítva minden vonatkozó közösségi jogszabály is szabályozta.

A katasztrófavédelmi szervek csak 2007 májusától rendelkeztek a veszélyes áruk közúti szállítása területén önálló megállítási joggal. Ezt megelőzően csak a rendőrséggel, vagy a közlekedési felügyelettel közös ellenőrzések során volt lehetőségük ellenőrzésre a katasztrófavédelmi szervezeteknek. Az egyes veszélyes árukat szállító közúti járművek útvonalának kijelöléséről szóló 122/1989 (XII.5.) MT rendelet több hatóságot jelölt ki. Településen belül a jegyző, főváros, illetve megyén belüli szállítás esetén a területileg illetékes közlekedési hatóság, míg több megyén és a határon átnyúló szállítás esetén a Útgazdálkodási és Koordinációs Igazgatóság rendelkezett hatóságként útvonal kijelölési joggal. A katasztrófavédelmi szervek az útvonal kijelölésében szakhatóságként működtek közre. A közúton történő ellenőrzésre a rendőrséggel és a közlekedési felügyeletekkel együttműködve a megyei katasztrófavédelmi igazgatóságok, míg a főváros területén a Fővárosi Tűzoltóparancsnokság rendelkezett jogosítványokkal. Amennyiben a közúti ellenőrzés során megállapítást nyert, hogy a jármű útvonal engedélytől eltérő útvonalon közlekedik, akkor a hatóság szabálysértési feljelentéssel élhetett. 2007-től kezdődően a katasztrófavédelmi szervek önállóan folytattak hatósági ellenőrzéseket. Az ellenőrzéshez kapcsolódóan a szabálytalanság megszüntetéséig feltartóztatási és bírságolási jog is megillette a katasztrófavédelmi szerveket. [6]

A veszélyes ipari üzemek tekintetében az OKF hatósági jogosultságokkal rendelkezett, de a Magyar Kereskedelmi Ellenőrzési Hivatalt szakhatóságként be kellett vonni.

A TANÁCS 96/82/EK IRÁNYELVE (1996. december 9.) a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyeinek ellenőrzéséről alapján került kialakításra a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 1999. évi LXXIV. törvény (a továbbiakban: katasztrófavédelmi törvény) IV. fejezete.[7] A katasztrófavédelmi törvény egyértelműen meghatározza a szabályozásba bevont tevékenységek körét, a tevékenységgel kapcsolatos szakhatósági feladatokat, a veszélyes létesítmények üzemeltetőinek, a kormányzatnak és az önkormányzatoknak a súlyos ipari balesetek megelőzésével, az azokra való felkészüléssel és azok elhárításával kapcsolatos feladatait, meghatározza a közvélemény

tájékoztatásával kapcsolatos kötelezettségeket. A törvény megfogalmazta, hogy veszélyes ipari üzemre, veszélyes létesítményre építési engedély, használatbavételi engedély, továbbá veszélyes tevékenység megkezdésének engedélyezése csak az Országos Katasztrófavédelmi Főigazgatóság engedélye alapján adható. A szabályzás veszélyes üzemek esetében az alsó és felső küszöbértéket határozott meg. 2010-ben a 89 alsó és 71 felső küszöbértékű veszélyes üzem volt hazánkban. Az üzemeltető kötelezettségeinek teljesítését – biztonsági elemzés és biztonsági jelentés valóságtartalma, stb.- teljesítését az katasztrófavédelmi szervek hatósági ellenőrzés keretében ellenőrizték. Üzemi, vagy üzleti titok esetében a hatóság jogköre volt a nyilvánosságra hozatal esetén megállapítani, hogy mely részek nem kerülhetnek nyilvánosságra.

A hatóság a településrendezési tervezés területén is jogosultságokat kapott azzal, hogy a veszélyes üzemek körüli veszélyességi határokat kijelölte, s azokat a településrendezési tervben fel kellett tüntetni. A hatóság közreműködése nélkül nem lehetett a veszélyességi övezeten belüli fejlesztéseket végrehajtani.

Összességében megállapítható, hogy az egyes hatóságok által hozott egyedi döntésekről nem történt meg a többi hatóság tájékoztatása. Hiányzott a rendvédelmi feladatokat ellátó szervezetek szakirányítása, az egységesség.

2012. JANUÁR 01-ÉT KÖVETŐ VÁLTOZÁSOK

Az év kezdetével a törvényi szabályozás alapján kialakult az egységes hivatásos katasztrófavédelmi szerv. A tűzvédelem, a polgári védelem szervezete megváltozott, s kialakításra került az iparbiztonsági szakterület. A hivatásos katasztrófavédelmi szervek hatósági feladataiban is változások következtek be, melyek igazodtak a szervezeti változásokhoz. A központi, területi és helyi szervezeti felépítés továbbra is megmaradt. Központi szerv esetén is a BM OKF. A területi szintű szervezetek feladatát a Megyei Katasztrófavédelmi igazgatóságok látják el. A területi és helyi szint az, ahol a legnagyobb változás következett be. Kialakításra kerültek a Katasztrófavédelmi Kirendeltségek, amelyek alárendeltségébe kerültek a Hivatásos tűzoltóságok. Jelenleg 65 kirendeltség és 105 hivatásos tűzoltóság működik. A közigazgatásban 2013. január 01-től 175 járás került kialakításra, melyekhez az illetékességi területmódosításra került. Kirendeltségek esetében területi átfedések fordulnak elő.

A hivatásos katasztrófavédelmi szervezet a Kat. IV. fejezetének hatálya alá tartozó üzemek tekintetében ún. „supervisori” jogosultságot kapott, mely megteremtette az integrált katasztrófavédelmi ellenőrzés alapját. Az ellenőrzések koordinálásán túlmenően az ellenőrzések eredményeit tartalmazó nyilvántartás vezetése és annak értékelése is hozzá tartozik a tevékenységhez. [8]

A tűzvédelemmel kapcsolatos piacfelügyeleti eljárás továbbra is a hivatásos katasztrófavédelmi szervek hatáskörébe maradt. Változás annyiban történt, hogy az eljáráshoz kapcsolódó helyszíni hatósági ellenőrzések végrehajtására a kirendeltségek lettek kijelölve. A hatósági eljárás végét esetlegesen lezáró bírságolási szempontok kerültek meghatározásra.

Tűzvédelem területén jelentkező hatósági tevékenység végrehajtásában is változások történtek. Az egyik jelentős módosulás, hogy kormányrendeletben [2] általános első fokú hatóságként a katasztrófavédelmi kirendeltségek (a továbbiakban: kirendeltségek) kerültek kijelölésre. Ezzel a tűzoltóságok számára az önálló hatósági tevékenység megszűnt, ők csak a tűzoltási és kárelhárítási tevékenységet végzik. A hatósági feladatok ellátásában természetesen részt vesznek, mint a hivatásos katasztrófavédelmi szervek egyik szervezete.

[2] 259/2011. (XII. 7.) Korm. rendelet a tűzvédelmi hatósági feladatokat ellátó szervezetekről, a tűzvédelmi bírságról és a tűzvédelemmel foglalkozók kötelező élet- és balesetbiztosításáról

Ilyen feladat a tűzvizsgálati tevékenyég megkezdése, hatósági ellenőrzésekben való részvétel, egyes a hatósági eljárásokhoz kapcsolódó eljárási cselekmények végrehajtása. [9] A tűzvédelem területén továbbra is megmaradtak az első fokú hatósági eljárások címzettjeinek elkülönülései. Általános első fokú hatáskörrel a kirendeltségek rendelkeznek, meghatározott esetekben, ügykörökben a területi és a központi szervek váltak a közigazgatási eljárás szabályai szerint hatáskörök címzettjei. Általános másodfokú hatóságként a hivatásos katasztrófavédelmi szervek területi szervei kerültek kijelölésre, míg azokban az esetekben, ahol elsőfokú eljárásként a területi szerv járt el a központi szerv lett másodfokú hatóságként meghatározva. A kirendeltségek végzik az tűzmegelőzési tevékenységet, melyben nem következett be változás.

A tűzvédelmi bírságolás rendszerében is módosulás következett be azzal, hogy a veszélyesség függvényében meghatározásra kerültek azok az esetek, amikor kötelező a bírságolás kiszabása. [3] Ez a megoldás egységessé tette a bírságolási gyakorlatot, s csökkentette a szubjektív elemeket. A bírságolási gyakorlat is egységessé vált.

A tűzvédelem területén a tűzvizsgálati tevékenyégben is változás következett be. .[9] A tűzvizsgálati tevékenység végzésére a területileg illetékes hatóság vezetője biztosítja a személyi és tárgyi feltételeket. Ebben az esetben a kirendeltség az a hatóság, mely a vizsgálatot lefolytatja a Ket.[4] szabályai szerint. Az eljárásban a hivatásos tűzoltóság tűzoltásvezetői jogosultsággal rendelkező állománya résztvevője, illetve megkezdője a vizsgálati eljárásnak.

A tűzmegelőzési szakterületen a korábbi hivatásos önkormányzati tűzoltóság hatásköreit a kirendeltségek vették át. A tevékenység tartalmában nem következett be változás.

A hivatásos katasztrófavédelmi szerveknél új feladatként jelentkezik a kéményseprő ipari közszolgáltatásokkal kapcsolatos hatósági feladat, mely egyrészt a kirendeltségek, másrészt a területi szervek hatáskörébe tartozik. A kéményseprő ipari közszolgáltatást a szolgáltatási tevékenység megkezdésének és folytatásának általános szabályairól szóló 2009. évi LXXVI. törvény szerint kell bejelenteni. A szolgáltatás közben feltárt hiányosságok esetén a szolgáltató felhívja a tulajdonost az időszakos ellenőrzés végrehajtásának engedélyezésére, vagy a hiányosság kijavításra. Amennyiben ennek a felhívásnak az építmény tulajdonosa, használója nem tesz eleget, úgy a területileg illetékes kirendeltség hatósági jogkörében tűzvédelmi bírságot szab ki. Természetesen a bírságolást megelőzi hatósági ellenőrzés a helyszínen. Magának a közszolgáltatónak a hatósági és szakmai felügyeletét a területileg illetékes hivatásos katasztrófavédelmi szerv hajtja végre hatósági jogkörében eljárva. A területi szerv a szolgáltatás felügyelet körében nyilvántartást vezet a közszolgáltatókról, ellenőrzi azt, hogy a közszolgáltató a bejelentés köteles tevékenyégét jogszabályok előírásai szerint végzi és nem utolsó sorban a közszolgáltatóval szembeni bejelentéseket vizsgálja ki. A közszolgáltatót kétévente kell ellenőrizni. A közszolgáltatók névjegyzékét a területi szerv a honlapján teszi közzé.

A Magyar katasztrófavédelem rendszerében az iparbiztonság új önálló szakterületként jelent meg. Létrejött egy egységes iparbiztonsági hatóság, amely a megelőzési munka keretében szigorú hatósági felügyeletet lát el a veszélyes anyagot gyártó, tároló, forgalmazó és felhasználó üzemek felett.

---

[3] 259/2011. (XII. 7.) Korm. rendelet a tűzvédelmi hatósági feladatokat ellátó szervezetekről, a tűzvédelmi bírságról és a tűzvédelemmel foglalkozók kötelező élet- és balesetbiztosításáról 1. számú melléklete. Ebben a mellékletben szerepelnek az egyes szabálytalanságokhoz kapcsolódó bírságösszegek.

[4] 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól előírásai szerint kell a hatósági tevékenységet végezni. 2000. január 01-ét követően kialakított katasztrófavédelmi rendszerben az államigazgatási eljárás általános szabályairól szóló1957. évi IV. törvény előírásai szabályozták a hatósági tevékenység végzését.

A hatósági tevékenység kiterjesztődött az alsó küszöbérték alatti üzemekre is. Ezzel a veszélyes anyagokkal foglalkozó üzemek száma megközelítette a 700-at. A hatóság a jogszabályi követelmények alapján megújította az üzemekről meglévő nyilvántartását. A hatósági tevékenység szankció rendszere kibővült, s megnőtt az olyan esetek száma, mely bírságolást von maga után. A hatóság által hozott döntést felügyeleti jogkörben nem lehet megváltoztatni, illetve megsemmisíteni. Ez egy erős jogosítvány a hatóság számára, mely növeli a biztonságot. A veszélyes üzemek számára katasztrófavédelmi hozzájárulás került bevezetésre az üzemek biztonságának növelése érdekében. Az az üzem, mely a kockázat szintjének csökkentését szolgáló műszaki intézkedést(eket) végez, úgy a befizetésének egy negyedét visszaigényelheti.

A katasztrófavédelmi hozzájárulás intézménye 2012. augusztus 24-től megszüntetetésre került.

A hozzájárulás megszüntetése a katasztrófavédelmi megelőzési feladatokra szánt összeg ráfordíthatóságát csökkentette. A katasztrófavédelmi bírság rendszere hasonló kialakítást nyert, mint a tűzvédelmi bírság. Meghatározott szabálytalanságok esetén meghatározott mértékű bírság kiszabása történik meg. A bírság mértéke 300.000,- Ft és 3.000.000,- Ft közé esik, s nagysága a szabálytalanság súlyosságához igazodik.

A veszélyes anyagok közúti szállítását 2007 óta ellenőrizheti önállóan a katasztrófavédelmi szervezet. Az ellenőrzés tartalmában nem történt változás. Nem változtak az ellenőrzésre vonatkozó jogszabályok, ezért a szakterület ezen részén csak az ellenőrzésbe bevonhatók köre módosult a hivatásos katasztrófavédelmi szervek szervezeti változásának megfelelően. A hivatásos katasztrófavédelmi szervek ellenőrzés köre kiterjed a vasúti és belvízi veszélyes anyagok szállításokra is, mely ellenőrzések végrehajtására és a bírságolás rendjére kormányrendelet került kiadásra.[5] A BM OKF által 2011-ben végzett telephelyi és közúti ellenőrzés számáról készített táblázatok a mellékletben találhatók. A táblázatok összehasonlításából összességében az állapítható meg, hogy az ellenőrzések számával nőtt a hiányosságok száma, ellenben az intézkedések száma csökkent 2011-ben 2010-hez képest. A 2012. évi ellenőrzések adatainak összevetését a hivatásos katasztrófavédelmi szervek szervezeti változásai miatt nem végeztem el. Az értékeléshez legalább két egymás után következő évi adataira van szükség. Ezért azt legkorábban 2014. év elején célszerű elvégezni.

A polgári védelmi tevékenység hatósági feladataiban mélyreható változás nem történt. A polgári védelmi feladatok további körében alapvető változások történtek, de ezek nem tartoznak a cikkben tárgyalt témához. A hivatásos katasztrófavédelmi szerveztek polgári védelmi területen megjelenő egyes hatósági feladatait az egyes jogszabályok határozzák meg.

Az új hatósági feladatok teljesítéséhez szükséges volt az egységes katasztrófavédelmi felsőfokú képzés megteremtése a Nemzeti Közszolgálati Egyetemen. A katasztrófavédelmi szakon folyó képzés célja, hogy a végzett hallgatók alkalmasak legyenek az általános katasztrófavédelmi igazgatás részterületein (katasztrófa-megelőzés, katasztrófa-elhárítás szervezése, helyreállítás, polgári védelmi felkészítése feladatok ellátása), illetőleg a tűzmegelőzési, tűzoltási-műszaki mentési, tűzvizsgálati, az ezzel kapcsolatos felkészítés és az elsődleges katasztrófa-elhárítási tevékenységek, továbbá az iparbiztonsággal kapcsolatos általános megelőzési és hatósági feladatok végzésére. [10]

[5] 312/2011. (XII. 23.) Korm. rendelet a hivatásos katasztrófavédelmi szerv eljárásai során a veszélyes áruk vasúti és belvízi szállításának ellenőrzésére és a bírság kivetésére vonatkozó egységes eljárás szabályairól, továbbá az egyes szabálytalanságokért kiszabható bírságok összegéről, valamint a bírságolással összefüggő hatósági feladatok általános szabályairól.

ÖSSZEFOGLALÁS

A cikkben kizárólag a hatósági tevékenység változásait vettem górcső alá. A szervezeti és egyéb változásokat nem érintettem, mert az külön önálló értékelést kíván. 2012. január 01-től kezdődően még csak egy teljes év telt el, mely nem alkalmas a megváltozott hatósági rendszer átfogó értékelésére. A hatósági feladatokhoz kapcsolódó statisztikai adatok mint ahogy az új követelmények esetében történik mindig kimagasló eredményeket mutatnak. Egy folyamat méréséhez megfelelő időt kell biztosítani. Az eltelt időszak alatt mind a kormányzat, mind a hivatásos katasztrófavédelmi szerv részről kisebb szervezeti, változtatások, pontosítások és jogszabályi igazítások történtek, melyek a végrehajtás szervezeti és személyi oldalait érintették.

Megtörtént a hatósági tevékenység végrehajtásban résztvevő állomány képzése, melyet rendszeres - az eljárás tapasztalatait felhasználó azokat magába foglaló – továbbképzések követnek. [11]

Az eltelt közel másfél év alatt megállapítható, hogy a hatósági rendszer ilyen mértékű megváltoztatása, átalakítása jó elgondolásnak minősült, de valójában legalább még két teljes év szükségeltetik ahhoz, hogy a kisebb javítások megtörténjenek és a rendszer működéséről objektíven lehessen véleményt alkotni.

Felhasznált irodalom

[1] 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról;

[2] 1996. évi XXXVII. törvény a polgári védelemről;

[3] 2004. évi CV. törvény a honvédelemről és a Magyar Honvédségről;

[4] 1999. évi LXXIV. törvény a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről;

[5] Muhoray Árpád pv. mk. alezredes, a katasztrófavédelem helyezte Magyarországon, az Országos Főigazgatóság és a Megyei Igazgatóságok létrehozásának tapasztalatai file:///F:/doktorijelentkez%C3%A9s/2012-13If%C3%A9l%C3%A9v/tudom%C3%A1nyoscikk/KATASZTR%C3%93FAV%C3%89DELEM%20HELYZETE%20MAGYARORSZ%C3%81GON___.htm (letöltve 2013. 05. 10. 13.20 óra)

[6] http://hadmernok.hu/2010_2_bardos.pdf (letöltve:2013. 05. 15. 15.22 óra)

[7] Lauer János. Prof.Dr Solymosi József . Dr Vincze Árpád veszélyes üzemek biztonsági értékelése http://www.zmne.hu/tanszekek/vegyi/docs/fiatkut/pdf/lauer_03_01.pdf (letöltve: 2013.05.10. 13.15 óra)

[8] Kátai-Urbán Lajos, Vass Gyula: Development of Hungarian System for Protection against Industrial Accidents. In: Jozef Ristvej (szerk.)18. medzinárodná vedecká konferencia Riešenie krízových situácií v špecifickom prostredí. Zilina, University of Zilina, pp. 229-239.(ISBN:978-80-554-0699-2).

[9] Dr. Schweickhardt Gotthilf A tűzvizsgálati tevékenységre való felkészítés áttekintése http://www.vedelem.hu/letoltes/tanulmany/tan406.pdf (letöltve: 2013.06.08. 15.15 óra)

[10] Kátai-Urbán Lajos: Industrial Safety Preparation in the Higher Education System of Disaster Management in Europa and in Hungary: Iparbiztonsági felkészítés az európai és magyar katasztrófavédelmi felsőfokú képzés rendszerében. In: Dobor József (szerk.) Proceedings "Safety of Industrial Establishments 2013. International Scientific Conference on Industrial Safety: Előadás gyűjtemény "Veszélyes üzemek biztonsága" Nemzetközi Iparbiztonsági Tudományos Konferencia. Budapest: Nemzeti Közszolgálati Egyetem, 2013. pp. 79-100. (ISBN:978-615-5305-08-5).

[11] Dr. Muhoray Árpád: a katasztrófavédelem aktuális feladatai http://mhtt.eu/hadtudomany/2012_e_Muhoray_Arpad.pdf (letöltve: 2013. 06. 08. 15.20 óra)

Felhasznált jogszabályok jegyzéke:

[1] 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról;

[2] 1996. évi XXXVII. törvény a polgári védelemről;

[3] 2004. évi CV. törvény a honvédelemről és a Magyar Honvédségről;

[4] 1999. évi LXXIV. törvény a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről;

[5] 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól,

[6] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról,

[7] 2012. évi XC. törvény a kéményseprő ipari közszolgáltatásról;

[8] 259/2011. (XII. 7.) Korm. rendelet a tűzvédelmi hatósági feladatokat ellátó szervezetekről, a tűzvédelmi bírságról és a tűzvédelemmel foglalkozók kötelező élet- és balesetbiztosításáról

[9] 342/2012. (XII. 11.) Korm. rendelet a kéményseprő ipari közszolgáltatás ellátásáról szóló 2012. évi. XC törvény végrehajtásáról;

[10] 115/1996. (VII. 24.) Korm. rendelet a tűzvédelmi hatósági tevékenység részletes szabályairól, a hivatásos önkormányzati tűzoltóságok illetékességi területéről.

[11] 79/2007. (IV. 24.) Korm. rendelet a tűzvédelmi hatósági feladatokat ellátó szervezetekről,

[12] 259/2011. (XII. 7.) Korm. rendelet a tűzvédelmi hatósági feladatokat ellátó szervezetekről, a tűzvédelmi bírságról és a tűzvédelemmel foglalkozók kötelező élet- és balesetbiztosításáról,

[13] 208/2011. (X. 12.) Korm. rendelet a katasztrófavédelmi bírság részletes szabályairól, a katasztrófavédelmi hozzájárulás befizetéséről és visszatérítéséről,

[14] 312/2011. (XII. 23.) Korm. rendelet a hivatásos katasztrófavédelmi szerv eljárásai során a veszélyes áruk vasúti és belvízi szállításának ellenőrzésére és a bírság kivetésére vonatkozó egységes eljárás szabályairól, továbbá az egyes szabálytalanságokért kiszabható bírságok összegéről, valamint a bírságolással összefüggő hatósági feladatok általános szabályairól;

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Dobor József - Szendi Rebeka
rebeka.szendi@katved.gov.hu

VESZÉLYES ÜZEMEK AZONOSÍTÁSA ÉS A KAPCSOLÓDÓ HATÓSÁGI TEVÉKENYSÉG(EK)

Absztrakt

Az elmúlt időszakban számos olyan súlyos ipari baleset történt, melynek hatása több országot is érintett. A hasonló események megelőzéséhez összehangolt nemzetközi fellépés, egységes jogi szabályozás és azonos szemlélet szerint kialakított eljárások és módszerek szükségesek. Ezt felismerve az Európai Unióban több rendelet és irányelv született, melyek célja az ipari katasztrófák elleni hatékony védekezés. A hatályos szabályzókat a jogharmonizáció keretében Magyarország is integrálta jogrendjébe. A cikk célja annak ismertetése, hogy miképp változtak az uniós és a hazai katasztrófavédelemmel kapcsolatos fő szabályozók, illetve annak bemutatása, hogy hogyan történik a gyakorlatban – a hazánkban jelenleg hatályos jogszabályoknak megfelelően - a veszélyes üzemek azonosítása, és melyek a hatóság ezzel kapcsolatos engedélyezési és felügyeleti feladatai.

In the last space of time many serious accidents happened, whose impacts affected more countries. For the prevention of similar events harmonized international action, standardized regulation and new procedures and methods, framed in pursuance of equal view are required. After realizing this there have been worked out more regulations and directives in the European Union (EU), whose purpose is the effective protection against industrial disasters. Within the frame of the harmonization of laws the valid rules have been integrated into the law and order of Hungary. The aim of this article is to represent how the EU's and Hungarian main rules, related to disaster management had been changing; respectively demonstrating how the identification of hazardous plants happens in practice, in accordance with the currently effective rules in Hungary, and what kind of licensing and supervision task the authorities have related to this activity.

Kulcsszavak: *Seveso, veszélyes üzem, üzemazonosítás, küszöbérték alatti üzem, katasztrófavédelem ~ Seveso, hazardous plant, identification of plants, below tier plant, disaster management*

1. BEVEZETÉS

A veszélyes anyagok előállítása, felhasználása és tárolása magában hordozza a súlyos ipari balesetek kialakulásának kockázatát, [1] melyek az eddigieknél jóval nagyobb veszélyt jelentenek mind az emberek, mind pedig az őket körülvevő természetes illetve mesterséges környezet számára.

Az elmúlt évtizedekben bekövetkezett súlyos ipari katasztrófák hatásai sokszor átnyúltak egy-egy ország határain, s ez rávilágított arra, hogy megelőzésük és az ellenük való védekezés csak egységes jogi szabályozással és az eljárások, eszközök és módszerek összehangolásával lehetséges.

Ennek eredményeképp az Európai Unióban számos egyezmény és irányelv született, melyeket később hazánk is integrált jogrendjébe. [2]

A Magyarországon érvényben lévő jogszabályok 2011. évi módosítását követően az új katasztrófavédelmi törvény, illetve a hozzá kapcsolódó kormányrendelet részletesebben meghatározza a veszélyes üzemekkel kapcsolatos hatósági feladatokat, emellett az új szabályozás egy új üzemtípust nevesít, ami szükségessé tette – az alsó és felső küszöbértékű üzemek mellett - ezen veszélyes üzemek hatóság általi azonosítását, mely tevékenység jelenleg is folyamatban van. [3] [4]

Jelen cikkben főként a vonatkozó irodalmak és jogszabályok feldolgozásával, valamint a munkám során gyűjtött anyagok és szerzett tapasztalatok felhasználásával szeretném bemutatni a vonatkozó EU-s irányelvek és rendeletek, illetve az ezek magyarországi jogharmonizációja során kialakult hazai jogszabályok rövid ismertetését, továbbá a veszélyes üzemek azonosításának helyzetét és az ehhez kapcsolódó hatósági engedélyezési, illetve felügyeleti tevékenységet

2. NEMZETKÖZI SZABÁLYOZÁS

Az elmúlt évtizedekben számos olyan katasztrofális esemény következett be, mely rámutatott a veszélyes anyagokkal kapcsolatos tevékenységek kockázataira, a megelőzéssel, illetve a kockázat és a lehetséges hatás csökkentésével kapcsolatos egységes jogi szabályozás fontosságára. [5]

Ilyen volt például az 1976-ban az olaszországi Sevesoban történt súlyos esemény, melynél egy üzemben a triklór-fenol előállítása során túlhevítés miatt igen mérgező anyag tetraklór-dibenzo-paradioxin keletkezett, mely kijutott a levegőbe. A kikerülő anyag igen nagy területen terjedt szét, beterítve Seveso falut és több ezer ember maradandó egészségkárosodását, továbbá a növények és a talaj szennyeződését eredményezte. [6]

A különböző országokban bekövetkezett súlyos következményekkel járó ipari balesetek, valamint az egyes tagállamokban megfigyelhető komoly eltérések az ipari tevékenységek irányítása és ellenőrzése terén szükségessé tették nemzetközi és regionális jogszabályok kialakítását a súlyos balesetek veszélyeinek megelőzése és csökkentése terén. Ennek első lépéseként megalkotásra került az egyes ipari tevékenységekkel járó súlyos baleseti kockázatokról szóló 82/501/EGK, vagyis a Seveso I. Irányelv, mely nevét az 1976-os eseményről kapta. [7] Célja az volt, hogy széleskörű szabályozás, valamint szigorú ellenőrzés révén csökkentsék a veszélyes üzemekben bekövetkező ipari balesetek kockázatát, valamint különféle védelmi intézkedésekkel minimalizálják a balesetek lehetséges hatásait. [5] Az irányelv fontos eleme volt olyan hatóságok létrehozása, melyek ellátják a veszélyes létesítmények felügyeletét, ellenőrzését. [8]

1984-ben Indiában, Bophalban következett be ipari szerencsétlenség, melynek során egy növényvédőszert előállító üzem földalatti tartályából metil-izocianát szabadult ki, aminek hatására több mint 3100 ember vesztette életét és további 400000-en szenvedtek

egészségkárosodást. Azóta a balesettel összefüggésbe hozható halálos áldozatok száma 16000-re tehető. [9] 1986-ban pedig a svájci Baselben történt súlyos baleset, amikor egy rovarirtó szert raktározó gyárban tűz ütött ki. A szabadba kikerült füst a lakosságnál szem- és légzőszervi irritációt okozott, az oltás során keletkezett nagy mennyiségű szennyezett víz pedig a Rajnába jutott és több száz km hosszan kipusztította a folyó élővilágának jelentős részét. [6]

A bophali és baseli események tapasztalati alapján a Seveso I. Irányelv módosításra került, melynek eredményeképp megszületett a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyeinek ellenőrzéséről szóló 96/82/EK Irányelv, azaz a Seveso II., melynek célja a Seveso I. Irányelv hatékonyabb végrehajtása, alkalmazási körének kiszélesítése, valamint a tagállamok közti információcsere fokozása volt. Fontos új elemként jelenik meg a veszélyhelyzeti tervek alkalmazhatóságának gyakorlati kipróbálása, illetve az üzemek létesítésekor, vagy fejlesztésekor a területfejlesztési tervekben – a hosszú távú igényeket figyelembe véve – megfelelő távolság tartása a lakott, vagy védett területektől, illetve fontos objektumoktól. [8] [10]

A szabályozás terén tett erőfeszítések ellenére a későbbiekben ismét több súlyos ipari baleset következett be, rámutatva annak hiányosságaira. 2000-ben az Aurul részvénytársaság romániai üzemi derítőjéből nagy koncentrációjú cianidszennyezés került a Láposba, majd onnan a Szamos és a Tisza vizébe, aminek következtében a Tisza élővilága csaknem kipusztult. Szintén 2000-ben a hollandiai Enschede közelében következett be robbanás egy petárdagyárban, ami 21 halálos áldozatot és több mint 1000 sérültet követelt. 2001-ben pedig a franciaországi Toulouse-ban történt robbanás egy műtrágyagyárban, melynek során 21 ember vesztette életét, 700 pedig megsérült. [5]

A fenti események és a belőlük levont tapasztalatok indokot szolgáltattak a Seveso II. Irányelv módosítására, mely a 2003-ban elfogadott 2003/105/EK Irányelv hatályba lépésével történt meg. [5] A módosítás főbb eredményei közé sorolható egyebek mellett, az irányelv tárgyi hatályának kiterjesztése, egyes fogalom-meghatározások pontosítása, a nevesített anyagok listájának és némely anyagosztályoknak felülvizsgálata, valamint egyes küszöbmennyiségek változása. [10] [11] A nevesített anyagok, illetve az anyagosztályok, valamint a hozzájuk tartozó küszöbmennyiségek módosulásait az 1. táblázat mutatja. Az Egyesült Nemzetek Szervezetének keretében napjainkra kidolgozásra kerültek az osztályozás és címkézés harmonizált kritériumai, amelynek eredményeként létrejött a „Vegyi anyagok osztályozásának és címkézésének globálisan harmonizált rendszere” (GHS). Ehhez kapcsolódóan az Európai Parlament és a Tanács 2008. 12. 16-án elfogadta az anyagok és keverékek osztályozásáról, címkézéséről és csomagolásáról szóló 1272/2008/EK rendeletet (CLP), mely 2009. 01. 20-án lépett hatályba. [12] Így a Seveso II. Irányelvben, illetve annak 1. számú mellékletében foglaltakat, összhangba kell hozni az említett CLP rendelet előírásaival. Fentiekre való tekintettel, illetve a rendelkezések eredményesebbé, hatékonyabbá és ésszerűbbé válásának biztosítása, s ezzel a védelem szintjének megtartása és további javítása érdekében az Európai Parlament és Tanács 2012-ben elfogadta a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezeléséről, valamint a 96/82/EK Irányelv módosításáról és későbbi hatályon kívül helyezéséről rendelkező 2012/18/EU Irányelvet, azaz a Seveso III-at. Az irányelv 2012. 08. 13-án lépett hatályba, az egyes tagállamoknak az új szabályozást 2015. 05. 31-ig kell bevezetni. [13] Az új irányelv egyik fontos változását a nyilvánosság tájékoztatására vonatkozó rendelkezések az Aarhusi egyezményben foglaltaknak való megfeleltetése jelenti, mindemellett a legfőbb eleme az 1. számú melléklet összehangolása a CLP előírásaival. [14] Kiszélesedik a nevesített anyagok listája, a korábbi 11 veszélyes anyag kategória pedig 21 kategóriára bővül, melyeken belül – összhangban a CLP előírásaival - megkülönböztetésre kerülnek az egészségi, a fizikai a

környezeti és az egyéb veszélyek külön betűjellel. [13] Az új veszélyes anyag kategóriákat, illetve az újonnan bekerülő nevesített anyagokat a 2. és 3. táblázat tartalmazza.

Fentiekből látható, hogy a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezés, illetve az ehhez kapcsolódó jogszabályok megalkotása egy folyamatos, a tapasztalatok alapján újabb és újabb védelmi igények kielégítését szolgáló tevékenység.

A Seveso II. Irányelv eredeti változatának 1. mellékletében szereplő táblázatok		
Veszélyes anyagok	Küszöbmennyiség (tonna)	
	Alsó	Felső
Ammónium-nitrát	350	2 500
Ammónium-nitrát	1 250	5 000
A következő KARCINOGÉN ANYAGOK: 4-aminobifenil és/vagy sói, benzidin és/vagy sói, bis (klór-metil) éter, klór-metil metil-éter, dimetilkarbomil-klorid, dimetil-nitrozamin, hexametil-foszfor-triamid, 2-naftalamin és/vagy sói, 1,3-propánszulton és 4-nitrodifenil	0,001	0,001
Motorbenzin és egyéb kőolajtermékek	5 000	50 000
Veszélyes anyag veszélyességi osztályok	Küszöbmennyiség (tonna)	
	Alsó	Felső
9. KÖRNYEZETRE VESZÉLYES R-mondatokkal kombinálva: (i) R50: „Nagyon mérgező a vízi szervezetekre” (ii) R51: „Mérgező a vízi szervezetekre”; és R53: „A vízi környezetben hosszan tartó károsodást okozhat”	 200 500	 500 2 000

A Seveso II. Irányelv módosított változatának 1. mellékletében szereplő táblázatok		
Veszélyes anyagok	Küszöbmennyiség (tonna)	
	Alsó	Felső
Ammónium-nitrát	5 000	10 000
Ammónium-nitrát	1 250	5 000
Ammónium-nitrát	350	2 500
Ammónium-nitrát	10	50
Kálium-nitrát	5 000	10 000
Kálium-nitrát	1 250	5 000
A következő KARCINOGÉN ANYAGOK 5 tömegszázalék feletti koncentrációban: 4-aminobifenil és/vagy sói, benzo-triklorid, benzidin és/vagy sói, bis (klór-metil) éter, klór-metil metil-éter, 1,2-dibróm-etán, dietil-szulfát, dimetil-szulfát, dimetilkarbomil-klorid, 1,2-dibróm-3-klórpropán, 1,2-dimetil-hidrazin, dimetil-nitrozamin, hexametil-foszfor-triamid, hidrazin, 2-naftalamin és/vagy sói, 4-nitrodifenil és 1,3-propánszulton	0,5	2
Kőolajtermékek: a) Motorbenzin és nafta b) Kerozinok (sugárhajtómű-üzemanyagot is beleértve) c) Gázolajok (a diesel üzemanyagot, a háztartási fűtőolajokat és a gázolajkeverékeket is beleértve)	2 500	25 000
Veszélyes anyag veszélyességi osztályok	Küszöbmennyiség (tonna)	
	Alsó	Felső
9. KÖRNYEZETRE VESZÉLYES R-mondatokkal kombinálva: (i) R50: „Nagyon mérgező a vízi szervezetekre” (beleértve az R50/53-at is) (ii)R51/53: „Mérgező a vízi szervezetekre; A vízi környezetben hosszan tartó károsodást okozhat”	 100 200	 200 500

1. táblázat. a SEVESO II. Irányelv eredeti és módosított változatának 1. mellékletében szereplő nevesített anyagok és nem nevesített veszélyes anyagosztályok táblázatai közötti különbségek ([10], [11] alapján)

Veszélyességi kategóriák az 1272/2008/EK rendeletnek megfelelően	A veszélyes anyagra vonatkozó küszöbmennyiségek (tonna)	
	Alsó küszöbérték	Felső küszöbérték
„H" szakasz - Egészségi veszélyek		
H1. Akut toxikus 1. kategória	5	20
H2. Akut toxikus 2. és 3. kategória	50	200
H3. Célszervi toxicitás (STOT) – egyszeri expozíció	50	200
„P szakasz – Fizikai veszélyek		
P1.a Robbanóanyagok	10	50
P1.b Robbanóanyagok	50	200
P2. Tűzveszélyes gázok	10	50
P3.a Tűzveszélyes aeroszolok	(nettó) 150	(nettó) 500
P3.b Tűzveszélyes aeroszolok	(nettó) 5 000	(nettó) 50 000
P4. Oxidáló gázok	50	200
P5.a Tűzveszélyes folyadékok	10	50
P5.b Tűzveszélyes folyadékok	50	200
P5.c Tűzveszélyes folyadékok	5 000	50 000
P6.a Önreaktív anyagok és keverékek és szerves peroxidok	10	50
P6.b Önreaktív anyagok és keverékek és szerves peroxidok	50	200
P7. Öngyulladó folyadékok és szilárd anyagok	50	200
P8. Oxidáló folyadékok és szilárd anyagok	50	200
„E" szakasz – Környezeti veszélyek		
E1. A vízi környezetre veszélyes az akut 1 vagy a krónikus 1 kategóriában	100	200
E2. A vízi környezetre veszélyes a krónikus 2 kategóriában	200	500
„O" szakasz – Egyéb veszélyek		
O1. Anyagok vagy keverékek az EUH014 figyelmeztető mondattal	100	500
O2. Az 1. kategóriába tartozó, vízzel érintkezve tűzveszélyes gázokat kibocsátó anyagok és keverékek	100	500
O3. Anyagok vagy keverékek az EU029 figyelmeztető mondattal	50	200

2. táblázat. a Seveso III. Irányelv által bevezetett veszélyességi kategóriák ([13] alapján)

Veszélyes anyagok	Küszöbértékek (tonna)	
	Alsó küszöbérték	Felső küszöbérték
Vízmentes ammónia	50	200
Bór-trifluorid	5	20
Hidrogén-szulfid	5	20
Piperidin	50	200
Bisz(2-dimetil-amino-etil) (metil)amin	50	200
3-(2-etilhexiloxi)propil-amin	50	200
Nátrium-hipoklorit vízi akut 1. kategóriába [H400] sorolt keverékei, melyek 5%-nál kevesebb aktív klórt tartalmaznak és amelyeket az I. melléklet 1. részében egyik veszélykategóriába sem sorolták be	200	500
Propil-amin	500	2 000
Terciel-butil-akrilát	200	500
2-metil-3-butén-nitril	500	2 000
Tetrahidro-3,5-dimetil-1,3,5, -tiadiazin-2-tion (Dazomet)	100	200
Metil-akrilát	500	2 000
3-metil-piridin	500	2 000
1-bróm-3-klór-propán	500	2 000

3. táblázat: a Seveso III. Irányelvbe újonnan bekerülő nevesített anyagok és küszöbértékeik ([13] alapján)

3. HAZAI SZABÁLYOZÁS

Magyarország vállalta, hogy a jogharmonizáció keretében 2003. 01. 01-ig integrálja jogrendjébe a Seveso II. Irányelvet és végrehajtja az abban foglaltakat. Ennek keretében megalkotásra került a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 1999. évi LXXIV törvény (katasztrófavédelmi törvény) és annak IV. fejezete végrehajtását szolgáló, a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 2/2001. (I. 17.) Korm. rendelet. [2] Később, a Seveso II. Irányelv 2003. évi módosításának megfelelően módosításra került a katasztrófavédelmi törvény, a 2/2001. (I. 17.) Korm. rendeletet pedig felváltotta a 18/2006. (I. 26.) Korm. rendelet. [15] A szabályozás egyértelműen meghatározza mind az érintett tevékenységek körét, mind pedig a kormányzatra, az önkormányzatokra és az üzemeltetőkre háruló megelőzéssel, felkészüléssel és elhárítással kapcsolatos kötelezettségeket, továbbá meghatározza a veszélyes üzemek engedélyezésével és felügyeletével összefüggő hatósági feladatokat. [14] A lakosság biztonságának növelése, a katasztrófák elleni hatékonyabb védekezés, a katasztrófavédelmi szervezetrendszer erősítése, valamint az új Alaptörvényben foglaltak végrehajtása érdekében 2011-ben új törvény és hozzá kapcsolódó kormányrendelet készült, a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény (Kat.) és a 219/2011 (X. 20.) Korm. rendelet (Rendelet), melyek 2012. 01. 01-én léptek hatályba, majd 2012. április 15-ével mind a Kat., mind a Rendelet módosításra került.

A korábbiakhoz képest az új szabályozás amellett, hogy kibővíti és részletesebben meghatározza a hatóság hatáskörét és feladatait – a módosítást követően - már nem a katasztrófavédelem központi szervét nevezi meg hatóságként, hanem magát a hivatásos katasztrófavédelmi szervet, ezzel a hatósági jogkörök az országos szintről lekerültek területi szintre, azaz a veszélyes üzemekkel összefüggő hatósági tevékenység Fővárosi, illetve megyei Katasztrófavédelmi Igazgatóságokon folyik, melyhez kapcsolódóan egyes eljárási cselekményeket (pl.: helyszíni szemlék, üzemek azonosítása) a helyi szintű szervezeti egységek (Katasztrófavédelmi Kirendeltségek) végeznek (együtt: hatóság). A feladatok ily módon történő ledelegálása lehetővé teszi azok hatékonyabb elosztását, illetve azt, hogy a saját illetékességi területükön nagyobb helyismerettel rendelkező helyi szervek is hatósági jogkörrel működjenek közre a veszélyes üzemekkel kapcsolatos azonosítási és ellenőrzési tevékenységekben. Ez pozitívan befolyásolta az ipari balesetek megelőzésével és kivédésével kapcsolatos feladatok elosztását, valamint a veszélyes anyagokat használó üzemek nyilvántartásának, felügyeletének lehetőségét. [4], [16]

Továbbá, míg az előző szabályozás csak az alsó, illetve felső küszöbértéket elérő veszélyes üzemekre fordított figyelmet, addig a Kat. bevezeti az ún. „küszöbérték alatti üzem” fogalmát, melyek azok az üzemek, amelyeknél a jelen lévő veszélyes anyagok mennyisége eléri vagy meghaladja a rendelet 1. melléklete 1. illetve 2. táblázatában meghatározott alsó küszöbérték egynegyedét, valamint ebbe a kategóriába tartoznak az ún. „kiemelten kezelendő létesítmények” is. [3] Ezen üzemcsoport bevezetése az Európai Unióban érvényben lévőnél szigorúbb szabályozást jelent. Ezzel bővül azon üzemek köre, melyek a jogszabályok hatálya alá esnek és melyekre így a katasztrófavédelem szerveinek figyelmet kell fordítaniuk.[16]

4. A VESZÉLYES ÜZEMEKKEL KAPCSOLATOS HATÓSÁGI TEVÉKENYSÉG

A veszélyes üzemekhez kapcsolódó hatósági feladatok két csoportba sorolhatóak. Ezek az engedélyezési, illetve a felügyeleti tevékenységek.

4.1. Engedélyezés

A Kat. alapján veszélyes anyagokkal foglalkozó üzemre, létesítményre építési engedély csak a hatóság katasztrófavédelmi engedélye alapján adható, illetve veszélyes tevékenység kizárólag a hatóság katasztrófavédelmi engedélyével végezhető. [3]

Az engedélyezési folyamat megindulhat kérelemre, vagy a hatóság által hivatalból is megindítható.

A kérelemre indult eljárásban a veszélyes üzem üzemeltetője, amennyiben az általa elvégzett üzemazonosítás indokolja a hatóság részére benyújtja a - veszélyes tevékenység végzéséhez, folytatásához szükséges katasztrófavédelmi engedély iránti kérelem mellékleteként – a Rendelet 2. melléklete szerinti adatlapokat, melyek valóságtartalmát a hatóság helyszíni vizsgálat keretében ellenőrzi. Emellett az alsó küszöbértéket elérő üzem üzemeltetője biztonsági elemzést (BE), míg felső küszöbértékű üzem üzemeltetője biztonsági jelentést (BJ) nyújt be a hatósághoz, melynek elfogadása az engedély kiadásának egyik feltétele. A BJ-ben, illetve BE-ben az üzemeltető bemutatja az üzem veszélyeinek azonosítását, a lehetséges balesetek kockázatát és a megelőzés- elhárítás lehetőségeit, a dokumentum mellékletét képező Belső Védelmi Tervben (BVT) pedig kidolgozza a veszélyek elhárításához szükséges intézkedéseket és eszközöket.[4]

A hatóság a beérkezett dokumentumok valóságtartalmát helyszíni ellenőrzéssel vizsgálja, melynek során az üzemeltetőtől további információkat szerez be.

A továbbiakban a benyújtott dokumentum elbírálása történik, melynek során a hatóság értékeli, hogy a benne szereplő kockázatelemzést, a lehetséges eseménysorok feltárását, bemutatását megfelelően végezték-e el, valamint, hogy a veszélyhelyzeti irányítás, a védekezésben résztvevő szervezetek, illetve a kapcsolódó infrastruktúra alkalmasak-e a tervben feltárt, súlyos balesetekből adódó feladatok ellátására, továbbá, hogy felszerelésük, felkészítésük megfelel-e a követelményeknek. Ennek érdekében sor kerülhet újabb helyszíni szemlére, vagy további információk bekérésére. Amennyiben a hatóság úgy ítéli meg, hogy az üzemben folytatott tevékenység általi kockázat szintje meghaladja a meghatározott elfogadható értéket és a bemutatott intézkedések nem elégségesek, akkor az üzemeltetőt kiegészítő intézkedések megtételére kötelezi a veszélyeztető hatás elfogadható mértékűre csökkentése érdekében. Amennyiben ez nem megoldható, a hatóság korlátozhatja, vagy megszüntetheti a veszélyes tevékenységet, illetve elutasíthatja a katasztrófavédelmi engedély iránti kérelmet. Ha a dokumentumban foglaltak a kockázatokat és a veszély elhárítása érdekében elvégzendő intézkedéseket, feladatokat, továbbá a szükséges feltételeket megfelelően tartalmazzák a terv elfogadásával egyidejűleg a hatóság dönt a katasztrófavédelmi engedély megadásáról. A dokumentumok elbírálása során biztosítani kell a nyilvánosságot, vagyis azt, hogy a lakosság megismerhesse az őt érintő veszélyeket és ezzel kapcsolatban észrevételeket tegyen. A lakossági észrevételeket a hatóságnak döntése során figyelembe kell vennie. [4]

Küszöbérték alatti üzemek esetében a benyújtott adatlapok valóságtartalmát a hatóság helyszíni szemle keretében vizsgálja, és ezek alapján megállapítja, hogy az adott üzem a Kat. IV. fejezetének hatálya alá tartozik-e, avagy sem. Az eredmény függvényében a küszöbérték alatti üzem részére katasztrófavédelmi engedély kerül kiadásra, vagy a hatóság az üzemeltetőt Súlyos Káresemény Elhárítási Terv (SKET) készítésére és benyújtására kötelezi. A SKET – a belső védelmi tervhez hasonlóan – a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének azonosítását, részletes elemzését tartalmazza, továbbá bemutatja a megelőzéshez,

illetve a védekezéshez rendelkezésre álló szervezeti és eszközrendszert. [17] A továbbiakban a benyújtott SKET elbírálása az előzőekben foglaltakhoz hasonlóan történik, ám ebben az esetben nem szükséges a nyilvánosság bevonása. A hatóság döntése jelen esetben szintén a veszélyes tevékenység korlátozása, megszüntetése, vagy a katasztrófavédelmi engedély megadása lehet. [4]

Hivatalból indított eljárásra akkor kerül sor, ha a be nem jelentkezett üzem esetében megállapítást nyer, hogy az a jelenlévő veszélyes anyagok mennyisége miatt a Kat. IV. fejezete hatálya alá esik. Ebben az esetben a hatóság megindítja az üzemazonosítási eljárást; kötelezi az üzemeltetőt az üzemazonosítás elvégzésére és a szükséges dokumentumok benyújtására, melyek elbírálása a fentiekben leírtaknak megfelelően történik. [3]

Az új szabályozás életbe lépése után a veszélyes anyagok gyártását, felhasználását, tárolását végző üzemeknek 2012. május 15-ig kellett elvégezniük a telephelyeikhez kapcsolódó üzemazonosítást és az eredmény függvényében a szükséges dokumentumokat megküldeni a hatóság részére. Számos adatlap érkezett, melyek alapján - a rendeletben foglaltaknak megfelelően - a hatóság helyi szerve minden esetben helyszíni szemlét tartott, melynek eredményéről tájékoztatta az illetékes területi szervet. A hatóság területi szerve a helyi szerv javaslatai alapján megtette a szükséges intézkedéseket – döntött a katasztrófavédelmi engedély megadásáról, vagy súlyos káresemény elhárítási terv készítésére kötelezte az üzemeltetőt. A veszélyes üzemek azonosítása jelenleg is folyik azon üzemek helyszíni szemle keretében történő vizsgálatával, melyek nem jelentkeztek be a megadott határidőig és amennyiben a telephelyen található anyagmennyiség szükségessé teszi, a hatóság az üzemeltetőt kötelezi az üzemazonosítás elvégzésére és a Rendelet szerinti adatlapok benyújtására. [16] Ez idáig több mint 1400 üzemazonosítási eljárás megindítására került sor. [18]

4.2. Felügyeleti tevékenység [4]

Az engedéllyel rendelkező, már működő veszélyes üzemek felett a hatóság felügyeletet gyakorol. Ebbe tevékenységi körbe tartozik az üzemek területén lefolytatott hatósági ellenőrzés, az üzemeltetők által készített dokumentációk és tervek felülvizsgálata, a gyakorlatok ellenőrzése és a veszélyes üzemekben bekövetkezett balesetekkel kapcsolatos jelentési és adatszolgáltatási feladatok.

A hatóság a felső küszöbértékű üzemekben legalább évente, míg az alsó küszöbértékű üzemekben legalább kétévente időszakos hatósági ellenőrzést tart. Emellett a hatóság a veszélyes üzemek vonatkozásában a társhatóságokkal összehangolt, komplex iparbiztonsági ellenőrzéseket szervez. Ez utóbbi hozzájárul a társhatóságokkal való eredményes együttműködés kialakításához, az egymás közti adatmegosztás, információcsere hatékonyabbá válásához.

Az üzemeltető által elkészített és benyújtott dokumentumokat, illetve terveket a jogszabályban meghatározott időközönként, illetve – a veszély kockázatának növekedésével járó változás esetén – a hatóság, vagy az üzemeltető kezdeményezésére felül kell vizsgálni és amennyiben a változtatások szükségessé teszik egységes szerkezetben ismételten benyújtani a hatóság felé elbírálásra.

A veszélyes üzemek üzemeltetőinek évente részleges három évente pedig teljes BVT, illetve SKET gyakorlatot kell tartaniuk, melyen a hatóság területi szerve részt vesz és a helyszínen értékel. A helyi szerv az üzemeltető által készített BVT jegyzőkönyvvel és értékeléssel együtt megküldi saját értékelését a hatóság részére. Ezek alapján a hatóság a gyakorlatot elfogadja, vagy ismételt lefolytatására kötelezi az üzemeltetőt.

A veszélyes üzemekben bekövetkezett baleset esetén az üzemeltető bejelentését követően tájékoztatja a polgármestert, a hatóság helyi szerve pedig kivizsgálja az esemény körülményeit. Az üzemeltető is vizsgálatot folytat le, amennyiben a baleset a Rendelet 11.

mellékletében szereplő feltételek közül legalább egyet teljesít, úgy a vizsgálat eredményéről részletes jelentést küld a hatóság felé. A hatóság pedig tájékoztatja a polgármestert az eseményről. [4]

A 2012. évi jogszabályi változások következtében jelentősen megnőtt az egyes katasztrófavédelmi igazgatóságok illetékességi területéhez tartozó veszélyes üzemek száma. Ez a kapcsolódó feladatok számának és így a hatóság leterheltségének növekedését is eredményezte. A feladatok területi, illetve helyi szintre való delegálásával elérhető, hogy azokat a központi szerv helyett, az illetékességi területüket jobban ismerő területi, illetve helyi szervezeti egységek hajtsák végre. Emellett a feladatok megosztásával az egyes szervezetek leterheltsége csökkenthető. Ennek eredményeképp hatékonyabbá válhat a feladatok végrehajtása.

A Kat. és a Rendelet egyes eljárásaiban – így az üzemazonosításnál, az engedélyezésnél és a különböző dokumentációk felülvizsgálatánál - az üzemeltetőnek a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezés hatósági eljárásaiban az igazgatási szolgáltatási díj fizetési körébe tartozó hatósági eljárásokról, igazgatási jellegű szolgáltatásokról és bejelentésekről, továbbá a fizetendő díj mértékéről, valamint a fizetésre vonatkozó egyéb szabályokról szóló 51/2011. (XII. 21.) BM rendelet (BM Rend.) előírásainak megfelelően igazgatási szolgáltatási díjat kell fizetniük. [3], [19] Ez jelentős költségterheket ró az üzemeltetőkre, melyet a kockázatelemzések és a különböző dokumentumok elkészíttetésének költségei tovább növelnek. Ám ez a megelőzésre fordított összeg jóval kevesebb, mint amekkora anyagi kárt egy esetlegesen bekövetkező súlyos baleset okozna, illetve mint amennyi erőforrás szükséges lenne annak felszámolásához.

Emellett az igazgatási szolgáltatási díjak az eljáró hatóság bevételét képezik [19], így ezt a bevételt a katasztrófavédelmi szervezetek technikájuk korszerűsítésére, illetve a bekövetkező katasztrófák elhárítására fordíthatják ezzel növelve a védekezés hatékonyságát. Továbbá a környezetvédelemben már régóta érvényben lévő „szennyező fizet elvhez” hasonlóan az embereket, illetve a környezetet veszélyeztető tevékenységet végző üzemektől elvárható, hogy a kockázat csökkentése és a megelőzés eredményességének növelése érdekében elkészíttessék a szükséges dokumentációkat, illetve az eljárási díjakkal hozzájáruljanak egy esetleges katasztrófa elhárításainak költségeihez.

4.3 Hatósági feladatokat ellátók felkészítése

Az iparbiztonsági jogi szabályozás alkalmazási gyakorlata megmutatta, hogy jelentős számban szükséges speciális felkészültséggel rendelkező szakértők képzése, amely képzést a hatósági feladat- és hatáskörökkel rendelkező hivatásos katasztrófavédelmi szervezet iparbiztonsági szakterületének bevonásával és egyetértésével szükséges megalapozni és az oktatásban alkalmazni. A Nemzeti Közszolgálati Egyetemen 2013/14. évben indul a katasztrófavédelem szak keretében iparbiztonsági szakirányú képzés.

A katasztrófavédelmi szakon folyó képzés célja, hogy a végzett hallgatók alkalmasak legyenek az általános katasztrófavédelmi igazgatás részterületein (katasztrófa-megelőzés, katasztrófa-elhárítás szervezése, helyreállítás, polgári védelmi felkészítése feladatok ellátása), illetőleg a tűzmegelőzési, tűzoltási-műszaki mentési, tűzvizsgálati, az ezzel kapcsolatos felkészítés és az elsődleges katasztrófa-elhárítási tevékenységek keretében jelentkező, továbbá az iparbiztonsággal kapcsolatos általános megelőzési és hatósági feladatok elvégzésére.

Az új szabályozás alkalmazása nemcsak a katasztrófavédelem, a közreműködő rendvédelmi szervek és az együttműködő társhatóság számára ad feladatokat, hanem a felügyelt, veszélyes anyaggal foglalkozó vagy kritikus infrastruktúraként azonosított gazdálkodó szervezetek részére is.

Az iparbiztonsági szakirányon tanulmányokat folytató hallgatók mind nappali, mind levelező tagozaton, tervezetten elsajátíthatják a veszélyes üzemek létesítésére és működésére

vonatkozó jogszabályokban és hatósági előírásokban foglaltakat, azok gyakorlati alkalmazásának rendszerét; valamint a veszélyes anyagok különféle szállítási módozataival kapcsolatos jogszabályi és hatósági előírásokat, és az ezekre vonatkozó hatósági eljárás rendjét; továbbá a kritikus infrastruktúrákkal összefüggő hazai és nemzetközi szabályozásokat, és a működési rendjüket meghatározó biztonsági követelményrendszereket. [20]

5. ÖSSZEFOGLALÁS

Az elmúlt időszak sokszor több országot is érintő, súlyos ipari szerencsétlenségei rámutattak a megelőzés fontosságára. Ez a tevékenység viszont csak egységes szabályozással, átgondolt és összehangolt módszerek alkalmazásával lehet eredményes. Ennek kialakítása céljából az Európai Unióban több egyezmény és irányelv került megalkotásra, melyeket a tagállamok integráltak saját jogrendjükbe. Magyarország a jogharmonizáció keretében megalkotta saját, katasztrófavédelemi jogszabályait, melyek többször módosításra kerültek. A hatályban lévő szabályozás megköveteli az alsó és felső küszöbértékű üzemek mellett az ún. küszöbérték alatti üzemek azonosítását, melyet a hatóság a Rendeletben foglaltaknak megfelelően, az 1. mellékletben megadott szabályok szerint végez. A jogszabályi változások hatására megnövekedett a Kat. IV. fejezetének hatálya alá eső üzemek száma, amelyeknek az üzemazonosításhoz és más eljárásokhoz kapcsolódóan igazgatási szolgáltatási díjat kell fizetniük. Minthogy ezen díj az eljáró hatóság bevételét képezi, hozzájárulhat fejlesztések véghezviteléhez és ezáltal a katasztrófavédelmi szervezetek munkájának hatékonyabbá válásához. A hatósági jogkörök és feladatok kiszélesítése, valamint területi, illetve helyi szintre történő delegálása emellett lehetővé teszi a katasztrófavédelmi szervezetek feladatainak megosztását, ezáltal a veszélyes üzemekhez kapcsolódó engedélyezési és felügyeleti tevékenységek eredményesebb végrehajtását, amint arra szerzőtársammal már korábban is rámutattunk. [16]

A veszélyes üzemekkel kapcsolatos hatósági tevékenység magas szintű végrehajtását segítheti középtávon a Nemzeti Közszolgálati Egyetemen induló iparbiztonsági szakember-képzés is.

Szükséges a továbbiakban a speciális üzemtípusoknál alkalmazandó üzemazonosítási módszerek és eljárások kidolgozása, melyekkel lehetővé válik, hogy az egyes üzemtípusoknál a különböző anyagok besorolása, tulajdonságaiknak és mennyiségüknek a számítás során történő figyelembe vétele a lehető legpontosabban tükrözze az üzem által jelentett kockázatokat.

Emellett fontos annak vizsgálata is, hogy a már nemzetközileg elfogadott Seveso III. Irányelv hazai bevezetése miként hatna a szabályozás hatálya alá eső üzemek számára és összetételére, valamint, hogy milyen változtatásokra lenne szükség a minél hatékonyabban alkalmazható új jogszabályok kialakítása érdekében.

Felhasznált irodalom

[1] Kátai-Urbán Lajos, Vass Gyula: 7. Katasztrófavédelem (SEVESO); 7.3. Útmutató a biztonsági dokumentáció elkészítéséhez, In: Sárosi György (szerk.) Veszélyes áruk szállítása és tárolása. 2009. október, Budapest: Verlag Dashöfer Szakkiadó, 2010. pp. 1-54.

[2] Lauer János, Dr. Solymosi József, Dr. Vincze Árpád: Veszélyes Üzemek Biztonsági Értékelése. p. 11. www.zmne.hu/tanszekek/vegyi/docs/fiatkut/pdf/lauer_03_01.pdf 2013. 03. 26.

[3] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

[4] 219/2011. (X. 20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről

[5] Bíróné Ősz Julianna, Bojti Imre, Cimer Zsolt, Dr. Damjanovich Imre, Hoffmann Imre, Dr. Kátai-Urbán Lajos (szerk.), Dr. Mógor Judit, Dr. Szakál Béla, Vass Gyula: Módszertani segédlet a veszélyes anyagokkal kapcsolatos súlyos ipari balesetek elleni védekezés területi és helyi feladatainak ellátásához. 2005. p. 104. http://www.vedelem.hu/letoltes/jegyzet/jegy18.pdf 2013. 03. 26.

[6] Dr. Halász László, Dr. Pellérdi Rezső, Dr. Földi László: Katasztrófavédelem I. Egyetemi jegyzet. ZMNE, Budapest, 2009. p. 517.

[7] Az ipari balesetek elleni védekezés nemzetközi szabályozása. BM OKF, 2004. http://www.katasztrofavedelem.hu/index2.php?pageid=seveso_tajekoztato_rendszer1 2013. 01. 04.

[8] Bognár Botond, Dr. Damjanovich Imre: A súlyos ipari balesetek megelőzésével és elhárításával kapcsolatos nemzetközi és európai uniós szabályozások összefoglalása. p. 10. www.inventor.hu/ceco/kock/konyv/ofoglalo.pdf 2013. 03. 26.

[9] Mi a teendő vegyi baleset esetén? Segédlet a súlyos balesetek elleni védekezés lakossági tájékoztató kiadvány elkészítéséhez. BM OKF, 2003. p. 45. www.katasztrofavedelem.hu/letoltes/lakossag/lakossagi.pdf 2013. 03. 26.

[10] A Tanács 96/82/EK Irányelve a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyeinek ellenőrzéséről. Brüsszel, 1996. eur-lex.europa.eu 2013. 03. 26.

[11] A Tanács 96/82/EK Irányelve a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyeinek ellenőrzéséről. Brüsszel, 1996. – a módosításokkal egységes szerkezetbe foglalt változat http://europa.eu/legislation_summaries/environment/civil_protection/l21215_hu.htm 2013. 04. 02.

[12] Az Európai Parlament és a Tanács 1272/2008/ek rendelete az anyagok és keverékek osztályozásáról, címkézéséről és csomagolásáról, a 67/548/egk és az 1999/45/ek irányelv módosításáról és hatályon kívül helyezéséről, valamint az 1907/2006/ek rendelet módosításáról. Strasbourg, 2008. http://www.okbi.hu/index.php/hu/ghs-jogszabalyok 2013. 04. 01.

[13] Az Európai Parlament és a Tanács 2012/18/EU Irányelve a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezeléséről, valamint a 96/82/EK tanácsi irányelv módosításáról és későbbi hatályon kívül helyezéséről. Strasbourg, 2012. http://ipsc.jrc.ec.europa.eu/?id=503 2013. 04. 02.

[14] Kátai-Urbán Lajos, Vass Gyula: Development of Hungarian System for Protection against Industrial Accidents. In: Jozef Ristvej (szerk.)18. medzinárodná vedecká konferencia Riešenie krízových situácií v špecifickom prostredí. Zilina, University of Zilina, pp. 229-239.(ISBN:978-80-554-0699-2).

[15] A veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezés szabályai - Felkészítés a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésre. http://www.katasztrofavedelem.hu/index2.php?pageid=kozigazgatas_veszelyes_anyagok 2013. 04. 06.

[16] Szendi Rebeka, Dr. Dobor József: Identification of dangerous establishment in practice, in: Proceedings „Safety of Industrial Establishments 2013.” International Scientific Conference on Industrial Safety Budapest, 10 April 2013, Budapest, NKE, 2013. pp. 136-143. ISBN: 978-615-5305-08-5

[17] Szendi Rebeka: A fővárost fenyegető ipari katasztrófák és az ellenük való védekezés lehetőségei a 2012. évi jogszabályváltozások tükrében, Védelem Online, Budapest, 2012. p. 8.

[18] Dr. Vass Gyula: Veszélyes üzemek ellenőrzése Magyarországon in: Előadásgyűjtemény „Veszélyes Üzemek Biztonsága 2013.” Nemzetközi Iparbiztonsági Tudományos Konferencia Budapest, 2013. április 10., Budapest, NKE, 2013. pp. 29-34. ISBN: 978-615-5305-08-5

[19] 51/2011. (XII. 21.) BM rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezés hatósági eljárásaiban az igazgatási szolgáltatási díj fizetési körébe tartozó hatósági eljárásokról, igazgatási jellegű szolgáltatásokról és bejelentésekről, továbbá a fizetendő díj mértékéről, valamint a fizetésre vonatkozó egyéb szabályokról

[20] Kátai-Urbán Lajos: Industrial Safety Preparation in the Higher Education System of Disaster Management in Europa and in Hungary: Iparbiztonsági felkészítés az európai és magyar katasztrófavédelmi felsőfokú képzés rendszerében. In: Dobor József (szerk.) Proceedings "Safety of Industrial Establishments 2013. International Scientific Conference on Industrial Safety: Előadásgyűjtemény "Veszélyes üzemek biztonsága" Nemzetközi Iparbiztonsági Tudományos Konferencia. Budapest: Nemzeti Közszolgálati Egyetem, 2013. pp. 79-100. (ISBN:978-615-5305-08-5).

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Nikodém Edit
nikodem@t-email.hu

AZ ANYAGI JAVAK MEGÓVÁSÁNAK SZEREPE ÉS HANGSÚLYOSSÁGA A LAKOSSÁGVÉDELEMBEN

Absztrakt

A XXI. században egyre inkább jelentkező új típusú kihívások és veszélyforrások nagymértékben fenyegetik létbiztonságunkat és ezzel együtt a létfenntartáshoz szükséges anyagi javakat. Minden állam igyekszik lakosságának és a területén élőknek biztonságát szavatolni, amelynek érdekében számos intézkedés, védelmi tervet, módszert és eszközt sorakoztat fel. Mindamellett, hogy a veszélyhelyzet megelőzésére, elhárítására, valamint annak helyreállítási munkálataira irányuló lakosságvédelmi módszerek és eszközök az ember életét, testi épségét és egészségét hivatottak megóvni, egyre nagyobb hangsúlyt szegeződik az anyagi javak megóvására. A szerző rávilágít a lakosságvédelem ezen szegmensének jelenkori fontosságára.

The new type of challenges and threats of the 21st century are greatly menacing our security along with the material goods essential for life. Each nation aims to guarantee the safety of its population and everyone living in the country and to ensure this, several different measures, security strategies, methods and resources are put in place. Apart from the methods and resources aiming the prevention of threats and the reconstruction operations, which intend to protect the life, health and integrity of people, increasing attention is drawn towards the preservation of material goods. The author will present the importance of this section of the public security methods in today's world.

Kulcsszavak: *anyagi javak, szükséglet, védelem, megelőzés ~ material goods, material needs, defence, prevention*

BEVEZETÉS

A lakosságvédelem szó hallatán sokakban az emberi élet megóvása és annak védelme köré épülő fogalomrendszer jut eszébe, amely magától értetődő. Már ősidők óta fontos szempont volt az embernek, hogy veszélyhelyzetben minden eszközzel védje életét, testi épségét, valamint menekítse és óvja azokat a tényezőket, amelyek a túlélést biztosítják számára, vagyis a létfenntartását biztosító anyagi javakat. A XXI. században, egy felgyorsult, energiaközpontú, termelés- és gazdaságorientált világban egyre kevesebb hangsúlyt fektetünk természeti erőforrásaink megóvására és ebből adódóan saját magunk biztonságára. A legtöbb esetben a katasztrófákra és balesetekre nem lehet felkészülni, azonban meg kell valósítani minden olyan lakosságvédelmi intézkedést, előkészületet és tervezést, amellyel bekövetkezés esetén minimálisra csökkenthetők az emberi és anyagi károk. A lakosságvédelem szó hallatán általában az emberi élet megóvása és annak védelme köré épülő fogalomrendszer asszociálunk. Egy esetleges katasztrófát követő időszakban azonban elengedhetetlen fontossággal jelentkezik az olyan anyagi javak védelme, mint például az ivóvíz, vagy az élelmiszerkészletek. Már az őskor óta fontos szempont volt az embernek, hogy vészhelyzetben minden eszközzel védje életét, testi épségét, valamint menekítse és óvja azokat a tényezőket, amelyet a túlélést biztosítják számára, azaz a létfenntartáshoz szükséges anyagi javakat. A lakosságvédelmi feltétel- és feladatrendszer tervezési, szervezési, kiépítési és megvalósítási fázisaiban egységesen kell, hogy megjelenjen az anyagi javak védelme.

ANYAGI JAVAK VÉDELMÉNEK JELENTŐSÉGE

Bármilyen szempontból is vizsgáljuk a biztonság megteremtésének, a megóvás és a védelem megvalósításának, vagy akár a veszélyelhárításnak a kérdését, annak középpontjában legfőképp – mint létünket meghatározó tényező és mint mindezek célkitűzésének iránya – az emberi élet áll. Azonban az emberi élet nem lenne fenntartható az olyan alapvető létszükségletek nélkül, mint az ivóvíz, az élelmiszer, gyógyszerkészletek, állatállomány stb. Éppen ezért az emberi élet és az azt biztosító anyagi javak között, a defenzíva szempontjából nem szabhatunk éles határvonalat. Természetes dolog, hogy maga az élet, mint a létezés az, amelyhez az Alkotmányos jogrend is az alapvető emberi jogokat társítja:

> „Minden embernek joga van az élethez és az emberi méltósághoz, a magzat életét a fogantatástól kezdve védelem illeti meg.”[1]

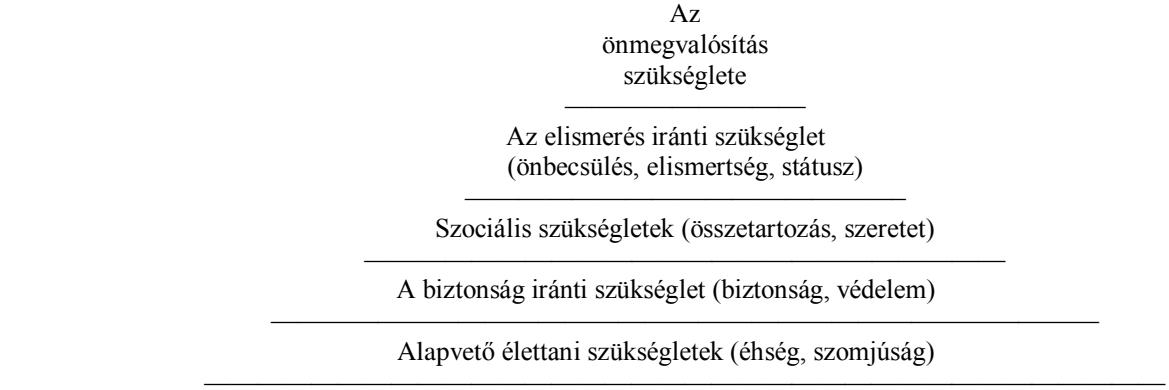
Ugyanakkor az Alkotmány közvetlen ez után arról is rendelkezik:

> „Mindenkinek joga van a szabadsághoz és a személyi biztonsághoz.”[2]

A fentiekben taglalt biztonságról, mint fogalomról kijelenthető, hogy egy komplex és nehezen körülhatárolható meghatározás, mivel számos értelmezésben definiálható és számos körülménytől tehető függővé. Ennek fajtáit a korábbi fejezetben foglaltak miatt itt nem részletezzük, azonban kijelenthető, hogy létezik a biztonságnak és a biztonságérzetnek egy, az emberi létszükségletek kielégítésére vonatkozó értelmezése. Ennek szemléltetésére vegyük alapul Abraham Maslow amerikai pszichológus munkásságát, aki a pszichológia területén elért tudományos eredményeivel és legfőképp az emberi szükségletek hierachiájának modelljével (Maslow-piramis) írta be magát a történelembe. Az 1943. és 1954. között kidolgozott modelljében a már említett – az ember érzetében jelentkező – biztonság fogalmát

[1] *Magyarország Alaptörvénye*. II. cikk (1) Magyar Közlöny, 2011. évi 43. szám.
[2] *Magyarország Alaptörvénye*. IV. cikk (1) Magyar Közlöny, 2011. évi 43. szám.

és a biztonság megteremtésének igényét megelőzi az alapvető élettani szükségletek kielégítése és az arra vonatkoztatott igény, amely e feltevésben minden más előtt, az első helyet érdemelte ki magának.



A fenti modellből is kitűnik, hogy a biztonság elérésének szükséges feltétele az alapvető létszükségletek, jelen esetünkben az anyagi javak megléte, megteremtése és egyben megóvása. Ebből adódóan, ha az életre és a hozzá kapcsolódó anyagi javakra irányuló védelmet és biztonságot vizsgáljuk, egyfajta ekvivalenciához jutunk. Mélyebben belegondolva számos olyan érv sorakoztatható fel az említett tézissel szemben, vagy mellette, amelynek eredményeképp a prioritás mérlegének nyelve a legtöbb esetben egyenlőséget mutat az anyagi javak megóvása és az emberi élet megóvásának fontossága között. Ha tüzetesebben megnézzük a legtöbb jogszabály, törvény és rendelet a szóban forgó kifejezést, minden esetben „az élet és anyagi javak védelme" szókapcsolatként alkalmazza, sőt a polgári védelem meghatározás alatt tágabb értelemben a lakosság és az anyagi javak védelmét kell érteni. Mindezek megerősítik és alátámasztják a két determináns elválaszthatatlanságát.[1]

Ebből adódóan találtam fontosnak megvizsgálni kifejezetten az anyagi javak védelmére vonatkozó lakosságvédelmi módszereket, intézkedéseket és a lehetséges fejlesztési irányokat, amelyek eredményét az alábbiakban részletezem.

ANYAGI JAVAK ÉS AZOK VÉDELMÉNEK MEGHATÁROZÁSA, RENDELTETÉSE

Az anyagi javak definiálására többféle meghatározás lehetséges:

„Létfenntartáshoz szükséges anyagi javak: a lakosság alapvető ellátását és életfeltételeit biztosító anyagok, eszközök, rendszerek és készletek összessége, különösen az ivóvíz-, az élelmiszer-, a takarmány-, a gyógyszerkészletek és a haszonállatok." [2][3] Egy másfajta megközelítésben „a létfenntartáshoz nélkülözhetetlen anyagi javak fogalma alatt az élelmiszer-, ivóvíz-, vetőmag-, takarmány és szaporítóanyag-készleteket, az állatállományt, valamint a gyógy- és kötszereket értjük." [3][4]

Részletesen és tételesen megvizsgálva az anyagi javak védelmének az alábbi alapvető területeit különböztetjük meg:

- a létfenntartáshoz szükséges élelmiszer és ivóvízkészletek védelme
- mezőgazdasági létesítmények, az állatállomány és a növényzet védelme
- takarmány és vetőmagkészletek védelme
- ipari létesítmények, berendezések, gépek védelme
- energiaforrások-, hálózatok, nyersanyagok védelme
- gyógy- és kötszerek védelme
- egészségügyi felszerelések, gépek, eszközök védelme

3 1.§ 27. pontja
4 58.o.

- pótolhatatlan kulturális értékek, műkincsek védelme
- a tűzvédelem feltételeinek megszervezése és megvalósítása
- közművek, út- és vasútvonalak, közlekedési csomópontok védelme
- műtárgyak, műkincsek védelme

Az anyagi javak védelmét deklarálja minden olyan védelmi elv, módszer, tevékenység, amelyet a létfontosságú, valamint az ország számára fontos ipari, mezőgazdasági és kulturális értékek és egyéb anyagi javak védelme érdekében alkalmaznak egy esetleges fegyveres összeütközés, vagy különböző katasztrófák esetén. Az anyagi javak védelmének célja, hogy garantálja a létfenntartáshoz és az állam működőképességének biztosításához szükséges létesítmények, közművek, erőforrások és értékek biztonságát.[4][5] Az anyagi javak védelmének, mint minden más lakosságvédelmi módszernek is az alapja a komplexitásban mutatkozik meg. Más védelmi eljárásokat, feladatokat magában ötvöző védelmi módszer van szó, amelynek összetettségéről a ma is hatályban lévő 2/1998. (I. 12.) számú, a földművelésügyi ágazat polgári védelmi feladatairól szóló FM rendelet az alábbiakban árulkodik:

„Az anyagi javak rbv. védelme kiterjed a mezőgazdaság, az élelmiszeripar, a vadgazdálkodás és halászat, az erdőgazdálkodás az elsődleges faipari termelés, az ezekhez kapcsolódó szolgáltatás, kutatás és fejlesztés, a mezőgazdasági termékforgalom, az agrár-környezetgazdálkodás, a növényegészségügy, az állategészségügy és élelmiszer-ellenőrzés területére és résztvevőire."[5][6]

„A szabályozás célja, hogy az élelmiszer, a mezőgazdasági termények, a takarmánykészletek, az állatállomány, a vadállomány, a faállomány, a szaporítóanyagok, ágazati termelő eszközök (a továbbiakban: ágazati anyagi javak) termelése, előállítása, tartása, tárolása, csomagolása, szállítása, elosztása és mentése, továbbá a termőtalaj védelme megfelelő módon és körülmények között valósuljon meg."[7]

Korábban számos, e témában készült tanulmányban, illetve törvényi jogszabályokban és rendelkezésekben, az anyagi javak védelmét kizárólag RBV (Radioaktív, Biológiai, Vegyi) védelem alatt taglalták, azonban a mára megjelent újfajta kihívások és veszélyforrások, a bekövetkezett ipari és természeti katasztrófák, viszonylag új szemléletmódba helyezték a lakosságvédelem e módszerét, így kissé háttérbe szorítva annak RBV szóhasználatát, amelyet manapság leginkább a terrorizmus és a tömegpusztító fegyverek elleni védelem kifejezése váltott fel. Mindez az anyagi javak védelmének célján és rendeltetésén mit sem változtat. E terület kihívásai, céljai igen szerteágazó feladatot és tevékenységet követelnek meg, amelyet a veszélyeztetettség függvényében térben és időben differenciáltan kell megvalósítani.

Az anyagi javak védelmének célja:

- A létfenntartáshoz és az állam működőképességének biztosításához szükséges létesítmények, közművek, erőforrások és értékek összességének védelme.
- Az élet fenntartásához elengedhetetlenül szükséges anyagi javak (víz, élelmiszer stb.) a lehető legkisebb mértékben sérüljenek.
- Az ország számára fontos, valamint az élet újraindításához elengedhetetlen értékek, anyagi javak védelme a lehető leghatékonyabban valósuljon meg.
- A lehető legkisebb ráfordítással valósuljon meg mind a szükséges, mind az elégséges védelmi szint.
- Ki kell alakítani egy olyan komplex védelmi rendszert, amely minden esetben a veszélyeztetettség függvényében, differenciáltan kivitelezhető.

5 55-73. old.
6 4. § (1)
7 4. § (2)

AZ ANYAGI JAVAK VÉDELMÉNEK FELADATAI

Az anyagi javak védelmének keretén belül jelentkező feladatokat, valamint az elvégzendő feladatok jellegét nagymértékben befolyásolja a veszélyeztetettség formája. Ennek tükrében az alábbi kategóriákat különböztetjük meg:

- Fegyveres összeütközés, vagy konfliktus (rombolás) elleni defenzív intézkedések
- Radiológiai, biológiai és vegyi szennyezés elleni védelem
- Természeti katasztrófák (árvizek, földmozgások, kártevők stb.) elleni védelem
- Tűz elleni védelem

Az anyagi javak védelmét befolyásoló tényezők:

1. Fontos befolyásoló tényezőként említhető a megóvásra szánt anyagi javak *fajtája és típusa*. Ezek vonatkoznak a növényekre, terményekre, háziállatokra, élelmiszerre, ipari üzemekre, raktárakra, közművekre, energia rendszerekre stb.
2. Az anyagi javak optimális *elhelyezési formái, módozatai*. Ez esetben tisztázni kell, hogy nyílt terepen, zárt térben, fényes, vagy fénymentes, fűtött, vagy fűtetlen, esetleg légkondicionált helyen célszerű ennek megvalósítása.
3. Számolni kell a *veszélyforrás jellegével*, továbbá a *várható káros hatások* formájával, típusával, mértékével. Efféle tényezők lehetnek a különböző vegyi, vagy radiológiai szennyeződések, biológiai kártevők, növények és állatok pusztulása, kis-. közepes-, nagy terjedelmű károsodás stb.
4. E felsorolásban meghatározó tényezőként szerepel a védekezéshez *rendelkezésre álló idő*, valamint *feltételrendszer*. Az előbbi esetében a felkészüléshez, továbbá a beavatkozás megkezdéséhez felhasználható időmennyiséget, utóbbi esetében pedig a személyi, anyagi és technikai feltételeket kell érteni.
5. Legvégső tényezőként kell megemlíteni a megvalósítani kívánt védekezési elvet és módszert, valamint annak fajtáját és típusát. Fontos szempont, a védekezés megvalósításának időintervalluma, valamint az, hogy önálló védekezésről, vagy esetlegesen egy folyamat részét képező védekezésről van szó.

A fentiekben leírt lakosságvédelmi módszerek mellett a védelemnek léteznek olyan kiegészítő tényezői, amelyek az alapvető védelmi módozatok alkalmazásának hatékonyságát növelik. Ezen tényezők közé sorolható:

- a létfenntartáshoz szükséges anyagi javak *megelőző védelmének* tervezése, valamint a fontos vagyontárgyak és a kulturális javak védelmére való felkészítés
- anyagi javak ellenőrzése
- anyagi javak mentesítése

ANYAGI JAVAK MEGELŐZŐ VÉDELME

Egy bekövetkezett veszélyhelyzet esetén oly mértékű káros hatású szennyeződés érheti az élelmiszergazdaságok területét (legyen az növénytermesztés, vagy feldolgozóipar), a tárolt, illetve elosztásra váró készleteket, hogy fogyasztható, szennyeződésmentes élelmiszer híján a lakosság létfenntartási válságba kerülhet. Mindezek tükrében a veszély elhárítása, a veszteségek csökkentése és a minőségi károsodások elkerülése érdekében szükségszerű biztosítani az alapvető anyagi javak megelőző védelmét.[6][8]

A védelem eme stádiumában jelentkező feladat, hogy a rendelkezésünkre álló eszközöket és módszereket felhasználva, igyekezzünk távol tartani létfenntartási javainkat (főképp az ivóvizet, élelmiszert, gyógyszereket stb.) a jelentkező káros hatásoktól. Ebben a preventív

8 94.o.

védekezési metódusban az építészeti és technológiai megoldásoknak meg kell felelniük az adott követelményeknek. Ez alatt kell érteni többek között a javak előállítását, tárolását, szállítását. Továbbá az anyagi javak megelőző védelméről beszélünk abban az esetben, amikor összegezzük azokat a követelményeket, előírásokat, rendszabályokat, módszereket, valamint műszaki-technikai feltételeket, amelyek a túlélés feltételeit biztosító anyagi javak megóvásának tervezésére, szervezésére és megvalósítására irányulnak.

A megelőzés legfőbb célját képezi az állami élet fenntartásának, valamint a termelés folyamatosságának biztosítása az ország lakosságának lehető legkisebb veszélyeztetése mellett.

A létfenntartási javak megelőző védelme magába foglalja a termesztéssel, előállítással, feldolgozással, csomagolással, szállítással, illetve tárolással kapcsolatos műszaki-, technikai-, tervezési-, telepítési-, kivitelezési követelményeket, előírásokat, a nyersanyagok, félkész- és késztermékek megelőző védelmi követelményeit, előírásait, végrehajtási módszereit, az ellenőrzés és mentesítés követelményeit, előírásait, normáit és módszereit, amelyek alkalmazásával veszélyhelyzet esetén is megfelelő minőségű, fogyasztható termékeket lehet biztosítani. Ennek keretében kell a létfenntartási javak termesztésére, termelésére, gyártásközi szállításra és elosztásra vonatkozó laboratóriumi, valamint helyszínen elvégzett vegyi-sugárellenőrzésével, biológiai vizsgálatával összefüggő tervezést előkészíteni. További tervezést kell végrehajtani a szennyeződött készletek mentesítéséhez szükséges berendezések, gépek, technológiák biztosítására. Megelőző védelem megvalósítására az alábbi követelmények betartása javasolt:

Növénytermesztés esetén még békeidőszakban kell tervet készíteni a gabonafélék, takarmánynövények, gyümölcsök betakarítására, a betakarított termények szennyeződés elleni védelmére (vermeléssel, silóházzal, tárházzal, magtárral és mindezek pormentes lezárásával)

Élelmiszeriparban szintén békeidőszakban kell tervet készíteni a nyersanyagok, félkész- és késztermékek szennyeződés elleni védelméről, különleges (szennyeződésmentes) gyártási technológiákról, a termelő berendezések szennyeződés elleni védelméről, az üzem pormentes lezárásának lehetőségéről, a felhasznált víz műszaki-technikai védelméről. Az ágazati szinten működő élelmiszeripar és az élelmiszeripari gazdaságok érdemelték ki az anyagi javak megelőző védelmének legfőbb jelentőségét. Ez abból adódik, hogy az ágazat védelme kiterjed magára az üzemre, továbbá az alap- és nyersanyagokra, késztermékekre, termelőeszközökre, gépekre, technológiai műveletekre stb.

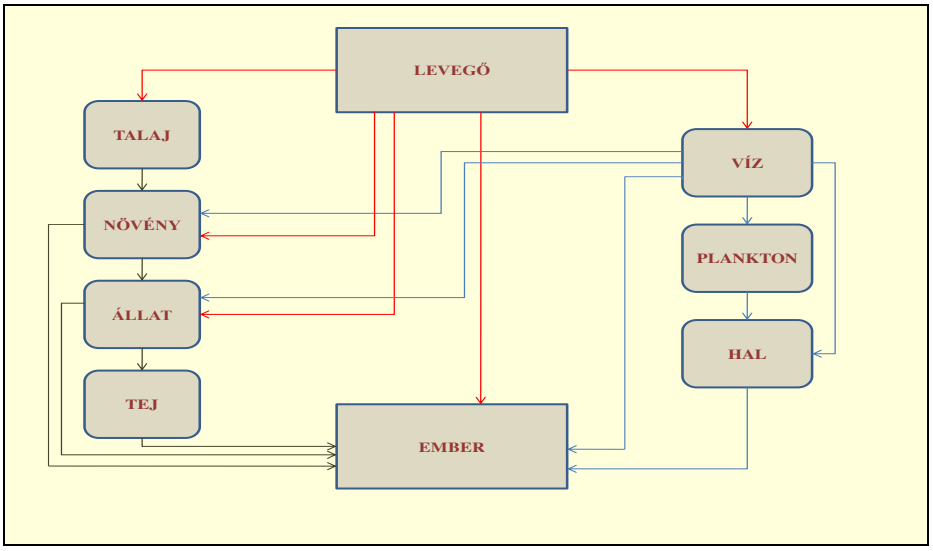
Kereskedelmi ágazatban békeidőszaki terv keretein belül kell megvalósítani a tárolt készletek védelmét, a kereskedelmi és vendéglátó bázisok készleteinek, berendezéseinek védelmét. Ezt általában a raktárak nyílászáróinak e célra való kialakításával, szellőztető berendezéssel, hermetizálással, letakarással és egyéb különleges technika bevezetésével valósítják meg.

Ivóvíz védelmének fontosságát tükrözi, hogy kizárólag a fogyasztásra alkalmas, tiszta, jó minőségű ivóvíz biztosítja az életben maradás alapvető feltételeit. Az ember mellet az állatállománynak ugyanúgy létszükséglete az ivóvíz. A mezőgazdaságban, annak növénytermesztő ágazatában sem közömbös a víz tisztaságának preferáltsága, mivel eme ágazatban rendkívül nagy vízmennyiséget használnak fel. Békés körülmények között is a felszíni, talaj-, mélységbeli és csapadékvíz sokféle mérgező-, fertőző- és szennyezőanyagot tartalmazhat. A csapadékvíz számos szennyező, fertőző anyagot tartalmazhat, mivel az esőcseppek kimossák a levegőből a szennyező anyagokat. A vízbázisvédelem célja, olyan környezetvédelmi – megelőző – intézkedések megtétele, amelynek legfőbb célja, hogy a felszínen minél kevesebb veszélyes szennyező anyag keletkezzen. A már felszín alá került a szennyeződés érdekében olyan ellenőrző rendszer üzemeltetése szükséges, amely előrejelzést és figyelmeztetést ad a szennyezés létére és ezzel meg lehet tenni a megfelelő üzemelési intézkedéseket.

Állat- és vadállomány megelőző védelme az ivó- és használati vízkészletek megelőző védelme mellett nagy jelentőséggel bír, mivel a túlélést biztosító élelmiszerek jelentős hányada állati eredetű alapanyagból készül. Esetleges veszélyhelyzet esetén az „élő élelmiszer tartalék" jelentősen csökkenhet, amely katasztrofális méreteket öltve egyfajta túlélési válságot is előidézhet. Az állatállomány megelőző védelmének megvalósítása során biztosítani kell az állattartó létesítmények védőképességét decentralizálással, távolsági védelem elvének és módszerének alkalmazásával, valamint különböző műszaki-technikai alkalmazással. Minden állattartási épületben védett körülmények között vizet és takarmányt kell tartalékolni.

Nyers-, alap- és segédanyagok megelőző védelme alá soroljuk a hús- és baromfiiparban, tejiparban, sütőiparban, malom- és növényolajiparban, hűtőiparban, cukoriparban, jelentkező megelőző tevékenységek összességét.[7][9]

A veszélyeztetett területen élő lakosság, valamint az egyéni gazdaságok esetében lehetőség adódik a felkészülésre, valamint a védelmi módszerek öntevékeny módon való elvégzésére. Gazdálkodó szervezetek vonatkozásában a megelőző védekezéssel összefüggő tervezést és kivitelezést az illetékes polgári védelmi szerv vezetője irányítja. A jogszabály minderről a következőképp rendelkezik: „Az ágazati anyagi javak rbv. megelőző védelme érdekében az előállítás, a feldolgozás, a tartás, a raktározás, a csomagolás, a szállítás technológiáinál biztosítani kell a rendszer zártságát, szükség esetén a zártság utólagos kialakításának előfeltételét, továbbá az rbv. ellenőrzés és mentesítés lehetőségének megteremtését. Az anyagi javak rbv. védelmi műszaki-technikai követelményeit a létesítmények kijelölése, tervezése, rekonstrukciója, a technológiai rendszer módosítása, a higiénés előírások meghatározása során a különböző szintű szakhatósági és hatósági előírásokban folyamatosan érvényre kell juttatni." [5][10]



1. ábra. A sugárszennyeződés alakulása a táplálkozási láncolatban. Készítette a szerző. Forrás: [7] [11]

Megállapítható annak ténye, hogy az anyagi javak megelőző védelmére vonatkozó műszaki intézkedések és elvek kidolgozását országos szinten kell elkezdeni. A végrehajtás során pedig a fő irányoknak megfelelően fokozatosan kell kidolgozni a helyi feladatokat, amelyek később egy komplex országos terv részét képezik majd. [7][12]

9 94.-143. o.

10 4. § (5)- (6)

11 97. o.

12 13. o.

ANYAGI JAVAK ELLENŐRZÉSE

Szükséges az adott termékeket, javakat egyfajta helyszíni, illetve laboratóriumi vizsgálat alá vetni, annak érdekében, hogy megállapítható legyen annak fogyaszthatósága (további felhasználhatósága), bizonyos mentesítésre való lehetősége (fertőtlenítés), vagy adott esetben megsemmisítése. Az ellenőrzés kiterjed a termelésben és technológiában felhasznált, valamint a háztartások és az azt körülvevő anyagi javak mintavételezésére és laborvizsgálataira. Példaként említve, egy nukleáris veszélyhelyzetben a létfenntartáshoz nélkülözhetetlen javakat speciális laboratóriumi ellenőrzésnek kell alávetni, ahol kiértékelhető és megállapítható a termék fogyaszthatósága. A vizsgálat eredménye egy olyan mutató, amely az élelmiszerben, vagy az ivóvízben lévő radioaktív anyagok jelenlétét, továbbá azok mennyiségét, ezáltal veszélyességét tükrözi. A kapott eredményt összevetik a vizsgált termék eleve adott fogyaszthatósági mutatóival. Ezzel kiderítve azt, hogy érte-e káros hatás a vizsgált anyagot. Amennyiben igen, választ adhat arra is, hogy adott esetben mentesíthető-e a vizsgált termék, vagy a szennyezettség olyan mértékű, hogy fogyasztásra nem alkalmas, vagyis meg kell semmisíteni.[8]

„Az anyagi javak rbv. ellenőrzési feladatait a megyei (fővárosi) Állategészségügyi és Élelmiszer Ellenőrző Állomások (a továbbiakban: ÁÉEÁ), a Növényegészségügyi és Talajvédelmi Állomások (a továbbiakban: NTÁ), továbbá egyéb bevont és hatósági jogkörrel ellátott iparági laboratóriumok, intézetek, kutató intézetek gyakorolják. Az ÁÉEÁ és NTÁ hatósági, illetve szakhatósági közreműködése során polgári védelmi feladatokat is ellátnak. A 4. § (2) bekezdésében felsorolt anyagi javak felhasználását, forgalomba hozatalát megelőzően a minőség-ellenőrzést végző hatóságnak rbv. anyagokra folyamatosan monitoring vizsgálatot, a minősített időszakban pedig tételes vizsgálatot kell végeznie, és engedélyt kiadni csak fogyasztásra alkalmas minősítés után szabad.” [5][13]

KÁROS HATÁSOK ÁLTAL SZENNYEZETT ANYAGI JAVAK MENTESÍTÉSE

Erre akkor kerülhet sor, amikor a vizsgálat alá vetett anyagi javak nem felelnek meg a fogyaszthatósági (felhasználhatósági) normáknak, azonban azok mentesítésére lehetőség van, sőt adott esetben szükséges is. Az anyagi javak szennyeződése, fertőződése esetén szükséges megtenni a kellő mértékű eltávolításra és mentesítésre irányuló intézkedéseket. A mentesítésnek ki kell terjednie a mezőgazdaság, az élelmiszeripar, a vadgazdálkodás, halászat, erdőgazdálkodás, elsődleges faipari termelés, az ezekhez kapcsolódó szolgáltatás, kutatás és fejlesztés, továbbá a mezőgazdasági termékforgalom, az agrár-környezetgazdálkodás, a növényegészségügy, az állategészségügy és élelmiszer-ellenőrzés területeire és műveleteire.

Az anyagi javak védelmének műszaki feladatai:

- a veszély elhárításával arányos módon, időben fel legyen sorakoztatva minden olyan műszaki technikai eszköz és felszerelés, amely a védekezéshez szükséges
- ún. műszaki számvetéseket kell abszolválni, amelynek eredményeként meghatározható a szükséges erőforrás. Mindezt annak céljából kell tenni, hogy a kialakult veszélyhelyzettel szemben megfelelő erő- és eszközmennyiség legyen felsorakoztatható.
- a műszaki felderítés eredményének tükrében ki kell dolgozni a kialakult veszélyhelyzet elhárításához szükséges legmegfelelőbb védekezési módszert.

13 5. § (1)- (2)

- munkaszervezési, javítási és anyagellátási tervet kell kidolgozni a védekezés műszaki munkáira vonatkozóan, valamint meg kell szervezni ezek végrehajtását.
- ki kell jelölni a műszaki védelem munkaterületeit és munkahelyeit, továbbá meg kell teremteni és azon felül folyamatosan biztosítani a műszaki technikai eszközök alkalmazási és üzemeltetési feltételeit.
- Szükségszerű a különböző technikai eszközök együttműködésének megtervezése, megszervezése, valamint mindezek biztosítása
- a műszaki eszközök esetleges részleges, vagy teljes kivonása során a felkészülés mellett el kell készíteni a a végrehajtás ütemtervét, továbbá a jelentkező logisztikai feltételeket biztosítani kell.
- A kulcsfontosságú anyagi javak megóvása és az állampolgár fizikai védelmének biztosítása érdekében – a veszélyeztetettség mértékének megfelelően – kell megtervezni és megszervezni a lakosság és az anyagi javak védelmét.
- A védelmi feladatok ellátását a lehető legrövidebb idő alatt, szervezetten és a legkisebb költséggel kell megvalósítani
- Minden esetben a veszélyeztetettségnek megfelelő mértékben kell alkalmazni a távolsági védelem rendszabályait, valamint az egyéni és kollektív védőeszközöket, felszereléseket, védelmi létesítményeket.[5]

ÖSSZEGZÉS

A lakosság és az anyagi javak védelmének tervezését, szervezését és megvalósítását főbb rendeltetésének megfelelően, szervezetten, a lehető legrövidebb idő alatt, továbbá lehetőségekhez mérten a legkisebb költséggel kell végrehajtani. A veszélyeztetettség mértékének megfelelő és célirányos alkalmazással tehetjük hatékonyabbá az egyéni és a kollektív védelem során használt és igénybe vett védőeszközöket, felszereléseket, védelmi létesítményeket.

Létfenntartáshoz szükséges anyagi javak védelme eredendően a lakosság alapvető ellátását és életfeltételeit biztosító anyagokra, eszközökre, rendszerekre és készletek összességére irányult, különösen az ivóvíz-, az élelmiszer-, a takarmány-, a gyógyszerkészletek és a haszonállatok tekintetében. Korábban ezek RBV védelmét jelentette, de napjainkra ez a kör más egyéb javakkal, feladatai más feladatokkal bővült. A rendeltetése az állam működőképességének, továbbá a lakosok életben maradásához szükséges javainak a megóvása.

Alapvető területei a létfenntartáshoz szükséges élelmiszer és ivóvízkészletek, műtárgyak, a mezőgazdasági létesítmények, az állatállomány és a növényzet, a takarmány és vetőmagkészletek, az ipari létesítmények, berendezések, gépek, valamint az energiaforrások-, hálózatok, nyersanyagok gyógyszerek- és kötszerek, egészségügyi felszerelések, gépek, eszközök védelme. Hozzátartoznak a pótolhatatlan kulturális értékek, műkincsek, a tűzvédelemhez szükséges eszközök, anyagok, gépek, valamint a közművek, út- és vasútvonalak, közlekedési csomópontok védelme.

A védelem a katasztrófák elleni védelemhez hasonlóan megelőző időszaki, a védekezés során folytatott, és a veszélyeztető hatás elmúlását követő időszakban végzett tevékenységekre csoportosítható. A védekezés során az anyagi javak védelme az állapotuk felmérésével, majd a szükséges mentési, mentesítési stb. eljárások alkalmazásával történik. A veszélyeztetettség mértékének megfelelő és célirányos végrehajtásával hatékonyabbá tehetőek az egyéni és a kollektív védelem során használt, valamint igénybe vett védőeszközök, felszerelések, védelmi létesítmények.

Felhasznált irodalom

[1] Czeglédi László: Minőségmenedzsment – A humánerőforrás minőségi kérdései. 2011. Eszterházy Károly Főiskola www.tankonyvtar.hu/hu/tartalom/tamop425/0005_42_minosegmenedzsment_scorm_10/1032_a_humnerforrs_minsgi_krdsei.html Letöltés ideje: 2013. 07. 12.

[2] 234/2011. (XI.10.) Korm. rendelet A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

[3] Polgári védelem alapjai – Katasztrófavédelem., Tansegédlet, Kiadó: CEDIT információtechnikai Kft.

[4] Dr. Tóth Rudolf: A lakosságvédelem aktualitása, helye, szerepe napjaink új kihívásainak tükrében. Polgári Védelmi Szemle V. évfolyam 2. szám (2009.)

[5] 2/1998. (I.12.) FM rendelet a földművelésügyi ágazat polgári védelmi feladatairól.

[6] Megelőző műszaki-technikai védelem – A Polgári Védelem Országos Parancsnokságának kiadványa, 1972.

[7] Megelőző műszaki-technikai védelem /7/- Megelőző RBV védelem /8/– A Polgári Védelem Országos Parancsnokságának kiadványa, 1972.

[8] Pellérdi Dezső: A polgári védelem és a nukleárisbaleset-elhárítás. (ZMNE)

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Tímár Tamás
tamastimarphd@gmail.com

A KÖRÖS MENTŐCSOPORT, MINT TERÜLETI POLGÁRI VÉDELMI SZERVEZET

III. RÉSZ

Absztrakt

A Békés megyei Körös Mentőcsoport (KMCS) speciális mentési és beavatkozási képességekkel rendelkezik. A katasztrófák elleni védekezés területi szinten történő megvalósulásának részeként a különleges mentőcsapat alkalmazására is sor kerülhet. Ezen felül az ország bármely pontján és külföldön is bevethetők. A tanulmány első része a csoport felépítését, a második rész a szerkezeti és funkcionális összetételt taglalja. A III. rész a képzési és továbbképzési rendszerrel, valamint a nemzeti minősítéssel foglalkozik, illetőleg az alkalmazásokra tér ki.

The Körös Rescue Team from Békés county has a special rescue and response capabilities. A special group can be use, in part of protection against disasters in local level. In addition, at any point in the country and abroad can be deployed. The first part of the essay includes the sructure of the team, the second section discusses the functional composition. The III. part comprises the educational training system, the national certification schemes and the activities.

Kulcsszavak: *Körös Mentőcsoport, katasztrófa, képzés, minősítés ~ Körös Rescue Team, disaster, training, qualification*

A KÖRÖS MENTŐCSOPORT GYAKORLATI KÉPZÉSE

A speciális csapat a megalakulásának évében egy rendszerbeállító gyakorlaton vett részt, majd a későbbiekben minden évben volt felkészítés. A gyakorlatok során olyan feladatokat hajtottak végre az alegységek, amelyek a nemzetközi előírásoknak megfelelő beavatkozást igényeltek. A komplex szimulációknak köszönhetően a mentőcsapat minden komponense elsajátíthatta a nagy kiterjedésű kárterületeken kialakult helyzetekből adódó bonyolult kutatási és mentési metodikákat, tevékenységi sorokat, továbbá fejleszthette eljárási rendjét. „A Körös Mentőcsoport kiemelt pozitívuma, hogy az egyenként kiemelkedő képességekkel rendelkező tagegységeket úgy sikerült összehangolni, hogy kialakult egy hatékony, alkalmazás esetén releváns és komplex segítséget nyújtó speciális mentőszervezet.” [1]

1. ábra. Körös Mentőcsoport eligazítása a gyakorlat kezdetén [2]

Kiképzések, gyakorlatok, felkészítések rendszere

A mentőcsoport felkészítése, kiképzése és gyakoroltatása éves rendszerességgel komplex és részgyakorlatok végrehajtásával biztosított. A kiképzések és gyakorlatok végrehajtása minden esetben más hivatásos elsődleges és üzemi kárelhárító szervezetekkel együttműködve történik, hiszen a társszervek összehangolt munkája szükséges a hatékony kárelhárításhoz.

Rendszerbeállító gyakorlat

A Mentőcsoport rendszerbeállító gyakorlata 2010. április 29-30-án zajlott, Gyomaendrőd településen. A széleskörűen, alaposan és élethűen kialakított gyakorlati helyszíneken minden egyes alegység képessége tesztelésre került. A KMCS kutatási, mentési és egészségügyi képességeit előtérbe helyezve kialakított kárhelyszíneken gyakorolt. A gyakorlat keretén belül a speciális feladatok szakszerű végrehajtásán kívül vizsgálták és ellenőrizték a mentőcsoport riaszthatóságát, a tagok beérkezésének normaidejét, a kommunikációs rendszer működtetését, valamint a hivatásos állományra vonatkozó irányítási, vezetési és egyéb logisztikai biztosítási feltételek meglétét is.

2. ábra. Körös Mentőcsoport riasztása [3]

Az értesítési feladatot követően a gyülekezési helyre érkeztek a csapat alegységei. Ezt követően elméleti felkészítés történt a teljes állományra vonatkozóan, bevetéselmélet, nemzetközi normák, kárterületi eljárások, tevékenységi sorok, munkavédelmi fejezet és részletes eligazítás a gyakorlat publikus adatairól (ugyanis olyan feladatelem is tervezett volt, amit nem tudtak előre a beavatkozók).

Az egységek a következő gyakorlatelemeket hajtották végre: 1. helyszínen kutyás kutatás, felderítés, mentés, alpintechnikai mentés, romos épület aládúcolása és tűzoltás; a 2. helyszínen vízről- és vízből mentés, továbbá árvízi védekezési feladatok.

3. ábra. Árvízi védekezési feladatok végrehajtása [4]

Nemzetközi gyakorlat

A KMCS 2011. évi felkészítésére április 13-14-én, Békéscsabán került sor. A gyakorlat keretén belül a Magyarország Kormánya és Románia Kormánya között a katasztrófák esetén történő együttműködésről és kölcsönös segítségnyújtásról szóló egyezmény [5] értelmében együttműködési gyakorlat került végrehajtásra. A magyar beavatkozó egységek mellett Romániából összesen 12 fő vett részt a gyakorlaton, 1 búvárcsoport 4 fővel, 1 tűzoltóraj 6 fővel, 2 fő műveleti tiszt irányítása mellett.

A 2011. április 13-án végrehajtott gyakorlat alapvető feltételezése szerint Békéscsaba településtől 3 kilométerre, délre található epicentrummal, a Richter skála szerinti 7,2-es erősségű földrengés-szituáció alakult ki. Az esemény jelentős épületkárokat okozott a településen, továbbá a rengések hatására ipari övezetekben műszaki és infrastrukturális meghibásodásokkal lehetett számolni. A beavatkozásokhoz kapcsolódóan szükségessé vált az elsősegély nyújtási és a mentálhigiéniás segítség is. Ezért a kiképzett KMCS állomány az együttműködő szervezetekkel került alkalmazásra.

A gyakorlat során a KMCS teljes állománya, 58 fővel került alkalmazásra. Feltételezve, hogy a Békés megyében rendelkezésre álló erők és eszközök nem elegendőek a kiterjedt kárterületen jelentkező speciális mentési és kárelhárítási, valamint egészségügyi feladatok ellátására, így a nemzetközi segítségnyújtás keretében román speciális mentőszervezetek állományai is riasztásra kerültek. A határ túl oldaláról, az Arad Megyei Veszélyhelyzeti Felügyelőség hivatásos szervének tűzoltó, speciális búvár képességekkel rendelkező csoportjai kerültek bevetésre.

Körös Mentőcsoport nemzeti minősítő gyakorlata

A katasztrófavédelem szabályozása alapján az önkéntes mentőszervezeteket a nemzeti minősítő rendszer keretén belül minősíttetni kell. Így csak azok az egységek vegyenek részt a katasztrófák felszámolásában, amelyek állománya rendelkezik a szükséges ismeretekkel, és vizsgát tesz. A katasztrófavédelmi törvény kimondja, hogy „az önkéntes mentőszervezetek olyan különleges képzettséggel rendelkező egyének alkotják, akik speciális technikai

eszközökkel a katasztrófákat követő hatásokat kivédik, a következményeket felszámolják, és legfontosabb feladatuk az élet mentése.” [6]

A Körös Mentőcsoport (KMCS) két kategória alapján minősíttette magát: a városi kutató és mentő (USAR), műszaki mentő képesség, valamint az árvíz-védekezési és -mentési képességek, a komplex árvízi védekezés alapvető szakmai követelményei alapján. A KMCS és a Jász-Nagykun-Szolnok megyei Tisza Mentőcsoport közös nemzeti minősítő gyakorlatára 2012. április 14-15-én került sor, Gyomaendrődön (a KMCS teljes állománya 58 fő, a Tisza Mentőcsoport állománya 52 fő). A törzsvezetési gyakorlaton az Országos Katasztrófavédelmi Főigazgatóság közvetlen irányítása alá tartozó Krízis-Intervenciós Csoport is részt vett.

4. ábra. Eligazítás a gyakorlaton [7]

Az első helyszínen a feltételezés szerint viharkár következtében megsérült épületek találhatóak, 2 fő sérülést szenvedett, a romok alatt rekedtek, valamint 1 személy eltűnt. A megközelítési útvonalat eltorlaszolja egy meghibásodott nehézgépjármű, ahol a járművet szerelő személy alászorult a kamionnak. A mentőcsoport a kamion alá szorult személyt kimentette, a torlasz megszűntetését is elvégezte. A kutyás területkutatást és személykeresést összehangoltan hajtották végre a mentőcsapatok kutató egységei. A felderítés során a szabadban és az épületekben talált sérülteket az egészségügyi komponens tagjai látták el. A romos épületrész aládúcolását külső megtámasztással, valamint belső födém-alátámasztással hajtották végre. Ezt követően a sérültek egészségügyi és krízisintervenciós ellátása történt meg.

5. ábra. A sérült egészségügyi és krízisintervenciós ellátása [8]

A további feltételezés és jelzés alapján egy átfejtő művénél történt baleset során két karbantartó áramütést szenvedett, villamos berendezés javítása közben. Alpintechnikai mentés, területbiztosítás és egészségügyi ellátási feladatok végrehajtása vált szükségessé, így 12 méter magasból a különleges mentési alkalmazások is bemutatásra kerültek.

A gyakorlat soron következő feltételezése szerint egy gyomaendrődi üzem szárítóegységének karbantartása közben két fő megsérült. Feltehetően lezuhantak a felvonó tetejéről. A munkások mozgásképtelenné váltak, és egy dolgozó elmondása szerint további 1

fő eltűnt. A mentési feladatok végrehajtása alpintechnikai módszer alkalmazásával történt. Az egységek a kárhelyszín műszaki biztosítását, valamint sérült személyek elsősegély-nyújtási és krízisintervenciós ellátási feladatait látták el. A kutatás keresőkutyákkal történt.

6. ábra. Alpintecnikai mentés [9]

Ezt követően a Hantoskerti holtágon volt feladat, ahol a feltételezés szerint négy felnőtt személy vízibiciklizés közben vízbe esett. Szükségessé vált az eltűnt személyek víz alatti kutatása, így a Körös Mentőcsoport búvár és vizimentő egysége radaros keresést hajtott végre. A kimentett személyeket egészségügyi ellátásban, a sétáló szemtanukat krízis intervenciós ellátásban kellett részesíteni. A Hármas-Körös szabadstrandján lévő kárhelyszínen 30 fő személy árvízi mentésére kellett intézkednie a mentőcsoport vezetési törzsének. A folyó gyomaendrődi szakaszán található hidaktól történt a szállítás a szabad strandra.

7. ábra. A Körös Mentőcsoport búvár és vízimentő egysége [10]

A mentőcsapat mentési és árvíz-védekezési képességekből is minősítésre készül, ezért védekezési feladatokat hajtottak végre, ennek keretében töltés megtámasztást (bordás megtámasztást), buzgár elfogást, védmű-fóliázást végeztek.

Az utolsó helyszín egy ipari park területén került kialakításra, ahol 120 km/h erősségű vihar söpört végig, épületkárok, romosodások keletkeztek. A feltételezés szerint a szélsőséges időjárás következtében a telephely vezetője nem találta a munkásait, így szükségessé vált az eltűnt személyek felkutatása és mentése, veszélyes anyag jelenlétében. A mentést nehezítette, hogy az eltűnt személyek betonpallók, vasbetonoszlopok, farönkök és vasszerkezetek alá szorultak, így a födémáttörés és a betonszerkezetek vágása is a megmérettetés eleme lehetett. A mentőcsapatok a tevékenységeket hajnali három órakor fejezték be.

8. ábra. A nemzeti minősítés értékelése [11]

A Körös és a Tisza mentőcsoportok a nemzeti minősítés által előírt szakmai követelményeknek eleget tettek.

A KÖRÖS MENTŐCSOPORT JELENTŐSEBB BEVETÉSEI:

Árvízi helyzet kezelése Borsodban:
A mentőcsoport segítségét kérte a kialakult árvízi helyzet kezelésekor Borsod-Abaúj-Zemplén Megye Védelmi Bizottsága (MVB) a Békés Megyei MVB elnökétől 2010. május 17-én, aki határozatban rendelte el a Körös Mentőcsoport alkalmazását. Összesen 35 fő segített Sajóecseg, Edelény, és Boldva településeken május 22-ig. A beavatkozás során a mentőcsoport tagjai vezetési és logisztikai feladatokat teljesítettek, továbbá hagyományos árvíz elleni védekezési feladatokat (nyúlgátépítés, bordásmegtámasztás, víz alatti fóliázás, személymentés, egészségügyi és pszichoszociális ellátás).

Viharkárok felszámolása Szabolcs-Szatmár-Bereg megyében:
A Körös Mentőcsoport mentési komponense a Nyírségben keletkezett viharkárok felszámolásában vett részt más hivatásos és önkéntes tűzoltó egységekkel együttműködve 2010 júniusában, Nyírbátor településen.

Vízfelszíni és víz alatti kutatás-mentési feladatok Békés megyében:
A mentőcsoport kutatási és mentési komponensének egy-egy búvár egysége a rendőrséggel és hivatásos tűzoltó szervekkel együttműködve rendszeresen végzi eltűnt emberek vízfelszíni és víz alatti kutatását, mentését a Békés megyei folyószakaszokon. Évente több alakalommal kerül sor a társszervektől ékező segítségkérésre.

Krízisintervenciós feladatok:
Békés megyében a 2011. év elején kialakult belvízi elöntések során a kitelepített lakosság lelki gondozásában nyújtottak segítséget a krízisintervenciós csoport tagjai.

KMCS búvár- és vízimentő szolgálat:
A Körös Mentőcsoport 2011. július 15. és szeptember 1. között a Fehér, illetve Kettős-Körös összesen 15,65 kilométeres szakaszán (Gyula Városerdő és Doboz közúti híd közötti folyószakasz) búvár és vízimentő készenléti szolgálatot látott el, hét fővel. A szolgálat ellátása során elsődleges szempont volt a kijelölt fürdőhelyek, valamint a hajók kikötésére alkalmas stégek felügyelete. Ezeken a helyeken voltak szabálytalan helyen fürdőző emberek, ahol az egység a szabadstrand használatára intézkedett. A mentőcsoport készenléti szolgálata javította az említett folyószakaszok és kijelölt fürdőhelyek biztonságát, így emberi élet mentésére nem volt szükség.

ÖSSZEGZÉS

A Körös Mentőcsoport a nemzetközi irányelveknek megfelelően kialakított egység. A komponensek egymásra épülnek, de ugyanakkor önállóan is képesek a feladat ellátására. A csoport minden évben szervez gyakorlatot az ismeretek folyamatos szinten tartása, a nemzetközi kapcsolatok mélyítése, valamint a továbbképzések fejlesztése miatt. A sikeres nemzeti minősítés megszerzését követően a Körös Mentőcsoport képes az országban bárhol, vagy külföldön is beavatkozni, illetőleg speciális kutatási és mentési munkálatokat végrehajtani. A katasztrófavédelmi törvény végrehajtási rendelete kimondja: „A Nemzetközi Minősítési Rendszer az ENSZ Nemzetközi Kutató és Mentő Tanácsadó Csoportja által kidolgozott irányelveknek és módszertannak megfelelően kialakított, elméleti oktatásból és gyakorlati kiképzésből álló, képesítést adó rendszer, amely alkalmas arra, hogy meghatározott eszközrendszerrel rendelkező, a hivatásos katasztrófavédelmi szerv területi szerve által nyilvántartásba vett és megfelelő szakmai képesítéssel rendelkező személyekből álló mentőszervezet részt vegyen a nemzetközi segítségnyújtásban.” [12] Így tehát a nemzeti minősítést követően több lehetőség van a mentőszervezetek számára.

A kormány évente több millió forintnyi támogatást biztosít ahhoz, hogy az önkéntes mentőszervezetek még hatékonyabban láthassák el feladataikat. A Békés Megyei Katasztrófa- és Polgári Védelmi Szövetség által benyújtott nyertes pályázatnak köszönhetően a Körös Mentőcsoport tagszervezetei támogatásban részesülnek, amelyből jut a feladatok ellátásához szükséges technikai- és védőeszközökre, azok fenntartására, valamint gépjárművek és technikai eszközök javítására, felújítására, továbbá a mentőszervezeti tagok oktatására is.

A Körös Mentőcsoport már több alkalommal bizonyította helyét és szerepét a katasztrófák elleni védekezésben, hazai és nemzetközi szinten. Az elsőként megalakuló, területi szintű mentőszervezet példáját azóta sok megye és katasztrófavédelmi igazgatóság követte. A csoport állományából 1 fő csapatvezető-helyettes, 2 fő alpintecnikai mentő, 2 fő műszaki mentő, 2 fő elsősegélynyújtó és 1 fő állatorvos integrálásra került a nemzetközi katasztrófa segítségnyújtási feladatok ellátására létrehozott HUSZÁR központi rendeltetésű mentőszervezetbe. A központi rendeltetésű mentőszervezet a hazai és a nemzetközi segítségnyújtásban bevethető alakulat, amely 2012. októberében Az ENSZ INSARAG [13] szerinti közepes városi kutató-mentő képesítést szerezte meg.

A CIKK A TÁMOP-4.2.1.B-11/2/KMR-0001 KRITIKUS INFRASTRUKTÚRA VÉDELMI KUTATÁSOK PROJEKT TÁMOGATÁSÁVAL KÉSZÜLT.

Felhasznált irodalom:

[1] A Körös Mentőcsoport minősítő gyakorlatának értékelése – Haskó György tű. alezredes, KMCS parancsnok

[2] Készítette: Csatári István tű. hadnagy, Gyomaendrőd, 2010. április 29.

[3] Készítette: Kisgyurka Sándor tű. főhadnagy, Békéscsaba, 2010. április 29.

[4] Készítette: Kisgyurka Sándor tű. főhadnagy, Gyomaendrőd, 2010. április 29.

[5] 2004. évi LXXXI. törvény a Magyar Köztársaság Kormánya és Románia Kormánya között a katasztrófák esetén történő együttműködésről és kölcsönös segítségnyújtásról szóló, Budapesten, 2003. április 9. napján aláírt Egyezmény kihirdetéséről

[6] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról, I. fejezet, 3. §, 19. bekezdés

[7] Készítette: Győző-Molnár Árpád tű. hadnagy, Gyomaendrőd, 2012. április 14.

[8] Készítette: Szűcs Csaba tű. főhadnagy, Gyomaendrőd, 2012. április 14.

[9] Készítette: Szűcs Csaba tű. főhadnagy, Gyomaendrőd, 2012. április 14.

[10] Készítette: Győző-Molnár Árpád tű. hadnagy, Gyomaendrőd, 2012. április 15.

[11] Készítette: Győző-Molnár Árpád tű. hadnagy, Gyomaendrőd, 2012. április 15.

[12] 234/2011. (XI. 10.) Kormányrendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásról, VIII. fejezet, 45. pont, 66. §. 3. bekezdés

[13] International Search and Rescue Advisory Group - Nemzetközi Kutató-mentő Tanácsadó Csoport (www.insarag.org – letöltés ideje: 2012. 10. 11.)

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Gulyás Attila
attila.gulyas@mil.hu

ENABLE COMMAND AND CONTROL BY UPDATED DEPLOYABLE CIS DEVICES

Abstract

The International Security Assistance Forces (ISAF) are to reduce its personnel and capabilities. In time of restructuring our forces, there is a need to continue providing high standards Communications and Information System connectivity between ANSF Advisory Teams/Security Forces Assistance Teams and Regional Headquarters. One of the most improved services is the tactical satellite connection and the devices that make that possible in this harsh environment. In the short article the author would like to sum up the methods and the possibilities enabling command and control by deployable communications equipment.

A Nemzetközi Biztonsági Együttműködő Erők (ISAF) műveleti képességeinek csökkenésével a személyi állomány létszámarányai is változnak, átalakításra kerülnek. Az átalakítás időszakában is szükség van magas színvonalú híradó és informatikai szolgáltatások biztosítására az Afgán Nemzeti Biztonsági Erők támogatását megvalósító Tanácsadói Csoportok és az ISAF Vezetési Pontok között. Az egyik alkalmazott, fejlett szolgáltatásokat biztosító rendszer a harcászati műholdas összeköttetések rendszere. A szerző rövid összefoglalójában bemutatja az alkalmazott összeköttetési módokat és a mögöttük álló lehetőségeket a telepíthető (tábori) híradó és informatikai rendszerek területén.

Keywords: *tactical satellite, CIS support ~ harcászati műholdas összeköttetés, híradó és informatikai támogatás*

INTRODUCTION

The international forces, in support of the Government of the Islamic Republic of Afghanistan (GIRoA), conducts operations in Afghanistan to reduce the capability and will of the insurgency, support the growth in capacity and capability of the Afghan National Security Forces (ANSF), and facilitate improvements in governance and socio-economic developments in order to provide a secure environment for sustainable stability that is observable to the population [1]. In accordance with all the relevant Security Council Resolutions1 [2], the International Security Assistance Forces (ISAF)'s main role is to assist the Afghan government in the establishment of secure and stable environment. ISAF forces are conducting security and stability operations throughout the country together with the Afghan National Security Forces and are directly involved in the development of the Afghan National Army (ANA) and Police (ANP) through mentoring, training and equipping. ISAF is supporting reconstruction and development (R&D) in Afghanistan, securing areas in which reconstruction work is conducted by other national and international actors. ISAF is also providing practical support for R&D efforts, as well as support for humanitarian assistance efforts conducted by Afghan government organizations, international organizations and Non Governmental Organizations. ISAF is helping the Afghan Authorities strengthen the institutions required to fully establish good governance and rule of law and to promote human rights. The principal mission is this respect consists of building capacity, supporting the growth of governance structures and promoting an environment within which governance can improve [3].

EFFORTS OF ISAF COMBINED TEAM NORTH IN TIME OF RESTRUCTURING

ISAF's intent is to keep ANSF in lead and continuously strengthen their abilities to provide security in all Afghanistan. The idea is to effectively utilize all available Regional Command (RC) resources in cooperation with civilian authorities along with governmental and non governmental organizations to contribute to lasting development in Afghanistan. The aim is to establish processes which are feasible and sustainable for the ANSF and which set the stage for a secure transition to post-ISAF [4].

ISAF's enduring priorities may be the following [5]:

- Support ANSF Senior Leadership and key ANSF HQs professionalization;
- Support ANSF in developing logistics and maintenance capabilities;
- Support ANSF infrastructure sustainment;
- Support ANSF in developing organic enablers like:
  a) ANSF EOD[2] and C-IED[3]
  b) ANSF Medical Capabilities incl. CASEVAC[4] and MEDEVAC[5]
  c) ANSF CIS[6]
- Support OCC-R/P[7] developments;
- Support ANSF non-kinetic capabilities (e.g. InfoOps[8], PA[9], CIMIC[10]).

[1] United Nations Security Council document S/RES/2096 (2013)
[2] EOD – Explosive Ordnance Disposal
[3] C-IED – Counter – Improvised Explosive Devices
[4] CASEVAC – CASualty EVACuation
[5] MEDEVAC – MEDical EVACuation
[6] CIS – Communications and Information System
[7] OCC-R/P - Operational Coordination Center Region/Province
[8] INFOOPS – Information Operations
[9] PA – Public Affairs

In support of ISAF operations, Regional Commands will simultaneously conduct theatre redeployment operations including the necessary base closure/transfer in line with HQ IJC Unified Implementation Plan.

HOW CAN ISAF REACH ITS GOALS?

ISAF may continue to train, assist and advise ANSF in areas with permanent ISAF presence. Among the ANSF, Regional Commands increasingly focuses on Afghan National Army and Afghan National Police BDEs as they are in charge for securing key terrain, the Afghan Uniformed Police (AUP) and the Afghan Locale Police (ALP) as the primary means for providing security. As ANSF capabilities steadily increase ISAF will „thin-up" their Security Forces Assistance (SFA) operations from „Brigade and provincial level" to „Corps and regional level" in a gradual approach [6]. ISAF continue to liaise and co-operate with the GIRoA to support development of governance. Operational momentum and SFA requirements will be synchronized with redeployment activities and the reset of the theatre. The overall plan will be supported by Information and Communication Activities.

POST-2014 END STATUS

ISAF mission may come to a successful ending when ANSF have taken over lead security responsibility in designated transition areas and have established a safe and secure environment for the third presidential and provincial council elections; ANSF retains security in Regional Commands' Key Terrains; ANP has security primacy in main population centers and possesses the capability, capacity to protect the Afghan population as well as the Border Crossing Points (BXPs); Enemy of Afghanistan (INS11) are operationally defeated and denied of safe havens in key terrains; their ability to threaten secured areas and main population centers has been disrupted and they are incapable of successfully undermining the legitimate and sovereign GIRoA; develop a more self-sustainable GIRoA with stronger connections between different levels of government; support development processes; act in accordance with Afghan Law and is accepted by the majority of the population; Coalition Force Posture and redeployment activities are synchronized with the momentum of SFA and ANSF operations; identified bases are successfully closed/transferred; GIRoA-ANSF-ISAF activities have been successfully communicated and positively perceived by target audiences [7].

The International Community's (IC) vision is that the Afghan National Security Forces is deemed competent to ensure safe and secure environment in many parts of the ISAF Area of Interest (AOI) without ISAF partnering and mentoring support. The Coalition Forces led by United States of America (USA) have generated and equipped afghan troops, have provided infrastructure adequate for the ANSF of 352k in accordance with GIRoA, NATO/ISAF and ISAF IJC priorities [8]. Long term planning for the future ANSF force size and International Community funding of the ANSF is almost certain to result in a smaller force post 2015. As a consequence of the equipping of the ANSF for a 352k force structure, GIRoA is going to find itself in possession of excess equipment and infrastructure should the force size be adjusted post 2015. Any coalition retrograde operations which result in transfer of equipment and infrastructure to the ANSF will exacerbate the fiscal burden which the international community and GIRoA will bear in sustaining the ANSF. This will occur at a time when the security ministries and the ANSF logistics systems are in the nascent stage of development

[10] CIMIC – Civil-Military Cooperation
[11] INS – Insurgents = Enemies of Afghanistan (COMISAF-approved term for insurgent troops)

and unable to sustain the increased demands of a large un-forecasted and unprogrammed equipment and infrastructure influx.

The opportunity and the challenge is how ISAF can provide support for own troops and ANSF as well during the restructuring and redeployment period. The CIS connectivity is one of the main efforts of any commander in theatre with primary and secondary objectives. In the next few chapters I would like to discover the commanding system between company/battalion levels and higher to Corps/Headquarters (HQ) level, to highlight the importance of CIS support and sum up the possibility of developments.

PROVIDING CIS SUPPORT FOR ISAF RESTRUCTURING

The continuing development of the Afghan National Security Forces is a crucial factor towards transition and therefore long term ISAF mission success in Afghanistan. A key element of this is the ability of the ANSF to communicate operationally and tactically, and exercise command and control at all levels within the operational area. Regional Commands and subordinate units need to monitor and develop the forces, through partnering and mentoring the ANSF communications capability at the Corps/HQ level and below. This includes direction to Regional Commands to formalize ANA/ANP/ISAF partnering, circulation for comment of the draft ANA/ANP assessment criteria.

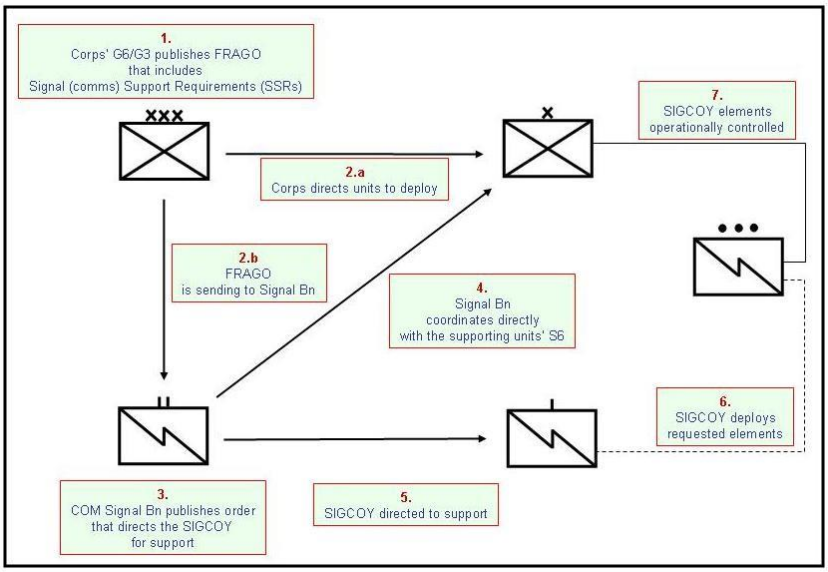
The developments should focus on ANA/ANP collective communications capability, building on the solid foundations provided by individual courses under the guidance of NATO Training Mission – Afghanistan (NTM-A) and Coalition Training and Advisory Group – Afghanistan (CTAG-A) by the view of partnering and mentoring ANSF forces. Partnering and mentoring are defined as follows [9]. *Partnering is an assigned relationship between like-size and like-type ISAF and ANSF units in which both share the goal of working together, "shoulder-to-shoulder" to build capacity and capability. Ideally, the units should live, work, plan, train and conduct full spectrum combat operations together. Mentoring has some differences. The mentor teaches, guides, and advises the ANSF unit by providing information and advice on how to best use the resources available within the Afghan construct. Mentoring is focused on building individual competency and capacity within the leadership and staff of the ANSF so that it is able to perform individual, leader and collective tasks. ANA mentors are referred to as Operational Mentor and Liaison Teams (OMLT) and ANP mentors are referred to as Police Operational Mentor and Liaison Teams (POMLT).* Both partnering and mentoring require rapid, ready and reliable communications and information system built-on to support the acting commanders and his/her staffs in the military decision making processes and provide timely and secure communications channels for the near-real-time connections. To provide seamless functions of command and control for partnering and mentoring teams, the following CIS services are necessary during ISAF restructuring and redeployment:

- Provides the ISAF Headquarters with an on-call contingency communications capability in the event that the fixed strategic network is disrupted or for other contingency operations;
- Provide deployable communications systems capable of supporting command and control;
- Provide connectivity between deployed elements, control centers and other users of the coalition strategic network;
- Focus on deployable capabilities, quick-reaction and limited-duration missions;
- Provide a capability to implement initial communications during the early phases of the teams' response to a crisis or other operations as prescribed by the Team Headquarters;

– Provide the Headquarters with redundant and geographically independent capability to reconstitute communications in the event of a disaster, attack or other contingency scenario.

The primary mission of the CIS support shall be to deploy on order in support of Corps/HQ-level missions within area of operations; install, operate, maintain and manage tactical primary, secondary and contingency communications in support of HQs, subordinate units and other governmental agencies in the area of operations for upgraded command and control capability. The secondary mission of the CIS support shall be to provide the Corps Headquarters with redundant and geographically independent capability to reconstitute communications in the event of a disaster, attack or other contingency scenarios [**10**].

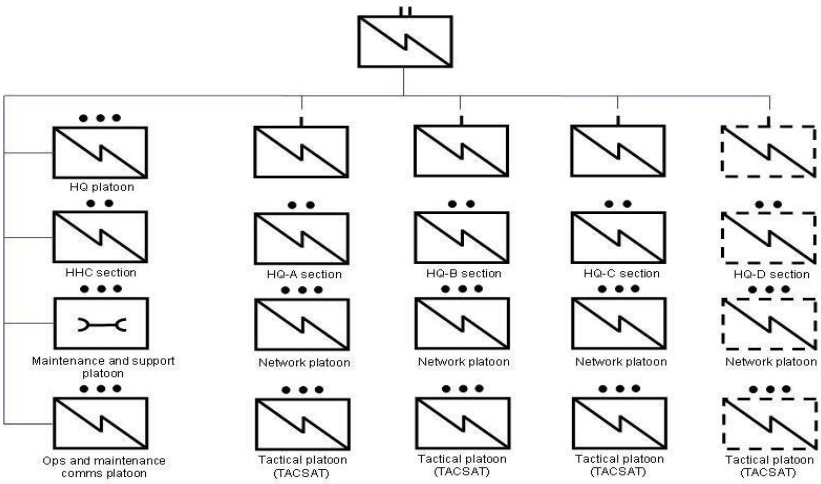
The acting force commander along with the staff determines operational and contingency missions the unit must support. Under the direction of the force commander, the operations branch (G3) with inputs for annexes from the staff, develops and publishes deployment orders. The communications branch (G6) is responsible for developing the communications annexes. The signal battalion (Bn) commander will direct the battalion S3 to determine the communications requirements to support the deployed element. Bn operations section (S3) develops and publishes orders for the company to support the mission. The Bn S3 is responsible for coordination with the requesting unit's S3 for communications and life support. Once the communications element deploys, they are Operationally Controlled (OPCON) by the supported unit, but remain Administratively Controlled (ADCON) to the signal battalion (Figure 01). Upon mission completion the unit and all support personnel will redeploy with all equipment to the signal battalion. Movement to home station will be in accordance with the deployment order.



1. figure. Operating concept flow[12]

The signal battalion, upon receiving requirements, determines the size and scope of the communications element deployed to support the requesting unit. Deploying units only articulate requirements; they do not dictate the size and scope of the communications company or unit. Mission success depends upon two equally important components, operations and support. Support of the asset or system is critical to operation success. The six facets of readiness will be used to address support issues. These include people, training, equipment, support, infrastructure and information.

[12] The author's theoretical planning for operating concept



2. figure. Signal battalion (theoretical) [13]

The signal battalion can provide CIS connectivity for ISAF forces in time of redeployment (retrograde). Its force structure makes it possible to support the force commander's different requirements. The theoretical signal battalion schema (Figure 02) gives us some interpretations how Coalition Forces can sum up the combat support CIS system. The four (4) companies[14] (SIGCOYs) provide HF/VHF/UHF connectivity and tactical satellite connections up to NATO/ISAF SECRET level for Coalition Forces. The manning of those SIGCOYs is eligible for proper and successful managements of radio communications systems. The SIGCOYs have tactical radio (signal) platoons for installing, operating and maintenance of tactical radio equipment (Tactical Satellite TACSAT) in field operations as well. Due to the hilly area mostly all over Afghanistan does not take opportunity at all times to make seamless Line of Sight (LoS) connectivity between troops, it is important to provide satellite LoS channels for better troop communications' manners [**11**]. That is why TACSAT platoon is one of the most important sub force in case of quick and seamless troop/team communications. In the next chapter I would like to provide an overview about the needs and the do's, the solutions of Tactical Satellite capability.

TACTICAL SATELLITE (TACSAT) CONNECTIONS

TACSAT provides ISAF with a secure, static and mobile communications capability, complementing the ISAF fixed voice and data communications networks. It is used as a method of Beyond Line of Sight Combat Net Radio (BLoSCNR) and gives users the ability to contact any other suitably equipped user who has been granted network access rights, and to broadcast to all users of the network simultaneously. In the ISAF the TACSAT is primarily for voice communications usage, a data capability is built within the radios but the necessary ancillary equipment - mostly - will not be provided. A single Office Module (OM) with IP data capability will be provided for Special Operations Forces (SOF) HQ. Although there are different types and models of TACSAT equipment in use within ISAF, they all have three possibilities of employment: On-The-Pause (OTP), On-The-Move (OTM) and Manpack (MP).

The On-The-Pause model describes the mode of operation where the TACSAT radio travels with its antenna stowed. The antenna must be erected, positioned, pointed and connected to the TACSAT radio before transmission or reception is possible. This has the advantage of using highly efficient directional antenna that can boost signal strength

[13] The author's theoretical plan
[14] Three (3) of the SIGCOYs are operational, one (1) SIGCOY is for reserve supporting forces

significantly, but takes time to set up. OTP includes desk-mounted stations that have larger, more robust directional antennas.

On-The-Move describes the mode of operation where the antenna mounted to a vehicle and is fixed to the TACSAT radio at all times. This has the advantage of being permanently available to receive or transmit, but the antennas are omnidirectional and do little to boost signal strength in difficult areas.

Manpack describes the mode of operation where the TACSAT is used in a field pack if units are dismounted from vehicles. It has an autonomous power supply by 2 rechargeable batteries in a battery box.

Due to the extended range at which TACSAT communications can be intercepted, ISAF encrypts all of its TACSAT channels to CONFIDENTIAL. Timings for crypto changes can be found by contacting the Crypto Custodian or looking in Special Instructions (SPINs) and the Electronic Key Management Record. The type of encryption device and associated keymat used is determined by the bandwidth of the channel to be encrypted or the mission supported by the network:

- NB[15]: ISAF NB channels can only be encrypted using the Advanced Narrow band Digital Voice Terminal (ANDVT) series of COMSEC;
- WB[16]: ISAF WB channels can only be encrypted using the crypto key VINSON series of COMSEC;
- SOCCE (Special Operations Command and Control Element): SOCCE networks utilize a different encryption keys;
- DAMA[17]: DAMA channels additionally use orderwire encryptions;
- PERIODICITY: Keys currently have a weekly periodicity. Exact time can be found on Electronic Key Management Record.

The main formats for TACSAT channel access are the dedicated channel (DC) and the Demand Assigned Multiple Access (DAMA). The DC is assigned by the appropriate authority for a specific use. The DAMA channel is one that is assigned to users who do not need to use the channel constantly.

The TACSAT radio command nets will be used as the primary, and only all-informed, secure C2 channel between Regional Commands and their Task Forces and Maneuver Units. These channels provide a regional "Troops in Contact" (TIC) net, which permits regional response to SIGACTS[18] without dominating in the Common Operational Picture. Units requiring additional call signs or use of the net in support of operations will coordinate with the regional command TACSAT controller.

There are different types of TACSAT radio nets organized by proper purposes supporting ISAF command and control systems. The TACSAT net for Joint Terminal Attack Controllers (JTAC) for requesting Close Air Support (CAS) is allocated by the Joint Command Air Support Operations Center (ASOC). Another TACSAT net model is a secondary request net (SRN) and this is for back-up to JTAC nets. It is a controlled net which provides secure voice communications for CAS support to ISAF forces. A controlled net means that it is intended for authorized users and authorized purposes only. Unauthorized use may result in a denial of further net usage or possible punitive action. The Special Operations Forces (SOF) Command

[15] Narrow Band (NB). NB channel is 5 KHz wide. This is adequate for voice communications, but may be more difficult to maintain whilst moving. This provides efficient use of scarce satellite bandwidth.

[16] Wideband (WB). WB channel is 25 KHz wide. This is better for data communications and provides better voice communications, but reduces the overall number of channels that can be allocated.

[17] DAMA: Demand Assigned Multiple Access

[18] SIGACT – Significant Actions

Nets support voice and data in order to enable operational Command and Control of SOF's in-theatre operations.

The TACSAT nets are always demand assigned and tailored for providing the best form of tactical and operational level of supporting the battle planning and executions.

SUPPORTING THE BOOTS IN GROUND OVER NORTHERN AFGHANISTAN

The ability to establish remote CIS points of presence (PoP) provides additional operational flexibility to ISAF forces. A PoP can be established by use of a mobile communications package tailored to meet operational requirements. A mobile asset based on mission requirements and may be consisted by the following systems [12]:

- DEU[19] nanoPoP;
- DEU microPoP;
- NATO MiniPoP, ISAF Mobile Communications Detachment (IMCD), Very Small Aperture Terminal (VSAT), Dual Band Auto Pointing Rapid Deployable Terminal (DART), Bi-Band Suitcase Satellite Terminal (BBSST) and/or Deployable Satellite Ground Terminal (DSGT).

The miniPoP system is not a deployable system so this is for stabile operational environments. The following system descriptions are going to be covering the deployable CIS (TACSAT) assets. The provision of mobile PoPs will allow Coalition Forces to expand the ISAF Secret Core Network across ISAF, thereby enabling respective troops the ability to join the ISAF Command and Control architecture.

The nanoPoP sytem is a simple, manpack satellite system using the BGAN[20] channels connected to laptop computer for the deployed forces' communications support (Figure 03).

3. figure. NanoPoP satellite system in operation [13]

The nanoPoP system provides one (1) ISAF SECRET (mission secret) BGAN communications channel with an approximately 20 kg weight that is eligible for a dismounted soldier to hold, install, operate and maintain the system by her/his own.

The microPoP provides a bandwidth of 512 kbit/s, 2x VoSIP[21], 6x ISAF SECRET workstations, 6x headsets, 2x NATO unclassified workstations, 1x USB[22] cameras, 1x ISAF SECRET network printer. The microPoP is deployed with a Receive Broadcast Management (RBM) satellite communications (SatCom) terminal. The microPoP is a self sustainable system, containing heating and cooling units. The overall weight of all equipment will be approximately 800 kg; a total of boxes must be booked as cargo, along with two passengers.

[19] DEU - Deutschland

[20] BGAN – Broadband Global Area Network: global satellite network with portable terminals for voice and data services. The terminals connect to a laptop computer, the line-of-sight to the satellite is necessary. Downlink/uplink speeds of BGAN terminals are up to 492 kbit/s.

[21] VoSIP – Voice over Secret Internet Protocol

[22] USB – Universal Serial Bus

Additional capacity of transporting is required if a mobile power generator is necessary. The Figure 04 shows the built-up of microPoP system.

4. figure. MicroPoP system built-up [14]

The configuration consists of as follows:

- Receive Broadcast Management terminal (RBM);
- Heating/Cooling;
- Black System;
- Red System;
- 6x Equipment-Boxes;
- 1x ISAF SECRET printer;
- 6x ISAF SECRET laptops;
- 2x NATO unclassified laptops;
- 2x Voice over SECRET IP (VoSIP) phones;
- 1x USB-Camera;
- Lightning protection.

Regarding to physical space, the environmentally controlled space must be allocated for red (classified systems) and black (unclassified systems) equipment with a minimum of 1 meter separation. The area around the proposed deployment site, including the transport box, network equipment and generator must be fenced with minimum 3x wire corridor and lockable door. The black side and red side will consist of transport boxes one for black side, and one for red side, containing a switch, TCE[23] 621B and UPS[24]. The satellite terminal must have an unobstructed view of a proper, approximately 200 degree azimuth and approximately 40 degree[25] elevation. A completely leveled elevated 3m square is required for the terminal footprint to prevent submersion during rain or other austere weather. Suitable location to install earth-point/grounding is required. The 1.2m satellite dish can provide 2Mb/s data channel bandwidth that allow the users to simultaneously use the 6x laptop computers and download and upload voice and data IP packets via satellite in Ku-band.

The MicroPoP system is not a stationery solution however it offers a great opportunity to join the ISAF SECRET cloud without any service reductions or loss. The VSAT connectivity provides wideband and narrowband connection to ISAF stationer systems and workstations and can provide connectivity to other Afghan Mission Network (AMN) systems.

[23] TCE – Telecommunications Cryptoized Equipment
[24] UPS - Uninterruptible Power Supply
[25] The azimuth and the elevation are valid in mid-Asia (per.es in Afghanistan, Pakistan) only. It is belongs to the system geographical installation.

ASSESSMENT AND DEDUCTIONS

In regards of service orientation at the ISAF tactical and operational headquarters levels, standard procedures of command and control are generally known throughout the commands, the commanders are effective with the deliberate planning process. Commanders plan, direct, and synchronize operations supported by communications while maintaining command and control of their subordinate elements with limited or no assistance. Development at the company level and delegation by commanders are areas of improvement, to include integrating company and platoon leaders into decision making, planning, and battle tracking operations. Maintenance and resource procurement is another area that needs improvement. This lack of visibility and understanding on sustainment threatens the ISAF progress and severely limits further ISAF advancement.

The usage of tactical satellite system has several benefits in the operational area which are not changeable to ground-ground or ground-air-ground radio connections. Providing seamless tactical satellite channels in tactical and operational level gives the commanders broaden moving possibilities between areas of responsibilities. The man-hold tactical satellite systems facilitate the sustaining processes of ISAF forces in the time of ISAF restructuring and provide positive inputs to commanders.

SUMMARY

The ISAF as a whole has made progress, although communications standards and quality are not uniform across the formations. There is still work to be done in the development and implementation of enduring and sustainable systems. At the operational level, ISAF IJC is partnering with the Afghan National Security Forces which includes advising and mentoring on systems, planning efforts and orders development, to include the seasonal orders. The ANSF continues to make progress in integrating staff functions into the Military Decision Making Process (MDMP).

Cross-pillar command and control continues to be reactive and requires concerted effort from advisors and ANSF leadership at all levels. However, advisory effort and ANSF leaders have demonstrated moments of improved capability. Although this cross-pillar coordination is encouraging, the complex plan to secure this vulnerable event is a long way from complete and will require intense advisor support until event execution. Because of the direction, planning, coordination, and synchronization across the entirety of the ISAF and the Afghan government, it should recognize and take note of this operation as a significant step in ISAF and ANSF command and control capacity. Although enemy contact was limited in the year of 2013, ISAF and ANSF leaders were able to successfully synchronize the CIS installations and maneuvers of this large force [15].

Enable seamless and updated CIS connectivity in time of redeployment and ISAF reductions, this is the primary effort of ISAF commanders in field. Support command and control by using TACSAT equipment is one of the most important challenge of the international community. The ISAF and the German Armed Forces' answer for those challenges is the Point of Presence's system applications. This is a successful development and need to be improved. Increasing the usage of those CIS devices give the user possibility to spare time for their basic job in time of reduction (troops and equipment, devices and vehicles). After the last phase of redeploying has been finished, the PoP-elements can be eligible for NATO forces in other hot-spot/battle-area of the Globe.

Rererences

[1] http://www.isaf.nato.int/mission.html Letöltés ideje: 2013. július 05. 14:42

[2] United Nations Security Council doc S/RES/2093 (2013) 19 March 2013 pp. 4-5. In: http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/2096(2013) Letöltés ideje: 2013 július 03. 15:10

[3] Tarn D. Warren: ISAF and Afghanistan In: NDU press, 4th Quarter Issue 59 pp. 46-49. http://www.ndu.edu/press/lib/images/jfq-59/JFQ59_45-51_Warren.pdf Letöltés ideje: 2013 július 06. 15:22

[4] Conference report, NATO Defense College Rome September 2012, NATO mission in Afghanistan post-2014: The transformation decade, pp. 3-5. In: http://securitymanagementinitiative.org/files/NATO%20CR_sep2012.pdf Letöltés ideje: 2013 július 01. 19:22

[5] R. Beljan: Afghanistan: Lessons learned from an ISAF perspective, Small Walls Journal, 30 May 2013, In: http://smallwarsjournal.com/jrnl/art/afghanistan-lessons-learned-from-an-isaf-perspective Letöltés ideje: 2013 június 26. 00:22

[6] SHAPE edition: Security Force Assistance Advisor Team Concept of operations 23 February 2012 pp. 4-6.

[7] A.H.Cordesman- A.A.Burke: Transition in the Afghanistan-Pakistan war: How does this war end, 11 July 2012, pp. 94-100 In: http://csis.org/files/publication/120111_Afghanistan_Aspen_Paper.pdf Letöltés ideje: 2013 június 22. 04:29

[8] http://www.nato.int/isaf/docu/epub/pdf/placemat.pdf Letöltés ideje: 2013. július 02. 11:32

[9] COMISAF Advisory Assistance Team: ISAF Security Force Assistance Guide pp. 195-196.

[10] STANAG 5048 C3 (edition 5) The minimum scale of connectivity for communications and information systems for NATO land forces, 16 February 2000. pp. 2-6.

[11] STANAG 4637 (edition 1) Tactical Communications (TACOMs) phase 1. 18 June 2010. pp. 16-22.

[12] Conrad Flachsbarth: Nächster Baustein für das Afghanistan Mission Network einsatzbereit, Hardthöhen Kurier Online In: http://www.hardthoehenkurier.de/index.php/component/content/article/115-beitraege/magazin-news/869-naechster-baustein-fuer-das-afghanistan-mission-network-einsatzbereit Letöltés ideje: 2013. július 08. 05:09

[13] G. Leonhardt: Einsatzführungskommando der Bundeswehr, slide No. 13. In: http://www.afcea.de/fileadmin/downloads/downloads_red/2_Vortrag_Leonhardt.pdf.pdf Letöltés ideje: 2013. július 08. 09:59

[14] G. Leonhardt: Einsatzführungskommando der Bundeswehr, slide No. 12. In: http://www.afcea.de/fileadmin/downloads/downloads_red/2_Vortrag_Leonhardt.pdf.pdf Letöltés ideje: 2013. július 08. 09:59

[15] Report on Progress Toward Security and Stability in Afghanistan, US Department of Defense, December 2012 pp. 45-49 In: http://www.defense.gov/news/1230_Report_final.pdf Letöltés ideje: 2013. július 08. 23:12

Abreviations

KEY TERM	DEFINITION
ABP	Afghan Border Police
ALP	Afghan Local Police
ANA	Afghan National Army
ANCOP	Afghan Civil Order Police
ANP	Afghan National Police
ANSF	Afghan National Security Forces
AUP	Afghan Uniform Police
BDE	Brigade
BN	Battalion
CASEVAC	Casualty evacuation
CIS	Communication and Information Systems
C-IED	Counter - improvise explosive devices
CIMIC	Civil-military cooperations
COM	Commander
COP	Combat Observation Post
COY	Company
CT	Combined Team
CT-N	Combined Team North
EOD	Explosive ordnance detachment
GIRoA	Government of the Islamic Republic of Afghanistan
GOV/DEV	Governance and Development
HQ	Headquarters
IC	International Community
IJC	ISAF Joint Command
INFOOPS	Information operations
ISAF	International Security Assistance Force
HHC	Headquarters – headquarters cell
KDK	Kandak, Afghan Term for Battalion
MEDEVAC	Medical Evacuation
NGO	Non Governmental Organization
NTM-A	NATO Training Mission Afghanistan
PA	Public Affairs
RC N	Regional Command North
RMTC	Regional Military Training Command
OCC-P/R	Operational coordination center province/region
OM	Office module
OTP	On-the-pause
OTM	On-the-move
TACSAT	Tactical satellite
TCN	Troop Contributing Nation
UIP	Unified Implementation Plan
USFOR-A	US Forces Afghanistan

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Kovács Zoltán
zkovacs@nbsz.gov.hu

„ELECTRONIC WRITTEN TASKING ORDER SYSTEM" ACCOMPLISHED WITHIN THE PROJECT „SECURE ELECTRONIC COMMUNICATION" I.

Abstract

The "Comprehensive Programme for Integrated Governmental Functions" includes such relevant national security developments as the project named "Secure Electronic Communication" initiated by the Special Service for National Security (SSNS). The so called "Electronic Written Tasking Order System" was accomplished within the framework of this project. The main objective of this system is to convey the written tasking orders sent to SSNS via secure electronic communication lines decreasing the quantity of the paper based data carriers, which results rapid fulfilment of the requests of the tasking organizations, as well as it creates opportunities to carry out several related procedures in electronic form. This article series describe the designation of the Electronic Written Tasking Order System through the activities of SSNS proving that this system is a cloud system in terms of the tasking organizations.

Az „Integrált kormányzati funkciók átfogó program" olyan nemzetbiztonságilag fontos fejlesztéseket is tartalmaz, mint például a Nemzetbiztonsági Szakszolgálat által kezdeményezett „Biztonságos elektronikus összeköttetés" tárgyú projekt. Ennek keretén belül került sor az un. elektronikus Szolgálati Jegy Rendszer megvalósítására, amelynek fő célja a szolgálathoz beérkező megrendelések biztonságos elektronikus úton történő továbbítása, ezáltal a papír alapú adathordozók számának jelentős csökkentése és a megrendelői igények mihamarabbi kiszolgálása, valamint bizonyos kapcsolódó ügymenetek elektronikus alapokra helyezésének megteremtése. A cikksorozat a Nemzetbiztonsági Szakszolgálat feladatain keresztül bemutatja az elektronikus Szolgálati Jegy Rendszer rendeltetését, majd bizonyítja, hogy az a megrendelők szempontjából felhő alapú rendszernek tekinthető.

Keywords: *electronic tasking order system, cloud computing, cloud security, critical information infrastructure ~ elektronikus Szolgálati Jegy Rendszer, felhő alapú rendszerek, felhő alapú rendszerek biztonsága, kritikus információs infrastruktúra*

INTRODUCTION

The following paragraph can be read in a study published in 2010, entitled: "Computer Network Operations: Threats and Possible Defence Solutions in Hungary"

"The "Comprehensive Programme for Integrated Governmental Functions" includes such important issues related to economy and national security that we cannot disregard. By means of the "Central Management System" the whole budget system of Hungary will become transparent, therefore misuse of data gained from this system might influence the whole economy of Hungary. Thus the protection of this system is a high priority. The "Taxpayer-centric data service model" sets up Data Warehouses, here the priority is to maintain tax secrecy. The "Secure Electronic Communication" affects the processes of the Special Service for National Security. Although this is one of the most interesting tasks, its technology is not known to the public. The budget of the whole programme is 13881 million Forints." [1]

If the author of this part of the study, Csaba Krasznay regarded the project named "Secure Electronic Communication" as one of the most interesting issues, it is worth examining what it means. Certainly, only those parts can be published which do not contain classified information, even though the principle of the above mentioned project can be known, with some other important pieces of information which can be necessary for the planning of other systems.

The first article of this series of articles reviews the designation of Electronic Written Tasking Order System (eWTOS) accomplished within the framework of the so-called "Secure Electronic Communication" project, and in accordance with the tasks of the Special Service for National Security (SSNS), the procedure of the orders, and then examines how the eWTOS can be applied in the IT strategy of the Ministry of Interior. The second article analyses a currently important issue proving that the eWTOS can be regarded as cloud computing in terms of the tasking organizations that send written tasking orders to the SSNS. Concerning this it groups the cloud computing along with their features and classifies the eWTOS in the appropriate category. The third article discusses the security issues of the cloud computing by analysing to what extent it concerns the eWTOS as well as how the security panels prevail during their accomplishment. Finally two conclusions are drawn. On the one hand, even though the eWTOS has not been qualified as a critical information infrastructure yet, as every condition is given it is only a question of time. On the other hand, thanks to the already evolved high level security panels, the system is protected properly, thus after the classification these do not have to be modified in merits.

The series of articles concentrate on – primarily security – solutions considered during the planning. These articles do not aim to analyse the technical or other problems which appeared during the implementation or to describe different mistakes and their handling. They will only be mentioned if it is necessary to explicate the previously mentioned issues.

THE DESIGNATION OF EWTOS

In order to understand the purpose and the functions of eWTOS, first we should clarify the tasks and the procedure of the services requested from the Special Service for National Security.

Responsibilities and Activities of the Special Service for National Security

Act No. CXXV of 1995. [2] entered into force in 1996 and the SSNS was separated from the National Security Office and it was established as an independent organization with special technical and operational capacities.

SSNS is a governmental agency with nationwide authority, which functions as an independent budgetary organization, however, it is not a traditional national secret service. According to the Act No. CXXV of 1995 it provides the special means and methods of covert information gathering and acquisition of data, but does not have independent intelligence, counterintelligence or investigative powers (except cases concerning the internal security). It uses special means and methods in order to carry out the requests of other organisations authorised by law to initiate and perform covert information gathering (tasking organisations).

After the multiple conversions of the tasking organization structure, currently the SSNS provides special means and methods of information gathering for the reconnaissance and investigative tasks for eight organizations:

- Constitution Protection Office
- Information Office
- Military National Security Service
- Counter Terrorism Centre
- National Police
- Service for Protection of Law Enforcement Agencies
- National Tax and Customs Administration of Hungary
- Prosecution Service of Hungary

With its criminal investigation supporting task-system the activities of SSNS goes beyond the sphere of national security, what is more, supporting these tasks, though indirectly, it is concerned in the execution of cases related to cross border criminal investigation tasks (e.g. organized crime, illegal migration) as well. The SSNS with its capacities of special means and methods has always had a great role in the reconnaissance of serious crimes and events occurring in Hungary emphasized from national security aspect.

So the basic function of SSNS is to provide operational and technical background for information gathering, acquisition of data, as well as expert services for organizations authorized by law with its special technical background and well trained personnel– within the framework of law. It should also be emphasized that the capacities of SSNS do not substitute the traditional national security and investigative work, but significantly increase the effectiveness of those activities.

The concentration of the capacities of information gathering and acquisition of data at the SSNS has professional and economic advantages, as well as provides legal guarantee.

Economic advantages:

- the budget sources are not fragmented,
- the responsibilities and the expenses related to the operation, maintenance and development are concentrated at one organization, the SSNS,
- all of the tasking organizations gain the advantages of the development.

Professional advantages:

- concentrated development adapted to the requests of the tasking organizations,
- nationwide coverage,
- non-stop availability, reacting to the requests immediately, meeting the requirements of the tasking organisations
- coordination ability in case of authority conflicts,
- the elimination of the danger of disclosure caused by equipment applications realized through different principles.

Legal guarantees:

- SSNS cannot dispose with the information gained, it is deleted from its records without reproduction,
- there is no opportunity for "stocking" data acquisition,
- the separation of the tasking organizations and executors strengthens the social trust,
- as an independent service organization the application of special means and methods differing from the content of the external authorization in another way than described in the authorisation is not permitted.

The SSNS – in accordance with the rules of law - has exclusive powers related to those segments of special means and methods of covert information gathering and acquisition of data subject to external authorization where the developing of complex, technical systems requiring significant financial investments, special skills and experience, as well as the existence of human resources possessing special skills (such as off-air intercept, postal censorship) are required. On the other hand, SSNS plays a major role in other fields, for example wiretapping, radio monitoring, physical surveillance and background check.

The Special Service for National Security runs an Institute for Expert Services, which is primarily responsible for providing expert opinions in the field of handwriting, linguistics, audio, photo-video, IT, document forgery and explosives. It also performs regulatory, authoritative, and expert functions. It defines the security specifications for and regulates and supervises the production of the so called security documents. SSNS plays a similar role in the field of securities (shares, stocks, bonds) and authorizes their issuance and controls their production.

The SSNS provides combined application of several services (complex execution) for the tasking organizations, thus with the exploitation of synergy the efficiency can be increased significantly.

In order to protect the personal data and the special means and methods of covert information gathering, all data obtained in the course of covert information gathering is transmitted to the tasking organizations in a documented form and then in accordance with the rules of law they are deleted from its record. The SSNS keeps a record including:

- the request of the tasking organization with the necessary authorization,
- the personal data required for the identification of the person named in the request,
- the description of the special means and methods applied in the given case, and
- the list of data carriers transmitted to the tasking organization.

The Procedure of Written Tasking Orders

The tasking organization is responsible for obtaining the external authorization or for the issuance of the internal authorization and for the legality of such authorizations. SSNS is responsible for the competent application of the means and methods of covert information gathering and acquisition of data.

The special means and methods of information gathering can be required from the SSNS in written form on unified written requests signed by leaders of high rank whose positions are defined by cooperation agreements. The services of SSNS, where unified written tasking orders are not adapted can be requested through written requests in letter form. The tasking order requesting the application of the special means and methods of information gathering subject to external authorization must be attached to an authorization signed by the Minister of Public Administration and Justice or a designated judge. In case of private requests the description of the task must also be attached.

The procedure of written tasking orders of covert information gathering requiring authorization by the designated judge or the Minister of Public Administration and Justice is shown in Figure 1.

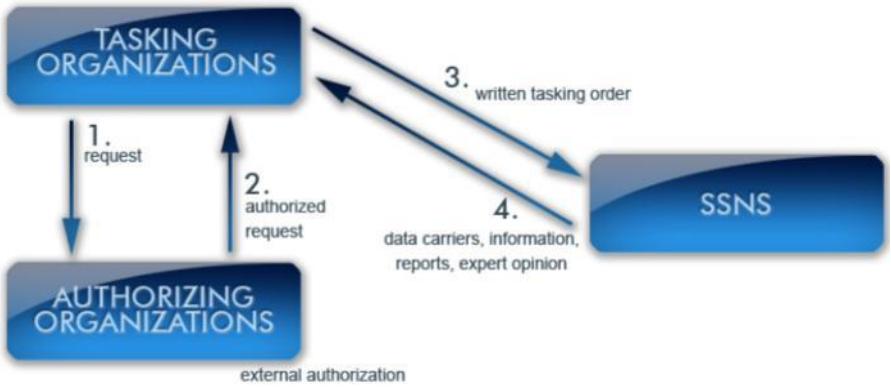


Figure 1. The Procedure of Written Tasking Orders
Source: http://www.nbsz.gov.hu/main.php?l=hu&p=1&a=7, (downloaded: 16/03/13)

From 2006 approximately 70,000 orders are obtained from the tasking organizations annually, which means 250, 000 sheets of paper with the supplementary documents every year.

The Functions of eWTOS and the Milestones of its History

The idea of Electronic Written Tasking Order System – i.e. fast and safe transmission of the written tasking orders and the supplementary documents to the SSNS – was the idea of the IT experts of SSNS in 2005. The SSNS negotiated about the main details and the previous cost estimates with the Ministry of Interior that year and with the other tasking organizations the following year. The project was first set in the action plan of National Development Agency (NDA) in Electronic Administration Operational Programme (EAOP) 2007-2008, and then based on the government decree 2142/2007. (VII.27.) [3] as an emphasized project in the 2007-2008 action plan under the title "The Structuring of Secure Electronic Communication". The tender was submitted at the end of 2007 and in the spring of 2008 the Grant Agreement was signed with the NDA.

What caused great changes in the project was the Act No. CLV of 2009 on the protection of classified information (PoCI) [4] accepted by the parliament on 14 December 2009. It fundamentally changed the classification of data, the handling of the classified data, the authorization of systems for handling and the regulations regarding the physical environment.

After the reconsideration of the project two important decisions were made. Firstly, the system will allow the handling of maximum Confidential! level documents instead of TOP SECRET!. This decision results that the documents classified above the level Confidential! will still be obtained in paper form, in exchange the costs of evolving a system suitable for TOP SECRET! level regulations (e.g. reconstruction of buildings) decreased significantly. According to the frames given by the PoCI the amount of documents classified maximum Confidential! will expectedly cover more than 85% of the written tasking orders and other

supplementary documents, thus an absolutely acceptable and rational decision was made. The other important decision was that the deadline of the project and the launching of eWTOS were amended to 31 December 2011 which was necessary to perform the new requirement and authorization system defined in PoCI.

In the summer of 2011 a final decision was made which determined that the document handling system of the eWTOS will be the so called "RoboCop" (RC). The background of this decision is the unification of document handling systems used in the bodies of the Ministry of Interior. The adjustment of RC to the eWTOS, the difficulties about the new encryption equipment (debuting in eWTOS), and the other issues which occurred related to reconstruction of the buildings – because of PoCI – and further technical reasons held back the launching of the eWTOS.

Because of the reasons mentioned above the deadline of the Grant Agreement was modified several times after signing in 2008, finally the system has been operating since 1 January 2013.

The function of the Electronic Written Tasking Order System, which was created within the project called "The Building of Secure Electronic Communication" is to transmit (mostly classified) written tasking orders and other supplementary documents (e.g. authorizations) from the tasking organizations to the Special Service for National Security in a secure electronic way instead of paper form. This will result a decrease in the amount of paper-based data carriers (written tasking orders, authorizations) and thanks to the online connection a faster fulfilment of the requests of the tasking organizations. According to the commitments of the project this means that the time of obtainment of the necessary documents from the tasking organizations decreases from 42 hours to 3, the number of paper based documents decreases from 250,000 to 25,000.

The complete electronization currently is not possible because of three reasons. One is that after negotiating with the tasking organizations 157 online terminals were installed which do not cover all the organizations issuing written tasking orders. The second is that the eWTOS handles only Confidential! level documents, thus the documents of higher classification are still obtained in paper form. The third reason is that in case of breakdown or VIS MAJOR (e.g. online terminal outages) the written tasking orders can be obtained in paper form.

The eWTOS has additional advantages besides the commitments. As a result of the two-way connection the system enables the reports to be transmitted to the tasking organization in an electronic form, in a secure way, as well as to lay the relating procedures on electronic basis. This – besides the acceleration of the previously mentioned procedures – results further paper savings in the long run, which was not mentioned in the project.

The Structure of eWTOS

In the eWTOS three different parties are named as follows:

1. Tasking organizations:
   - the previously mentioned eight bodies.

2. Authorising Organizations:
   - Minister of Public Administration and Justice,
   - the judges designated by the Budapest Metropolitan Court Criminal Department Military Panel,
   - the judges designated by the chairman of Budapest Metropolitan Court,
   - Public Prosecutor.

3. Provider:
   – Special Service for National Security (SSNS).

The principle of operation of the eWTOS is shown in Figure 2.

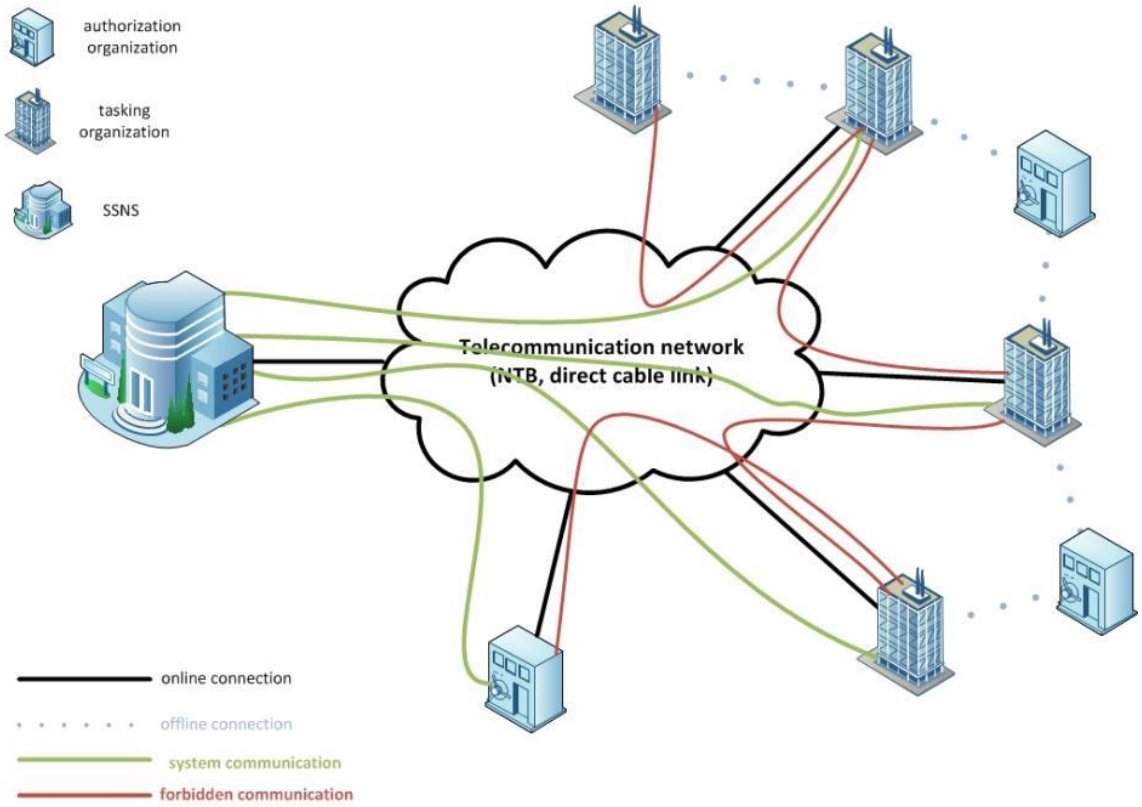


Figure 2. The Principle of eWTOS
Source: edited by the author

The figure shows that the tasking organizations are in connection with the devices installed at the SSNS. They send the written tasking orders here and receive the reports from here (Figure 1, Process 3 and 4). The system was constructed for a definite purpose, therefore the tasking organizations have no opportunity to share information different from the original purpose of the project. On the other hand, eWTOS provides the transmission of requests between the tasking organizations and authorising organizations (Figure 1, Process 1 and 2), but in this case the system installed at the SSNS works as an unavoidable quasi-mailbox. (Owing to the encryption and other guarantee elements everyone can only see their own documents, thus these documents are not available even to the personnel of the SSNS before the official transmission!)

The documents can be prepared and transmitted by means of the so-called online and offline terminals. The online work stations are connected to the SSNS centre through a telecommunication network (called National Telecommunication Backbone (NTB) or direct cable connection). In this case all the hardware devices are provided by the SSNS (except the SMART card necessary for the identification).

The structure of online terminals is shown in Figure 3.

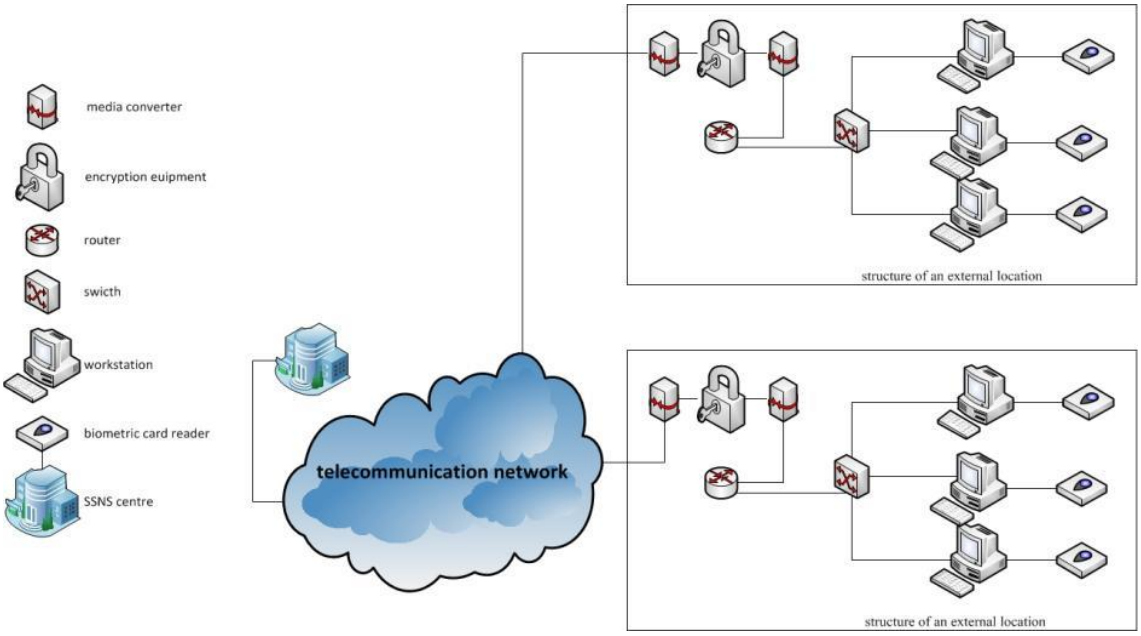


Figure 3. The Structure of Online Terminal
Source: edited by the author

In case of offline work stations the SSNS provides only an installation kit (since the application of eWTOS is bound to license). In this case the users utilize their own hardware infrastructure and card reader to make and send written tasking orders and other supplementary documents. However, these work stations are not in direct connection with the centre at SSNS. The documents made in offline work stations can be transmitted to the SSNS on data carriers (e.g. CD, flash drive) or through an online work station.

The offline clients can be installed to any suitable work stations, but the protection of classified information has to be provided to avoid unauthorized access and in case of transmission through the online work station it has to be compliant to other security regulations as well (e.g. authorisation of the use of flash drive based on unique identification).

For the operation and use of eWTOS the further devices (e.g. servers, other telecommunication devices etc.) are provided by the SSNS.

For the easier introduction and instruction the purpose of the developers was to replicate the paper-based processes known by the users in the best way possible However, certain changes in the process were unavoidable. These can be followed in the figure below (the workflow of paper-based process is shown in Figure 4, the electronic in Figure 5), where the position of the (system of) SSNS is the most remarkable in the chain.

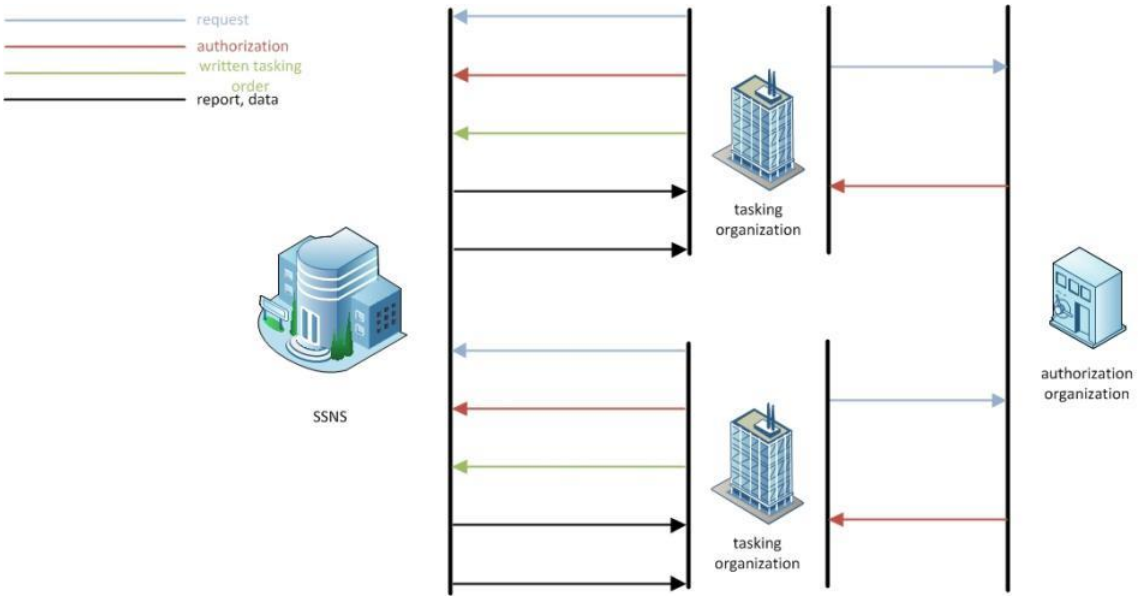


Figure 4. Workflow of Paper-based Process
Source: edited by the author

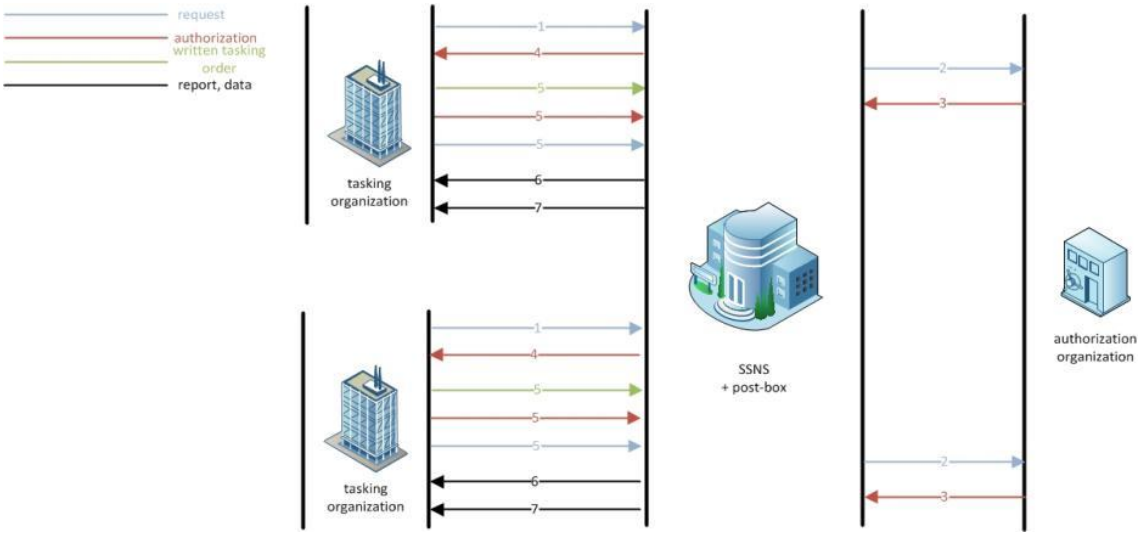


Figure 5. Workflow of Electronic-based Process
Source: edited by the author

However, this is not the only essential change resulted by the introduction of eWTOS. The main changes are as follows:

- the electronic files are transmitted,
- the electronic files are more detailed than the paper-based ones,
- the electronic files can only be opened with an application developed by the SSNS,
- the issuance and classification of documents are provided with a digital signature,
- the documents are certified digitally,
- the documents are classified digitally,
- The samples of handwriting signatures can be abolished,
- the handling of copies and appendices change,
- new documents are introduced.

The Adaptation of eWTOS in the IT Strategy of the Ministry of Interior

The idea of the eWTOS in 2005 was very promising as it suits to the IT strategy of the Ministry of Interior published in 2012(!). [5] As the decree includes the Ministry of Interior and its sectoral organizations, it covers the half of the tasking organizations of the SSNS (regarding the amount of the written tasking orders, this proportion is much higher).

Those parts will be highlighted below from the document mentioned above which justify the fit.

"III. Strategic methodology

2. The rolling wave planning

- The homogenization of IT systems on sectoral level is required in favour of cost-effectiveness, easier operation, and the use of knowledge base in the sector.
- The different levels of development and security should be approximated on sectoral level.
- Suitable for the legal frames, paper-free administration has to be evolved and the whole electronization of expert systems with customer service has to be evolved in favour of the establishment of an electronic, paper-free office [the introduction of RC NEO integrated management, case processing and electronic record management (hereinafter: RC NEO system)]
- The continuous increase in the level of IT security regulations and environment."

The terminals of eWTOS placed at the tasking organizations, the software on those terminals, document handling systems connected to it (in this case the RC), and the installed security devices (for handling of classified data, authorised encrypting devices and electronic systems, and the use of other security elements) are in the service of unification, approximation of development levels and strengthening and increasing security. The eWTOS itself will replace a part of paper-based processes, thus helping the development of a paper-free office.

The next step of this process is the expansion of RC document handling system on the side of the tasking organizations and SSNS, which will also make some parts of the process paper-free. Let us take a short digression into the future. About the development of RC the following issues can be found in the strategy:

"IV. Directions of Strategic Development

7. The Development of RoboCop System and the Implementation of RC Neo in the Sectors

...According to the directions of the Minister of 24 June 2011 a further development of RoboCop was prescribed on new technological basis within the frames of RoboCop NOVA project. In accordance with the decision, the RoboCop should be upgraded based on the current solutions so that it will be suitable for the claims of the new technology, legal background and the average professional standards in the long run preserving the outstanding values of the previous system. In addition, the purpose of the project is to define the regulations and standards which provide the unified technical, semantic, IT security, application development, methodological and project management and to control the environment providing the complete development, maintenance and operation of RoboCop. The realization and consistent enforcement of these purposes provide a guarantee for a RoboCop of excellent quality, based on firm technology and can be utilized in a modern user environment in the long run.

During the development the main objective is to emphasize the organizational and user requirements based on legal commitments, special sectoral expectations and operation more efficient than the market structure. The newly developed RoboCop – just like the current

system dependent on the intended targets - is needed to be audited in favor of the successful certification. A particular emphasis should be laid on the audit from the point of view of security…

"The interior sector develops RC, as a management and document processing system from its own resources which satisfies the professional claim in the short, medium and long run. The introduction of RC Neo in the sector was ordered by the Decree of 24/2011 (IX. 9.) of the Ministry of Interior on the regulation of the use of the integrated management and case processing system of RoboCop and on the introduction of unified electronic document management and the establishment of project organization supporting the implementation. After testing the system the management, the case processing and the electronic document management are allowed to be done according to the instructions."

So the RC will be the determinative document handling system in the Ministry of Interior and its sectoral organizations in the long run. After its upgrading the RoboCop along with eWTOS will be able to provide a secure, paper-free management between the SSNS and its (RC using) tasking organizations even in the entire process of the case (i.e. from the phases preceding the preparation of the written tasking orders to the activities after the process of the reports made at the Special Service for National Security).

In the eWTOS, as a system handling and transmitting classified data, the security issues have a highlighted role. In the IT strategy of the Ministry of Interior the following statements can be found regarding the eWTOS:

"8. IT Security

Regarding the philosophy of the IT Security Policy of the Ministry of Interior, in the field of IT security sectoral level, centralized purposes have to be followed. To the harmonization of the IT security levels the purposes have to be performed are as follows:

...– For the protection of communication of non-public data among the Ministry of Interior and its sectors at least IPSec encryption has to be used. Stronger, higher-level protection can only be used in task orientated, justified cases. ...

...– The Ministry of Interior and its sectoral organizations… have to define the borders of their IT network, within which they have to provide all IT protection themselves. In order to guarantee the security of the data stored and transmitted in the network of the organization homogeneously solid network protection devices and defence procedures must be applied.…

...In favour of the protection of the IT network of the Ministry of Interior and its sectoral organizations ... keeping a record of the access to the IT network, ... as well as the logging of the printing process.

In the Ministry of Interior and its sectoral organizations the following IT security conditions have to be established in favour of protecting non-public information:

– The use of not registered mobile data store devices without unique identification has to be abolished. ...

– All documents in the electronic document handling procedure must be provided with digital signature and timestamp by their issuers until 31 December 2014."

As the eWTOS is a system transmitting classified information the transmission of data require authorised national encrypting devices. The access and the protection of data stored and transmitted in the system are guaranteed by a multiple level protection, authorised devices and sites. The access processes and the printing are provided with high level protection, and completely logged. Only previously registered devices with unique identification can be connected, the events are completely logged in this case as well.

The eWTOS is already accomplishing the security element (the provision of the document with digital signature and timestamp) described in Chapter 8 in the IT strategy of the Ministry of Interior, which is not provided by any other IT systems of the Ministry of Interior, only mentioned as a medium term goal.

Finally, regarding encryption the strategy aims at the following purposes, which are accomplished by the eWTOS as well.

"9. Encryption

The Act No. CLV. of 2009 on the protection of classified information re-regulated all the aspects of the handling of national classified data with the attendance in international communities in Hungary. The purpose of the strategy of the Ministry of Interior on sectoral levels is: ...

– The establishment of uniformly high level encryption equipment parks.

– The execution of the transmission of classified data in a unified network."

CONCLUSIONS

As a conclusion it can be ascertained, that eWTOS outrivalled its time when it was invented. The basic conception was the electronization of a part of a completely paper based process of written tasking orders sent to the SSNS. Apart from the fact that it was a daring, favourable idea, it also had other advantages. On the one hand, eWTOS did not want to electronize the complete process, only its most critical part in terms of investment. It aimed at the field, where the endpoint terminals were installed in more than one organization, the communication lines between these terminals were used in common, that is why it was complicated to share the expenses in a fair way. Moreover the accomplishment of this part of the process could accelerate the electronization of the entire procedure. On the other hand, the implementation of eWTOS in this form enabled the tasking organizations to accomplish their electronic document handling processes concerning eWTOS using methods and equipment they wish. In addition they could do it considering their financial circumstances and developing priorities. Thirdly eWTOS includes such technical solutions and functions today, which were described as strategic objectives in the IT strategy in the Ministry of Interior in 2012.

However, considering the development concepts, certain areas of concern emerge. The root of the problems is that the eWTOS tries to reflect paper-based workflow to the greatest possible extent.

Undoubtedly it has several benefits. It is an exact process having been improved over the years, known in details, the replication of which is feasible. The users are familiar with the complete process, so their training is easier compared to the introduction of a brand new system.

Besides, some disadvantages can also be seen. First is that the above mentioned paper-based process can not be replicated with100 % accuracy. The other issue is that the electronic document handling does not have as clear, widespread rules as the paper-based one. In

addition, in case of electronic based document handling, such problems emerge that do not occur concerning paper based document handling, for example the missing of classified information caused by crash of terminal which can violate the principle of availability. [4]

Besides the above mentioned problems, it can be stated, that these are not the peculiarities of eWTOS, but they might occur in any electronic document handling systems. What has been said above it is clear that eWTOS is progressive not only in its solutions, but it also raises issues that might arise at other organizations in several years' time.

The future of eWTOS will probably be similar to that of other, greatly innovative ideas. After the launching of the system, it will change, will be refined according to the users' experience, while lacking or not completely existing legal regulations will be made, formed and the existing ones will also be modified based on experience.

References

[1] Kovács László (szerk.): Számítógép-hálózati hadviselés: Veszélyek és a védelem lehetséges megoldásai Magyarországon. Tanulmány. Budapest, 2010 Zrínyi Miklós Nemzetvédelmi Egyetem p. 56.

[2] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=99500125.TV – (2013.03.21.)

[3] A Kormány 2142/2007. (VII. 27.) Korm. határozata az Új Magyarország Fejlesztési Terv Környezet és Energia Operatív Programja, Elektronikus Közigazgatás Operatív Programja, az Államreform Operatív Programja, Társadalmi Megújulás Operatív Programja, a Társadalmi Infrastruktúra Operatív Programja, valamint a Regionális Operatív Programok 2007-2008. évekre vonatkozó Akcióterveinek jóváhagyásáról - Határozatok Tára 36. szám 2007. július 27. p. 263 - 277 http://www.kozlonyok.hu/kozlonyok/Kozlonyok/10/PDF/2007/36.pdf – (2013.03.21.)

[4] 2009. évi CLV. törvény a minősített adat védelméről http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0900155.TV – (2013.03.21.)

[5] 12/2012. (III. 22.) BM utasítás a Belügyminisztérium Informatikai Stratégiájáról. Hivatalos Értesítő, A Magyar Közlöny melléklete 13. szám 2012. március 22. p. 1626 - 1643 http://www.kozlonyok.hu/kozlonyok/Kozlonyok/12/PDF/2012/13.pdf – (2013.03.21.)

Figures

[6] Figure 1. The Procedure of Written Tasking Orders
Source: http://www.nbsz.gov.hu/main.php?l=hu&p=1&a=7 – (2013.03.16.)

[7] Figure 2. The Principle of eWTOS
Source: edited by the author

[8] Figure 3. The Structure of Online Terminal
Source: edited by the author

[9] Figure 4. Workflow of Paper-based Process
Source: edited by the author

[10] Figure 5. Workflow of Electronic-based Process
Source: edited by the author

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Kovács Zoltán
zkovacs@nbsz.gov.hu

FELHŐ ALAPÚ RENDSZEREK TÖRVÉNYES ELLENŐRZÉSI MÓDSZEREI VIZSGÁLATA I.

Absztrakt

Napjaink kommunikációs szokásait nagymértékben meghatározzák az Internetes kommunikációt biztosító felhő alapú rendszerek. 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 (pl. Facebook, Gmail, Dropbox, Twitter, Skype stb.) Ezen rendszerek törvényes ellenőrzésének igénye a felhasználás ütemével arányosan nő. A cikksorozat első része áttekinti az említett rendszerek törvényes ellenőrzésének kihívásait, majd publikus forrásokból elérhető információkra alapozva jellemző példákat mutat be külföldi nemzetbiztonsági szolgálatok és rendvédelmi szervek által használt módszerekre. A második rész megvizsgálja a törvényes ellenőrzéshez rendelkezésre álló technikai lehetőségeket, felállítja az ezek elemzéséhez szükséges szempontrendszert, majd az így kialakított szempontrendszer alapján elvégzi azok elemzését.

The habits of recent communication have been dramatically determined by cloud computing which ensures communication via Internet. 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 for free (e.g. Facebook, Gmail, Dropbox, Twitter, Skype, etc.). The requirement of lawful monitoring of these cloud computing systems has been growing proportionally to the growth of using. The first part of this article series is reviewing the problems appearing in lawful monitoring of cloud computing systems mentioned above, and then presenting representative lawful monitoring methods used by foreign national security services and law enforcement agencies based on public sources. The second part of this article series is analysing the possible technical solutions of lawful monitoring, setting up criteria which needed to analyse them, then doing the analysis of technical solutions by this criteria.

Kulcsszavak: *felhő alapú rendszerek, törvényes ellenőrzés, Skype ~ cloud computing, lawful monitoring, Skype*

BEVEZETÉS

A kommunikáció formái, lehetőségei az Internet és az azt kihasználó alkalmazások fejlődésével ugrásszerűen változnak, bővülnek. 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 (továbbiakban: PC/SaaS felhő alapú rendszerek). 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 PC/SaaS felhő alapú rendszerek törvényes ellenőrzésének igénye a felhasználás ütemével arányosan nő, hiszen a (potenciális) célszemélyi kör is ezt használja leginkább. A „Felhő alapú rendszerek törvényes ellenőrzési problémái" című cikk bemutatta az Internet és az azt felhasználó 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. Az összefoglalás és a következtetések részben a törvényes ellenőrzés hatékony kialakítása érdekében teendő továbblépéshez újabb elvégzendő feladatokat fogalmazott meg. Ezek közül az egyik a következő: *„… célszerű áttekinteni, összehasonlítani a törvényes ellenőrzésre jelenleg rendelkezésre álló technikai eszközöket és módszereket, azok előnyeivel, hátrányaival együtt."*. Jelen cikksorozat ezzel a foglalkozik részletesen.

A cikksorozat első része áttekinti a PC/SaaS felhő alapú rendszerek törvényes ellenőrzésének kihívásait, majd ezt követően publikus forrásokból elérhető információkra alapozva jellemző példákat mutat be külföldi nemzetbiztonsági szolgálatok és rendvédelmi szervek által használt módszerekre. A példák ismertetésénél főként a Skype-ot használja mintának. Egyrészt azért, mert ennek a rendszernek a lehallgatása minden országban megoldandó, de problémás feladatként jelentkezett, másrészt pedig azért, mert jól példázza, hogy egy új infokommunikációs rendszer törvényes ellenőrzése kapcsán a különböző országok képesek gyökeresen eltérő irányokba elindulni.

A második rész megvizsgálja a törvényes ellenőrzéshez rendelkezésre álló technikai lehetőségeket, majd felállítja az ezek elemzéséhez szükséges szempontrendszert. Az így kialakított szempontrendszer alapján elvégzi a felsorolt technikai megoldások elemzését, csoportosítva azok előnyeit, hátrányait. Végezetül a következtetések levonása után – illeszkedve a „Felhő alapú rendszerek törvényes ellenőrzési problémái" című cikk összegzésében leírtakhoz – további, a PC/SaaS felhő alapú rendszerek törvényes ellenőrzésének hatékony kialakítása érdekében végrehajtandó feladatokat fogalmaz meg.

A FELHŐ ALAPÚ RENDSZEREK TÖRVÉNYES ELLENŐRZÉSI KIHÍVÁSAI

A felhő alapú rendszerek törvényes ellenőrzése minden ország nemzetbiztonsági és rendvédelmi szervét kihívások elé állítja. Az elektronikus úton folytatott kommunikáció ma már jóval tágabb értelemben értelmezhető fogalom, mint a hagyományos hírközlés, hiszen lehetőségei, a kommunikációs formák száma messze meghaladják ez utóbbiét. Ennek következtében rengeteg olyan új rendszer, technológia jelent, jelenik meg, amelyek törvényes ellenőrzését az arra feljogosított szolgálatoknak meg kell, vagy legalábbis meg kellene oldani. Az új technológiák megjelenése mellett egy jól kivehető átalakulási folyamat is zajlik a hírközlés, vagy pontosabban fogalmazva az elektronikus úton folytatott kommunikáció

területén. 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 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 törvényes ellenőrzést végző szervezeteknek alapvetően az a feladata, célja, hogy a kijelölt célszemélyek kommunikációját lehetőség szerint teljes mértékben ellenőrizzék, függetlenül annak formájától, az általuk használt technológiától, eszközöktől, alkalmazásoktól. Az egyik legnagyobb feladat tehát, hogy pontosan meghatározzuk azt, hogy mit kell, mit célszerű ellenőrizni, majd ehhez ki kell alakítani a megfelelő technikai és jogszabályi környezetet.

Az elektronikus úton folytatott kommunikáció változásában nagy szerepük van a PC/SaaS felhő alapú rendszereknek, ahol is alkalmazásszolgáltatók biztosítják azokat a szolgáltatásokat, amelyeken keresztül – a lehető legkülönfélébb módon – elektronikus kommunikációt lehet folytatni. Ezen rendszerek törvényes ellenőrzésének megteremtése tehát kiemelt feladat az arra feljogosított szervek számára, ugyanakkor a feladat ellátását több probléma is nehezíti.

Az egyik probléma a jogi szabályozás hiányosságaiban keresendő. A rohamosan fejlődő technológiával, az ezen belül gyökeresen átalakuló kommunikációs módokkal, valamint az Internet szabadságával egyelőre nehezen birkózik meg a jogi világ. A hatályos jogszabályok nem, nem teljes mértékben vagy csak erős „beleértéssel” teszik lehetővé a PC/SaaS felhő alapú rendszerek ellenőrzését.

A másik problémát a technikai megoldások hiánya jelenti. Az új technológia új ellenőrző eszközöket kíván, kívánhat, ez pedig beruházást igényel. Sokszor azonban még nincsenek meg azok a technikai eszközök, amelyekkel az új technológiák törvényes ellenőrzését egyáltalán végre lehet hajtani. Ráadásul az eltérően felépített szolgáltatói infrastruktúrák miatt ez akár szolgáltatónként eltérő megoldásokat igényelhet, ami igen költséges.

A harmadik nagy problémát az okozza, hogy a hírközlés ellenőrzésnél régóta 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.

Az arra feljogosított szerveknek azonban addig is, amíg kialakul a mindenki által elfogadott, letisztult jogi környezet és az összes igényt kielégítő technikai háttér, a törvényes ellenőrzést – valamilyen formában – biztosítaniuk kell. Ehhez a korábban már kialakult kelléktárat és a hatályos jogszabályokat alapul véve próbálnak más és más megoldást alkalmazni. Még a fejlett demokráciával és ipari háttérrel rendelkező országok esetében is kiépítő, vagy nem is demokratikusnak tekintett országokról. Érdemes – a nyíltan elérhető anyagok alapján – megvizsgálni, hogy milyen módszerek állnak a titkos információgyűjtést végző szervezetek rendelkezésére, és azok alkalmazása során milyen buktatókba ütköztek. [1]

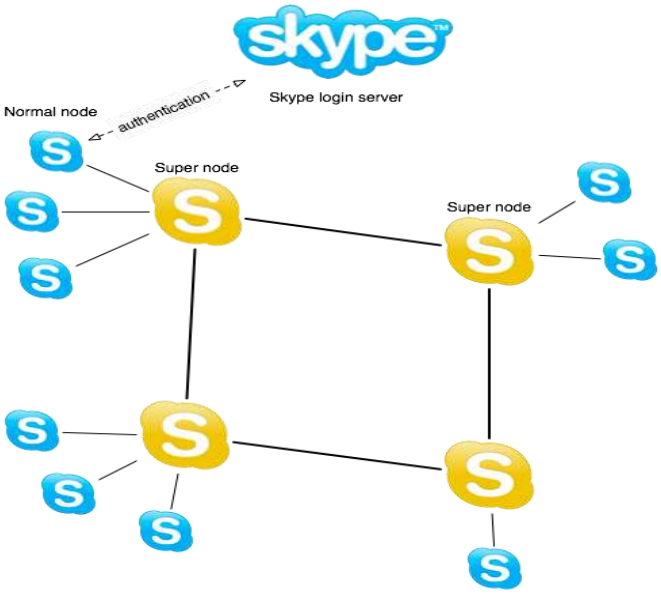
NEMZETKÖZI PÉLDÁK

Skype, mint „állatorvosi ló”:

A Skype esetét célszerű példaként, különállóan vizsgálni. Egyrészt azért, mert ennek a rendszernek a lehallgatása minden országban megoldandó, de problémás feladatként jelentkezett. Másrészt pedig azért, mert jól példázza, hogy egy új infokommunikációs rendszer törvényes ellenőrzése kapcsán még a fejlett demokráciával rendelkező országok is képesek gyökeresen eltérő irányokba elindulni, nem beszélve a demokráciát még éppen kiépítő, vagy nem is demokratikusnak tekintett országokat.

A rendkívül népszerű Skype első béta verziója 2003 augusztusában jelent meg, míg 2011-re átlagban 20 millió felhasználó használta egyidejűleg. [2] 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. [1] A Skype pedig szinte minden nemzetbiztonsági és bűnüldöző szerv prioritási listájának az élén áll.

Röviden érdemes áttekinteni, hogy mi is okozza a problémát ennek a rendszernek az ellenőrzése kapcsán. Az egyik maga a rendszer felépítése. (Ennek sematikus elrendezése az 1. ábrán látható.)



1. ábra. Skype topológiája
Forrás: http://crypto.stanford.edu/cs294s/projects/skype.html (letöltve: 2013.03.26.)

A működés leegyszerűsítve úgy történik, hogy a korábban már regisztrált felhasználó (a regisztrációhoz csupán egy érvényes email címre van szükség!) bejelentkezik felhasználói nevével a Skype központi szerverére, ahol a jelszava alapján megtörténik a hitelesítése. A hitelesített felhasználó lekérdezheti kontaktlistáját, felhasználó adatait, más felhasználókat kereshet stb. A tényleges kommunikáció közvetlen (a kommunikáló felek (Node) közvetlen összeköttetésben áll egymással), vagy közvetett (a kommunikáló felek Supernode-okon keresztül állnak összeköttetésben egymással) kapcsolaton keresztül zajlik, de nem folyik át egy központon. [3] [4] Éppen ezért már az egy felhasználóhoz tartozó kommunikáció elfogása

is – figyelembe véve a felhasználók mobil eszközökkel bárhonnan használhatják a szolgáltatást – rendkívül nehéz.

A másik problémát a felhasznált magas szintű titkosítás (RSA és AES-256) okozza. [5] Azaz, ha sikerül is „útközben" elfogni a kommunikációt, annak tényleges tartalmához csak a használt titkosítás visszafejtése után lehetséges hozzáférni. Az ehhez szükséges számítási kapacitás és időigény meglehetősen nagy, a tömeges méretű ellenőrzést ez meglehetősen megnehezíti, vagy inkább teljes mértékben kizárja.

További problémát okoz a korábban már említett regisztráció, amelyhez csupán egy érvényes email címre van szükség. Emiatt a törvényes ellenőrzés feladatrendszerébe beleértett – és hagyományos hírközlési szolgáltatók esetében hatékonyan alkalmazható – felhasználói/előfizetői adatok szolgáltatása [1] ebben az esetben nehézkesen és főleg hiányosan valósul meg.

A fentiek okán célszerű tehát – természetesen a publikusan elérhető információk korlátozott volta miatt – a teljesség igénye nélkül megvizsgálni, hogy melyik ország, hogyan ellenőrzi (vagy hogyan próbálja ellenőrizni) a Skype rendszert. Bár a példák elsősorban azt szolgálják, hogy az ellenőrzésre szolgáló elveket, technológiákat, valamint a használatuk kapcsán felmerült jogi, technikai problémákat áttekinthessük, emellett arra is megfelelnek, hogy analógiaként felhasználhatók legyenek majd más PC/SaaS felhő alapú rendszerek ellenőrzési kérdéseinek vizsgálatakor.

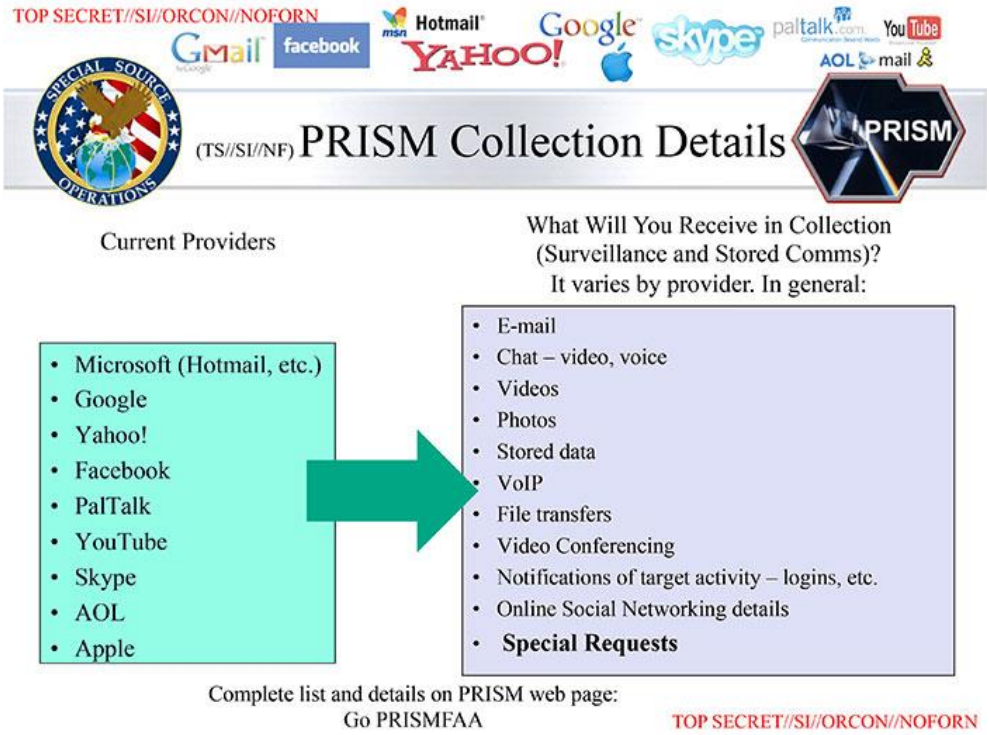
USA és a Skype:

A nyíltan elérhető források alapján arra lehet következtetni, hogy az USA a „Skype-probléma" megoldására a szolgáltatóval való együttműködést választotta. 2011 májusában már tényként könyvelték el, hogy a nagyhírű redmondi cég 8,5 Mrd USD-ért felvásárolta a Skype-ot.[6] Az ügyletet az Európai Unió versenyjogi végrehajtó szerve, az Európai Bizottság még az év októberében jóváhagyta, így elhárult minden akadály a fúzió elől. A felvásárlás már csak azért is „érdekes" volt, mert a Skype üzleti szempontból nem volt éppen sikertörténet. 2010-ben 7 millió dolláros nettó veszteséget könyvelhettek el amellett, hogy ugyanebben az évben december 31-én a társaság hosszú távú adósságállománya 686 millió dollár volt. [7]

A szaksajtóban már a felvásárlás bejelentésekor elindultak a találgatások, hogy miért is kell, kellhet a Skype a Microsoftnak. [8] [9] Az ott felvetetteken kívül nem kell túl nagy fantázia ahhoz, hogy az addig a titkosítás és a peer-to-peer struktúra miatt nagy nehézségekbe ütköző törvényes ellenőrzést is felírjuk a listára, alighanem az első helyre. Ennek megvalósítása az USA nemzetbiztonsági és bűnüldöző szervei számára ugyanis sokkal egyszerűbben kivitelezhető, ha egy egyesült államokbeli cég a tulajdonos, aki együttműködik az említett hatóságokkal, szervezetekkel. Ezt a feltételezést erősítik azok az információk is, hogy a felvásárlást követően a Microsoft megkezdte a Skype infrastruktúrájának átalakítását és egy központosítottabb hálózatot kezdett kiépíteni. A változás az addig rotációban a felhasználók között kiosztott un. Supernode-oknál indult el. Egyrészt számukat jelentősen csökkentették (több mint 48 ezerről kb. 10 ezerre), másrészt az új Supernode-ok már nem lehetnek felhasználók gépei, hanem csak és kizárólag a Microsoft/Skype központjába telepített eszközök. [10] Mára már az is bizonyított, hogy a Microsoft minden írott üzenethez hozzáfér, a továbbított üzenetekben pedig szűrést is végez. Ez a képesség pedig lehetőséget teremt arra is, hogy az üzenetek tartalmát hozzáférhetővé tegye a titkos információgyűjtésre feljogosított szervek számára. [11] [12] [13]

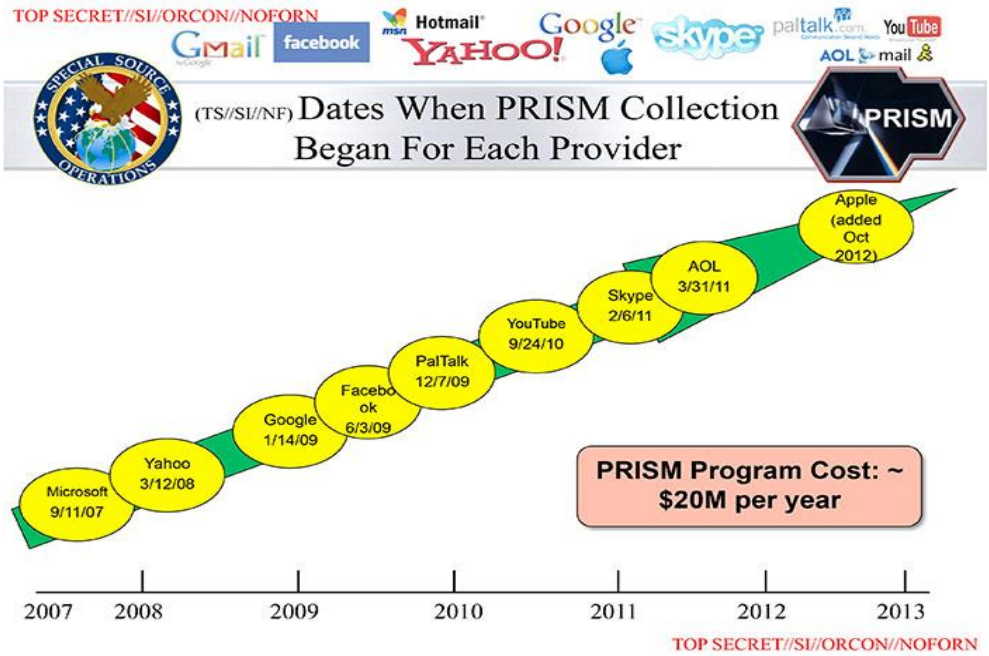
A Prism programról közzétett adatokból az is nyilvánosságra került, hogy a kilenc vezető internetes alkalmazás szolgáltató (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple) rendszerein tárolt és azokon átfolyó adatokhoz (pl. beszélgetések, video-chat, fényképek stb.) (2. ábra) – szolgáltatónként változó formában és mélységben – fér

hozzá az NSA (National Security Agency – Nemzetbiztonsági Ügynökség), az FBI (Federal Bureau of Investigation – Szövetségi Nyomozó Iroda) és az NSA-n keresztül az angol GCHQ (UK Government Communications Headquarters – Kormányzati Kommunikációs Központ). [14] A Skype-ot a kiszivárgott információk szerint 2011. 02. 06-án kapcsolták be a programba. (3. ábra.)



2. ábra. A Prism programban szereplő szolgáltatók és az általuk – különböző mértékben – biztosított adatok

Forrás: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (letöltve: 2013.07.02.)



3. ábra. A Prism programban résztvevő szolgáltatók és csatlakozásuk időpontja

Forrás: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (letöltve: 2013.07.02.)

Oroszország és a Skype:
Oroszország is a szolgáltatókkal történő együttműködést választotta, csak annak egy másik változatát. Az FSZB 2011-ben vetette fel, hogy be kellene tiltani a Skype, a Gmail és a Hotmail működését Oroszországban, mert azok ismeretlen algoritmusokat használnak a titkosításra, így ellenőrizhetetlen azok tartalma. Ez pedig biztonsági kockázatot jelent. [15] A Microsoft a felvásárlást követően bejelentette, hogy – a korábban más szoftvereinél alkalmazott gyakorlatának megfelelően – kész átadni a Skype forráskódját és titkosítási algoritmusát az orosz szolgálatnak, ezáltal elkerülheti annak betiltását. [16] [17] A lehallgatás, sőt a felhasználók pontos tartózkodási helyének meghatározási képességét orosz lapértesülésre hivatkozva a szaksajtó ma már tényként kezeli. [18]

Kína és a Skype:
A szolgáltatók Kínában is együttműködnek a törvényes ellenőrzést végző hatóságokkal. Az ázsiai országban a Skype egy speciális változatát használják, amelyet a – többségi tulajdonos – TOM Online (egy kínai Internet szolgáltató cég) és a Microsoft által alapított vegyesvállalat adott ki TOM-Skype néven. A szoftver feltörése után bizonyítottá vált, hogy kínai hatóságok ezen keresztül ellenőrzik a kommunikációt, az azonnali üzenetküldések esetében több ezer szavas szótár alapú kulcsszavas keresést használnak, és találat esetén rögzítik a teljes chatelést, vagy adott esetben blokkolják a forgalmat. [19]

Franciaország és a Skype:
Franciaország törvényi alapon kíván együttműködést elérni törvényes ellenőrzés tekintetében a Skype szolgáltatójával, mégpedig úgy, hogy hagyományos hírközlési szolgáltatónak kívánja minősíteni azt. Ennek megállapítása érdekében a francia hírközlési hatóság, az ARCEP beadvánnyal fordult az ügyészséghez. Amennyiben ez sikerül, akkor ugyanazok a kötelezettségek vonatkoznak a Skype szolgáltatójára is, mint a hagyományos hírközlési szolgáltatókra, azaz lehetőséget kell teremtenie a hálózatán keresztül a segélyhívó rendszerek elérésére, adót kell fizetnie a francia államnak, és – nem utolsó sorban – az arra feljogosított szervek számára biztosítania kell a törvényes ellenőrzést is. [20] [21]

Más példák:
Természetesen nem csak a Skype az, amit a hatóságok ellenőrizni kívánnak, és természetesen a fent említett módszerekkel nem csak a Skype, hanem más alkalmazásszolgáltatók rendszerein küldött és tárolt információk is ellenőrizhetők. A következő példákban is többnyire megjelenik a Skype ellenőrzése, de e mellett a más rendszerekből származó információk megszerzése a korábbiaknál sokkal hangsúlyosabban jelenik meg, így ezeket célszerű külön csoportban vizsgálni. Már csak azért is érdemes így tenni, mert a következő példák jól mutatatják, hogy egyrészt a szolgáltatóval való együttműködésen (vagy együttműködésre történő kényszerítésen) túl is vannak lehetőségek a titkos információgyűjtésre feljogosított szervezetek kezében, másrészt egy ország több ellenőrző módszert is használ (használhat).

Németország és az online házkutatás:
Németországból szivárgott ki a legtöbb információ a törvényes ellenőrzések során használt – és sok más névvel is illetett pl. kémprogramok, trójai programok – online házkutatásról. A módszer törvénybe iktatása, ezáltal a használat kereteinek kialakítása már régóta szerepelt a német parlament napirendjén. [22] Többszöri elutasítást [23] [24] követően a szövetségi alkotmánybíróság végül úgy foglalt állást, hogy a módszer használható, de szigorú keretek között (kizárólag kommunikáció ellenőrzésére – azaz gyakorlatilag az internetes telefon (pl. Skype) lehallgatására). Egy német hackercsoport a Chaos Computer Club (CCC) azonban

analizálta a német hatóságok által használt, a szintén német DigiTask által gyártott „maleware”-t, és megállapította, hogy annak képességei messze túlmutatnak a fent említett, szövetségi bíróság által megszabott kereteken. [25] [26]

Ezt követően a német hatóságok egy saját eszköz kifejlesztése mellet döntöttek, amelyet a BKA (Bundeskriminalamt – Szövetségi Bűnügyi Hivatal) berkein belül felállítandó un. Információtechnikai Ellenőrzési Kompetenciaközpontban (Kompetenzzentrum für informationstechnische Überwachung CC ITÜ) kívánnak legkésőbb 2014-ig létrehozni. Mindeközben azonban, annak elkészültéig a korábban már említett és kompromittálódott DigiTask szoftvere helyett egy kereskedelmi forgalomban kapható eszközt, az – egyébként szintén német – Eleman/Gamma Group termékét, az un. „FinFisher/FinSpy IT intrusion software kit”-et használják. [27] [28]

A kémprogramok használata nem csak Németországra jellemző, hanem – mint bizonyos körülmények között rendkívül hatékony, vagy sokszor egyetlen alkalmazható eszközt – más országok titkos információgyűjtésre feljogosított szervei is használják, vagy legalábbis használni tervezik. Ilyen témájú hírek érkeztek Svájc [29], Franciaország [30], Ausztria [31], Hollandia [32] és természetesen az USA [33] [34] és az Egyesült Királyság [35] vonatkozásában is.

Az online házkutatásra alkalmas eszközök, azaz kémprogramok természetesen jóval több információt tudnak biztosítani a célszemélyek számítógépéről (pl. tárolt fájlok), a számítógép technikai eszközein keresztül a célszemély tevékenységéről (pl. webkamera képek), mint amit pusztán az elektronikus úton folytatott kommunikációt biztosító szolgáltató – a törvényi feltételek megléte és maximális segítőkész hozzáállás mellett – képes. Az ilyen jellegű kémprogramokat azonban időről időre felderítik és alaposan analizálják az erre szakosodott biztonsági szakemberek vagy hackerek, majd – a törvényes ellenőrzést végző szervezeteknek nem kis anyagi és erkölcsi veszteséget okozva – eredményeiket sokszor publikálják is az Interneten. Erre a sorsra jutott az olasz Hacking Team nevű cég szintén kifejezetten rendvédelmi szerveknek árusított eszköze [36], és a fent említett német Eleman/Gamma Group terméke is. [37]

Érdekes, hogy míg a korábban leírtak szerint a törvényhozók is azon gondolkodnak, vitatkoznak, hogy használhatják-e az arra feljogosított szervek egyáltalán ez a technológiát törvényes ellenőrzésre, és ha igen akkor milyen keretek között, addig egészen meglepő elképzelések is napvilágot látnak. Ilyen az is, hogy a Commission on the Theft of American Intellectual Property nevű Egyesült Államokbeli szórakoztatóipari szervezet is hasonló programokat telepítene a zenei albumok, a filmek és a PC-s játékok adathordozóira, hogy az elkövetett jogsértéseket felderítse. [38]

Egyesült Királyság (UK) és a DPI:

Egy másik módszer a törvényes ellenőrzést végzők kezében az un. mély csomagelemzés (Deep Packet Inspection (DPI) módszere. Ennek lényege, hogy adott helyen átfolyó adatforgalom minden csomagjának a tartalmát vizsgálat alá veszik. Ezt a technológiát használják fel például a behatolás-érzékelő és –védelmi rendszerek (Intrusion Detection/Prevention Systems (IDS/IPS)) [39], [40], de Internetszolgáltatók is előszeretettel alkalmazzák bizonyos – általuk károsnak vélt vagy tartott tartalmak, forgalmak (pl. VoIP, peer-to-peer) – blokkolására. [41] Ugyanakkor ez a technológia lehetőséget teremt a törvényes ellenőrzést végző szolgálatok számára, hogy információhoz jussanak. [40] [42] Ez a hozzáférés azonban meglehetősen korlátozott, hiszen bár a nyíltan küldött adatok könnyen ellenőrizhetők, feldolgozhatók, a titkosított forgalmak esetében a titkosítást fel kell törni, ami időben hosszadalmas, nagy számítástechnikai eszközparkot igénybe vevő folyamat. Ráadásul a nyílt forgalmaknál is jelentősen megnehezíthető az ellenőrzés egy megfelelő – és

ingyenesen rendelkezésre álló – titkosító szoftver eszközök használatával (pl. HTTPS Everywhere). [40]

E korlát ellenére az angol GCHQ ezt a módszert használja „TEMPORA” nevű, a „PRISM”-hez hasonlóan nagyszabású, ám technikailag más alapokon nyugvó ellenőrző programjához. Itt – a kiszivárgott adatok szerint – 200 darab, egyenként 10 Gb/s adatátviteli sebességű optikai kábelen (ezek közül egy időben legalább 46-on) átfolyó összes információt kicsatolják és feldolgozzák a 2007 elején elindított „Mastering the Internet” projekt keretében. A programban öt ország (USA, UK, Kanada, Új Zéland és Ausztrália) titkosszolgálati szervei dolgoznak együtt és osztják meg egymás között az információkat – a kinyert tartalmat és a kísérő un. metaadatokat egyaránt. [43] [44] (Az NSA hasonló, „Upstream” fedőnevű tevékenységét a 4. ábra szemlélteti, amelyből jól látszik, hogy a Prism csak egy része az USA lehallgató rendszerének.)

4. ábra. Az Upstream program jól szemlélteti, hogy a Prism csak egy része az USA lehallgató rendszerének

Forrás: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (letöltve: 2013.07.11.)

Németország és a felhő alapú rendszerek titkosításainak törése:

Németországban az online házkutatás (vagy inkább a kémprogramok) használata mellett felmerült a felhő alapú rendszerek másfajta ellenőrzésének kialakítása is. Erre azért van szükség, mert az említett módszernek – mint minden másiknak – megvannak a korlátai. Azokhoz az információkhoz, amelyekhez nem lehet a kémprogramok segítségével hozzáférni, azokat egy másik módszer alkalmazásával lehet megszerezni. Ennek érdekében a BKA és a BfV (Bundesamt für Verfassungsschutz – Alkotmányvédelmi Hivatal) által működtetett SFZ TK (Strategie- und Forschungszentrum Telekommunikation – Távközlési Stratégiai és Kutatóközpont) nevű intézet azt a feladatot kapta az illetékes szervektől, hogy vizsgálja meg a felhő alapú rendszereknél használt titkosításokat, valamint azt, hogy azok megfejtésén keresztül hogyan lehet hozzáférni a felhasználói adatokhoz, fájlokhoz. [45]

Törvényi szabályozások:
Mint, ahogy a Skype példáján keresztül is látszik, az ellenőrzés egyik leghatékonyabb formája a szolgáltatóval való együttműködés, amelyet törvényi előírásokkal garantálni lehet. Ebbe az irányba több ország is tett lépéseket. Németországban a törvényes ellenőrzés kialakíthatósága és hatékony alkalmazhatósága érdekében a telekommunikáció fogalmát kívánják kiszélesíteni minden online adatcserére (beleértve az ezekhez tartozó felhasználói adatokat is), és ezekre a hagyományos hírközléssel analóg rendelkezéseket alkotni az erről szóló jogszabályban. [46] Hasonló jogszabályváltozásokat akar az USA is bevezetni, amelyekkel kötelezheti az olyan szolgáltatókat, mint a Google vagy a Facebook, hogy tegyék lehetővé a rajtuk keresztül folytatott online kommunikáció törvényes ellenőrzését, [47] ráadásul a törvényi szabályozás azt is garantálja, hogy minden szolgáltató bekényszeríthető a rendszerbe. Ugyanakkor az USA-ban a már létező jogszabályok (Protect America Act (2007), FISA (Foreign Intelligence Surveillance Act) Amendments Act (2008) is kötelezettségeket rónak a magáncégekre a törvényes ellenőrzés tekintetében. [14]

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

A cikksorozat első része – a „Felhő alapú rendszerek törvényes ellenőrzési problémái" című cikkre alapozva – áttekintette a PC/SaaS felhő alapú rendszerek törvényes ellenőrzése kapcsán felmerült problémákat, majd – a teljesség igénye nélkül – megvizsgálta, hogy különböző országok hogyan valósítják meg, vagy legalábbis hogyan próbálják megvalósítani az említett rendszerek törvényes ellenőrzését.
Jelen cikkből levonható következtetések:

1. A PC/SaaS felhő alapú rendszerek ellenőrzése minden ország törvényes ellenőrzést végző szervei számára kihívást jelentenek.
2. A törvényes ellenőrzést végzők számára több technikai megoldás is létezik a PC/SaaS felhő alapú rendszerek ellenőrzésére.
3. Ezen technikai megoldások jogi megítélése kétséges.
4. Nincsen olyan általánosan elfogadott jogi szabályozás a PC/SaaS felhő alapú rendszerek ellenőrzése kapcsán, amelyhez – akár Magyarországnak is – igazodni lehetne.
5. A felhozott külföldi példákból jól látszik, hogy – a technikai, jogi korlátok és a hatékony ellenőrzés okán – általában több módszert használnak a törvényes ellenőrzésre feljogosított szervezetek.

A nemzetközi példák bár széles, de nem teljes körű áttekintést adtak. Ennek egyrészt az az oka, hogy csak publikus információkra lehet támaszkodni, azok pedig – a problémakör jellegére tekintettel meglehetősen korlátozottak, ráadásul szinte sohasem igazoltak, így nem lehetnek teljes körűek. Másrészt pedig az, hogy a törvényes ellenőrzésre felhatalmazott szervek részére rendelkezésre álló módszerek ismertetéséhez, elemzéséhez egyébként sincs szükség teljes körű áttekintésre.

A nemzetközi tapasztalatok vizsgálata elsősorban tehát a technikai lehetőségek áttekintésére és bizonyos problémák felvetésére szolgált. Ezen tapasztalatok megismerését követően lehet – a „Felhő alapú rendszerek törvényes ellenőrzési problémái" című cikkben javasolt, az említett rendszerek hatékony ellenőrzésének kialakítása felé tett következő lépésként – elvégezni a törvényes ellenőrzésre jelenleg rendelkezésre álló technikai eszközök és módszerek leírását, összehasonlítását, azok előnyeinek, hátrányainak meghatározásával együtt. A fent említett módszereket még ki kell egészíteni az un. közbeékelődéses támadással (Man-in-the-Middle), amire ugyan a fentiekben nincs példa, de ez is fontos eleme a törvényes ellenőrzést végző szervezetek módszertárának. Ezekkel foglalkozik a cikksorozat második része.

Felhasznált irodalom

[1] Kovács Zoltán: FELHŐ ALAPÚ RENDSZEREK TÖRVÉNYES ELLENŐRZÉSI PROBLÉMÁI Hadmérnök, VIII. Évfolyam 1. szám - 2013. március

[2] Molnár Gábor, Zalatnay Zsolt: Szolgáltatások és architektúrák Skype előadás www.tmit.bme.hu/dl239 (2013. 02. 13.)

[3] Sándor Molnár, Marcell Perényi: On the identification and analysis of Skype traffic INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS 21 April 2010 in Wiley Online Library http://hsnlab.tmit.bme.hu/~molnar/files/ijcs2010.pdf (2013.06.18.)

[4] Salman A. Baset and Henning Schulzrinne: An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol (2004. 09. 15.) http://www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf (2013.06.18.)

[5] Does Skype use encryption? https://support.skype.com/en/faq/FA31/does-skype-use-encryption (2013. 07. 11.)

[6] Kara Swisher: Done Deal: Microsoft to Buy Skype for $8.5 Billion in Cash (2011. 05.10.) http://allthingsd.com/20110510/done-deal-microsoft-to-buy-skype-for-8-5-billion-in-cash/ (2013.06.17.)

[7] Az EU jóváhagyta a Microsoft Skype-felvásárlását (2011. 10. 07.) http://www.origo.hu/techbazis/20111007-az-europai-bizottsag-jovahagyta-a-microsoft-skypefelvasarlasat.html (2013.06.17.)

[8] Bodnár Ádám: A Microsoft megvette a Skype-ot (2011. 05. 10.) http://www.hwsw.hu/hirek/46667/microsoft-skype-voip-telefon-felvasarlas.html (2013.06.17.)

[9] Miért jó a Skype a Microsoftnak? http://insiderblog.hu/kulfold/2011/05/12/skype/ - (2013.06.17.)

[10] Skype does away with random supernodes (2012. 05. 01.) http://expertmiami.blogspot.hu/2012/05/skype-does-away-with-random-supernodes.html (2013.06.18.)

[11] Skype with care – Microsoft is reading everything you write (2013. 05. 14.) http://www.h-online.com/security/news/item/Skype-with-care-Microsoft-is-reading-everything-you-write-1862870.html (2013.06.18.)

[12] Jürgen Schmidt: Skype's ominous link checking: Facts and speculation (2013. 05. 17.) http://www.h-online.com/security/features/Skype-s-ominous-link-checking-Facts-and-speculation-1865629.html (2013.06.18.)

[13] Kirils Solovjovs: On Skype URL eavesdropping (3013. 05. 17.) http://seclists.org/fulldisclosure/2013/May/78 (2013.06.18.)

[14] Barton Gellman and Laura Poitras: U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program (2013. 06. 07.) http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (2013.06.28.)

[15] Betilthatják Oroszországban a Skype-ot, a Gmailt és a Hotmailt (2011. 04. 09.) http://www.sg.hu/cikkek/81250/betilthatjak_oroszorszagban_a_skype_ot_a_gmailt_es_a_hotmailt (2013.06.18.)

[16] Yuliya Fedorinova: Microsoft May Offer Skype Codes to Russia's FSB, Vedomosti Says (2011. 06. 09.) http://www.bloomberg.com/news/2011-06-09/microsoft-may-offer-skype-codes-to-russia-s-fsb-vedomosti-says.html?cmpid=yhoo (2013.06.18.)

[17] Lehallgathatják az oroszok a Skype-ot (2011. 06. 11.) http://www.sg.hu/cikkek/82579/lehallgathatjak_az_oroszok_a_skype_ot (2013.06.18.)

[18] Évek óta lehallgatható Oroszországban a Skype (2013. 03. 18.) http://www.sg.hu/cikkek/96074/evek_ota_lehallgathato_oroszorszagban_a_skype - (2013.06.18.)

[19] Vernon Silver: Cracking China's Skype Surveillance Software (2013. 03. 08.) http://www.businessweek.com/articles/2013-03-08/skypes-been-hijacked-in-china-and-microsoft-is-o-dot-k-dot-with-it (2013.06.20.)

[20] Koi Tamás: Egyre nagyobb a nyomás Európában a Skype-on (2013. 03. 13.) http://www.hwsw.hu/hirek/49958/skype-microsoft-franciaorszag-arcep-voip.html - (2013.06.20.)

[21] SKYPE REFUSES TO REGISTER AS AN OPERATOR (2013. 03. 12.) http://arcep.fr/index.php?id=8571&tx_gsactualite_pi1%5Buid%5D=1593&tx_gsactualite_pi1%5Bannee%5D=&tx_gsactualite_pi1%5Btheme%5D=&tx_gsactualite_pi1%5Bmotscle%5D=&tx_gsactualite_pi1%5BbackID%5D=26&cHash=baebcd8ef257d3194065360ecec41a90&L=1 (2013.06.20.)

[22] Mindenki lehallgatható lenne Németországban (2008. 01. 17.) http://www.sg.hu/cikkek/57484/mindenki_lehallgathato_lenne_nemetorszagban - (2013.06.24.)

[23] Dajkó Pál: A német rendőröknek egyelőre tilos a hackelés (2007. 02. 06.) http://itcafe.hu/hir/a_nemet_rendoroknek_egyelore_tilos_a_hackeles.html - (2013.06.24.)

[24] Dajkó Pál: Új alkotmányos jog született: az IT-jog (2008. 03. 01.) http://itcafe.hu/hir/bundestrojaner_alkotmany_itjog.html (2013.06.24.)

[25] Dajkó Pál: Lebukott az állami kémprogram (2011. 10. 10.) http://itcafe.hu/hir/chaos_computer_club_nemetorszag_bundestrojaner.html - (2013.06.24.)

[26] Chaos Computer Club analyzes government malware (2011. 10. 08.) http://ccc.de/en/updates/2011/staatstrojaner (2013.06.24.)

[27] Andre Meister: Secret Government Document Reveals: German Federal Police Plans To Use Gamma FinFisher Spyware (2013. 01. 16.) https://netzpolitik.org/2013/secret-government-document-reveals-german-federal-police-plans-to-use-gamma-finfisher-spyware/ (2013.06.28.)

[28] https://netzpolitik.org/wp-upload/BMI-Bericht-Sachstand-CC-TK%C3%9C.pdf (2013.06.28.)

[29] Superintendent Trojan (2006. 10. 09.) http://www.h-online.com/security/news/item/Superintendent-Trojan-731613.html (2013.06.28.)

[30] Cyberperquisitions (2008. 02. 28.) http://www.lemonde.fr/idees/article/2008/02/28/cyberperquisitions_1016773_3232.html (2013.06.28.)

[31] Ausztriában törvényes lesz az online házkutatás (2007. 10. 18.) http://www.sg.hu/cikkek/55658/ausztriaban_torvenyes_lesz_az_online_hazkutatas - (2013.06.28.)

[32] Külföldi szervereket is megtámadhat a holland rendőrség (2013. 05. 06.) http://www.sg.hu/cikkek/97134/kulfoldi_szervereket_is_megtamadhat_a_holland_rendorseg (2013.06.28.)

[33] Declan McCullagh: FBI remotely installs spyware to trace bomb threat (2007. 06. 18.) http://news.cnet.com/8301-10784_3-9746451-7.html (2013.06.28.)

[34] http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf (2013.06.28.)

[35] Duncan Gardham: Government plans to extend powers to spy on personal computers (2009. 01. 04.) http://www.telegraph.co.uk/news/uknews/law-and-order/4109031/Government-plans-to-extend-powers-to-spy-on-personal-computers.html (2013.06.28.)

[36] Sergey Golovanov: Spyware. HackingTeam (2013. 04. 23.) http://www.securelist.com/en/analysis/204792290/Spyware_HackingTeam 2013.06.28.)

[37] Morgan Marquis-Boire - Bill Marczak - Claudio Guarnieri - John Scott-railton: For their eyes only (2013.05.01.) https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf (2013.06.28.)

[38] The IP commission report (2013. május) http://ipcommission.org/report/IP_Commission_Report_052213.pdf (2013.06.28.)

[39] Ido Dubrawsky: Firewall Evolution - Deep Packet Inspection (2010. 11. 02.) http://www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection (2013.06.28.)

[40] Alex Wawro: A simple guide to Deep Packet Inspection (2012. 02. 01.) http://features.techworld.com/security/3334780/a-simple-guide-to-deep-packet-inspection/ (2013.06.28.)

[41] BEREC preliminary findings on traffic management practices in Europe show that blocking of VoIP and P2P traffic is common, other practices vary widely http://berec.europa.eu/doc/2012/TMI_press_release.pdf (2013.06.28.)

[42] Ellen Messmer : US government's use of deep packet inspection raises serious privacy questions (2013. 04. 24.) http://news.techworld.com/security/3444019/dhs-use-of-deep-packet-inspection-technology-in-new-net-security-system-raises-serious-privacy-questions/ (2013.06.28.)

[43] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball: GCHQ taps fibre-optic cables for secret access to world's communications (2013. 06. 21.) http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (2013.07.05.)

[44] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball: Mastering the internet: how GCHQ set out to spy on the world wide web (2013. 06. 21.) http://www.guardian.co.uk/uk/2013/jun/21/gchq-mastering-the-internet (2013.07.05.)

[45] Németország a felhőadatokat is ellenőrizné (2013. 04. 07.) http://www.sg.hu/cikkek/96458/nemetorszag_a_felhoadatokat_is_ellenorizne (2013.06.28.)

[46] Szigorítanák a német távközlési törvényt (2013. 04. 21.) http://www.sg.hu/cikkek/96798/szigoritanak_a_nemet_tavkozlesi_torvenyt (2013.06.28.)

[47] Ellen Nakashima: Panel seeks to fine tech companies for noncompliance with wiretap orders (2013. 04. 29.) http://www.washingtonpost.com/world/national-security/proposal-seeks-to-fine-tech-companies-for-noncompliance-with-wiretap-orders/2013/04/28/29e7d9d8-a83c-11e2-b029-8fb7e977ef71_story.html (2013.06.28.)

Ábrák jegyzéke

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Kovács Zoltán
zkovacs@nbsz.gov.hu

FELHŐ ALAPÚ RENDSZEREK TÖRVÉNYES ELLENŐRZÉSI MÓDSZEREI VIZSGÁLATA II.

Absztrakt

A napjaink kommunikációs szokásait nagymértékben meghatározzák az Internetes kommunikációt biztosító felhő alapú rendszerek. 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 (pl. Facebook, gmail, Dropbox, Twitter, Skype stb.) Ezen rendszerek törvényes ellenőrzésének igénye a felhasználás ütemével arányosan nő. A cikksorozat első része áttekinti az említett rendszerek törvényes ellenőrzésének kihívásait, majd publikus forrásokból elérhető információkra alapozva jellemző példákat mutat be külföldi nemzetbiztonsági szolgálatok és rendvédelmi szervek által használt módszerekre. A második rész megvizsgálja a törvényes ellenőrzéshez rendelkezésre álló technikai lehetőségeket, felállítja az ezek elemzéséhez szükséges szempontrendszert, majd az így kialakított szempontrendszer alapján elvégzi azok elemzését.

The habits of recent communication have been dramatically determined by cloud computing which ensure communication via Internet. 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 (e.g. Facebook, gmail, Dropbox, Twitter, Skype, etc.). The requirement of lawful monitoring of these cloud computing systems has been growing proportionally to the growth of using. The first part of this article series is reviewing the problems appearing in lawful monitoring of cloud computing systems mentioned above, and then presenting representative lawful monitoring methods used by foreign national security services and law enforcement agencies based on public sources. The second part of this article series is analysing the possible technical solutions of lawful monitoring, setting up criteria which needed to analyse them, then doing the analysis of technical solutions by this criteria.

Kulcsszavak: *felhő alapú rendszerek, törvényes ellenőrzés, Skype ~ cloud computing, lawful monitoring, Skype*

BEVEZETÉS

A kommunikáció formái, lehetőségei az Internet és az azt kihasználó alkalmazások fejlődésével ugrásszerűen változnak, bővülnek. 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 (továbbiakban: PC/SaaS felhő alapú rendszerek). 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 PC/SaaS felhő alapú rendszerek törvényes ellenőrzésének igénye a felhasználás ütemével arányosan nő, hiszen a (potenciális) célszemélyi kör is ezt használja leginkább. A „Felhő alapú rendszerek törvényes ellenőrzési problémái" című cikk bemutatta az Internet és az azt felhasználó 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. Az összefoglalás és a következtetések részben a törvényes ellenőrzés hatékony kialakítása érdekében teendő továbblépéshez újabb elvégzendő feladatokat fogalmazott meg. Ezek közül az egyik a következő: *„… célszerű áttekinteni, összehasonlítása a törvényes ellenőrzésre jelenleg rendelkezésre álló technikai eszközöket és módszereket, azok előnyeivel, hátrányaival együtt."*. Jelen cikksorozat ezzel a foglalkozik részletesen.

A cikksorozat első része áttekinti a PC/SaaS felhő alapú rendszerek törvényes ellenőrzésének kihívásait, majd ezt követően publikus forrásokból elérhető információkra alapozva jellemző példákat mutat be külföldi nemzetbiztonsági szolgálatok és rendvédelmi szervek által használt módszerekre. A példák ismertetésénél főként a Skype-ot használja mintának. Egyrészt azért, mert ennek a rendszernek a lehallgatása minden országban megoldandó, de problémás feladatként jelentkezett, másrészt pedig azért, mert jól példázza, hogy egy új infokommunikációs rendszer törvényes ellenőrzése kapcsán a különböző országok képesek gyökeresen eltérő irányokba elindulni.

A második rész megvizsgálja a törvényes ellenőrzéshez rendelkezésre álló technikai lehetőségeket, majd felállítja az ezek elemzéséhez szükséges szempontrendszert. Az így kialakított szempontrendszer alapján elvégzi a felsorolt technikai megoldások elemzését, csoportosítva azok előnyeit, hátrányait. Végezetül a következtetések levonása után – illeszkedve a „Felhő alapú rendszerek törvényes ellenőrzési problémái" című cikk összegzésében leírtakhoz – további, a PC/SaaS felhő alapú rendszerek törvényes ellenőrzésének hatékony kialakítása érdekében végrehajtandó feladatokat fogalmaz meg.

A TÖRVÉNYES ELLENŐRZÉS TECHNIKAI LEHETŐSÉGEI

Mint ahogy azt a cikksorozat első részéből kitűnik, az arra felhatalmazott nemzetbiztonsági és rendvédelmi szerveknek jelenleg több technikai megoldás is a rendelkezésére áll ahhoz, hogy a PC/SaaS felhő alapú rendszereket törvényes ellenőrzés alá vonják. Az összehasonlító elemzés elvégzése előtt azonban érdemes áttekinteni ezeket a módszereket, megoldásokat, és összefoglalni azok főbb jellemzőit, tulajdonságait.

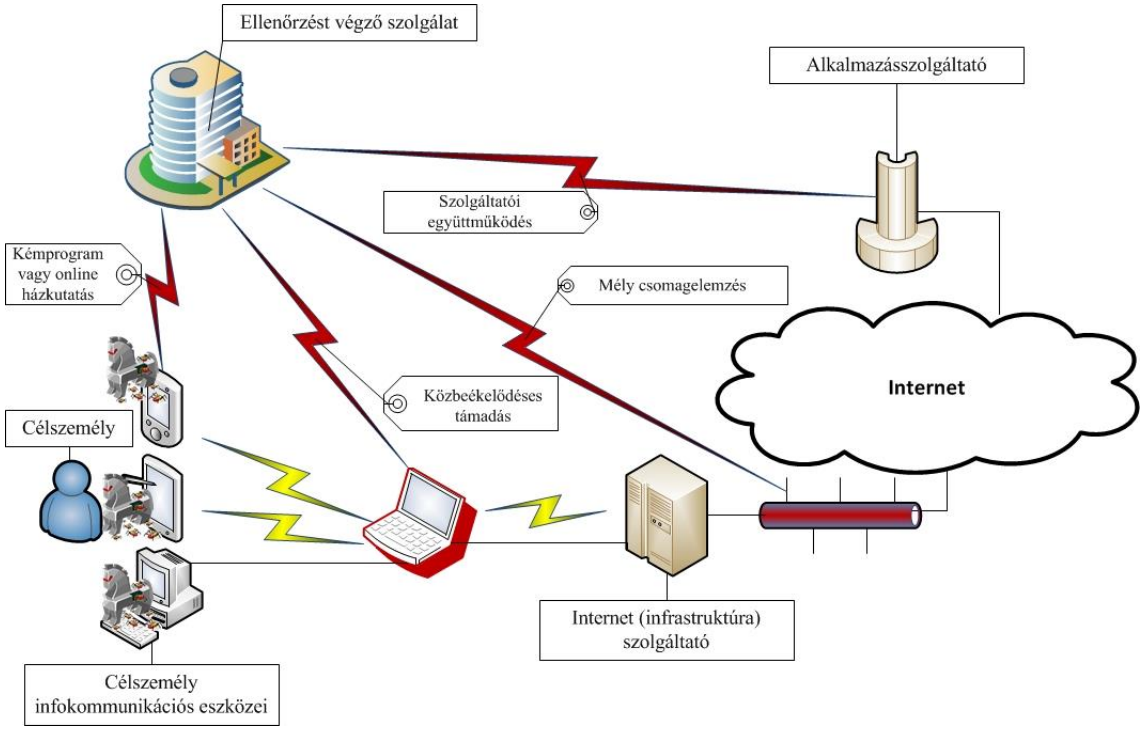
A cikknek nem célja az egyes módszereket minden részletet felölelően ismertetesse, azokat csupán általánosítva, csak az összehasonlítási szempontrendszer felállításához és a végkövetkeztetések levonásához szükséges mértékben tárgyalja.

A PC/SaaS felhő alapú rendszerek törvényes ellenőrzésre alapvetően az alábbi négy módszert használhatják az arra felhatalmazott szolgálatok:

1. aktív támadó eszköz vagy kémprogram (spyware),
2. közbeékelődéses támadás (Man in the middle),
3. mély csomagvizsgálat (Deep Packet Inspection (DPI)),
4. együttműködés a szolgáltatóval.

A módszerek elnevezései önkényesek. Valódi, mindenki által elfogadott magyar megfelelőik vagy nem alakultak ki, vagy az ezekről szóló szakirodalom is többféle megnevezéssel használja azokat.

A fenti módszerekre rendkívül jellemző az alkalmazásakor használt adatszerző, elfogó eszközök (ebbe bele kell érteni a hardver és szoftver elemeket egyaránt) távolsága a célszemélytől. Ezt jól szemlélteti az 1. ábra.



1. ábra. Az adatszerző, elfogó eszközök távolsága a célszemélytől
Forrás: saját

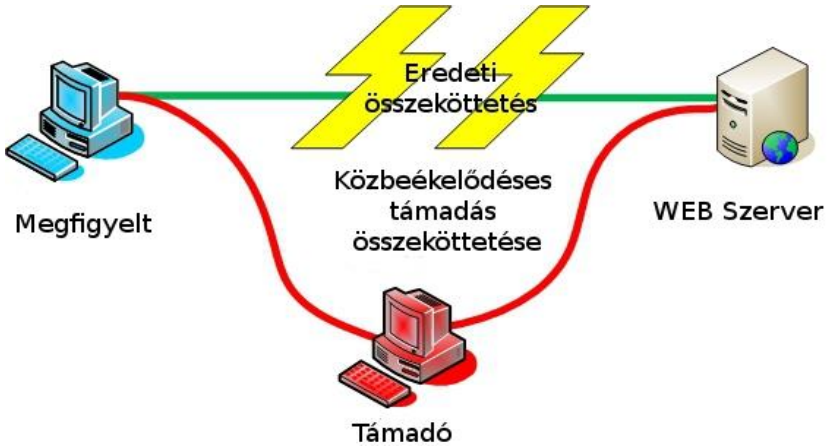
Aktív támadó eszköz (kémprogram vagy online házkutatás):

Az aktív támadó eszközök, vagy közismertebb, a cikksorozat első részében említett neveiken kémprogramok vagy online házkutatási eszközök esetében a célszemély infokommunikációs eszközére, eszközeire (pl. számítógép, telefon, tablet stb.) egy speciális „kártékony” szoftvert telepít az ellenőrzést végző szolgálat. Ez sok hasonlóságot mutat a valódi kártékony szoftverekkel, de ebben az esetben ez törvényes célokat szolgál. Talán azt az analógiát lehetne erre alkalmazni, mint amikor egy lőfegyverről beszélünk, amely más értelmet nyer egy bűnöző és mást egy rendőr kezében.

A kémprogram bejuttatása a célszemély eszközére több féle módszerrel is lehetséges, hasonlóan a kiberbűnözők által használt módozatokhoz (pl. elektronikus levél csatolmányaként, fertőzött weboldal segítségével, „0 day” sebezhetőség kihasználásával stb.). A működés során ezek képesek az online kommunikáció elfogására, de billentyűzetleütések tárolására, vagy akár – ha van – a webkamerával képek készítésére is. Az információkat azután összegyűjtve küldik el az aktív támadó eszköz tulajdonosának. [1] [2] [3] [4] [5]

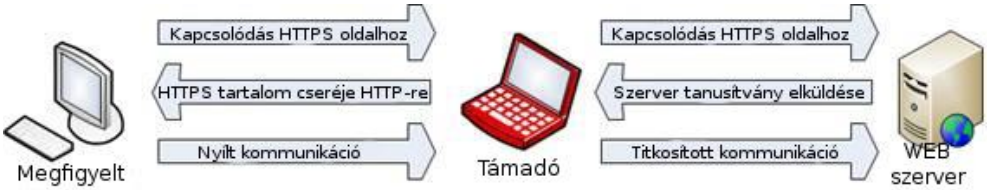
Közbeékelődéses támadás (Man in the Middle):

Leegyszerűsítve a dolgot, a közbeékelődéses támadás esetében a támadó (ellenőrzést végző szolgálat) úgy hallgatja le a két fél között zajló kommunikációt, hogy a kommunikációs csatornát megszakítja (legyen az vezetékes vagy vezeték nélküli), majd abba, a két kommunikáló fél közé „beállva" mindkettőjük számára a másik félnek adja ki magát. A kapcsolat ezáltal mindkét fél számára zavartalannak tűnik, valójában azonban a teljes forgalom „átfolyik" a támadó eszközén, amellyel az itt zajló kommunikációt lehallgathatja, ahhoz teljes mértékben hozzáfér. Ezt szemlélteti a 2. ábra.



2. ábra. Közbeékelődéses támadás
Forrás: https://www.owasp.org/index.php/Man-in-the-middle_attack (letöltve: 2013.07.16.)

A sikeres közbeékelődéses támadáshoz több feltételnek is teljesülnie kell. A támadónak hozzá kell férnie a kommunikációs csatornához, képesnek kell lennie annak megszakítására (legyen az vezetékes vagy vezeték nélküli kapcsolat) oly módon, hogy megakadályozza, hogy az üzenetek eljussanak a valódi címzetthez, majd le kell tudni lehallgatni a rajta küldött üzeneteket. Ez titkosítás nélküli kommunikáció esetében viszonylag egyszerű, de bizonyos esetekben, kis szerencsével és a valódi kommunikáló fél (felek) figyelmetlenségével akár titkosított kommunikáció esetén is megvalósítható. Ezt szemlélteti a 3. ábra.



3. ábra. Példa HTTPS kommunikáció lehallgatására
Forrás: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html (letöltve: 2013.07.16.)

Sikeres közbeékelődéses támadás akkor hajtható végre viszonylag egyszerű eszközökkel és nagy valószínűséggel, ha a célszemélyhez (azaz az egyik kommunikáló félhez) a támadó a lehető legközelebb helyezkedik el. [6] [7] [8] [9] 10] [11]

Mély csomagvizsgálat (Deep Packet Inspection (DPI)):

A mély csomagvizsgálat azt jelenti, hogy az adatcsomagoknak nemcsak a fejlécét, hanem azok adattartalmát is vizsgálat alá vetik, majd az adattartalom alapján kiszűrik az „érdekes" adatcsomagokat. A szűrés jellege a mély csomagvizsgálat felhasználásának céljától függ, a csomagvizsgálati módszerek azonban technikailag függetlenek attól. [12]

A mély csomagvizsgálatot leggyakrabban három esetben szokták alkalmazni. Az első eset a behatolást észlelő és behatolásvédelmi rendszerekben (Intrusion Detection Systems (IDS),

Intrusion Prevention Systems (IPS)) történő felhasználás. Ezek a rendszerek a csomagok elemzésekor speciális bitmintákat (ismert támadókódokat) keresnek erre dedikált eszközök segítségével, majd a felismert, rosszindulatú kódot tartalmazó csomagokat kiszűrik. [13] A második a hírközlési/Internet szolgáltatók rendszereiben történő alkalmazás. Itt az internet protokoll alapú hangátviteli szolgáltatások (VoIP) és a peer-to-peer (P2P) kapcsolaton alapuló fájlcsere forgalmának blokkolására használják a technológiát. [14] A harmadik a törvényes ellenőrzés, ahol a csomagok vizsgálata alapján dönthető el, hogy az ellenőrzést végző számára érdekes-e (pl. adott célszemélyhez tartozik-e az email), vagy sem. Itt a szűrés azonban nem a kiválasztott csomagok blokkolását szolgálja, hanem azoknak az ellenőrzést végző szolgálathoz (is) történő eljuttatását. [15] [16] [17] [18]

Titkosítás nélküli kommunikáció esetén a lehallgatás viszonylag egyszerűen, sőt – ebben az esetben, ellentétben a közbeékelődéses támadással – tömegesen is megvalósítható. Ugyanakkor titkosított kommunikáció esetén a tartalomhoz való hozzáféréshez feltétlenül szükséges a titkosítás feltörése, ez pedig is hosszadalmas, nagy számítástechnikai eszközparkot igénybe vevő folyamat. Ráadásul a kommunikáló felek akár a nyílt forgalmaknál is egyszerű – és ingyenesen rendelkezésre álló – titkosító szoftver eszközök használatával (pl. HTTPS Everywhere) jelentősen megnehezíthetik, vagy akár el is lehetetlenítik az ellenőrzést. [15]

Együttműködés a szolgáltatóval:

A szolgáltatóval való együttműködés a hagyományos hírközlési szolgáltatóknál már jól ismert és bevált modell szerint működik. Ekkor az ellenőrzést végző szerv eljuttatja a célszemélyhez kapcsolódó releváns adatokat (pl. felhasználói név) a szolgáltató rendszerébe, majd a szolgáltató automatikusan (emberi beavatkozás nélkül) vagy egyedi kiszolgálással (emberi beavatkozással) biztosítja a – rendszerében rendelkezésre álló – kért adatokat, információkat, vagy akár a rajta átfolyó kommunikáció tartalmát is. [17]

A TÖRVÉNYES ELLENŐRZÉSI MÓDSZEREK VIZSGÁLATI, ÖSSZEHASONLÍTÁSI SZEMPONTJAI

Az eddigiekből tehát látható, hogy a PC/SaaS felhő alapú rendszerek törvényes ellenőrzésre több lehetőség, módszer is a felhatalmazott szolgálatok rendelkezésére áll. Ezek a módszerek azonban jelentősen – mondhatni minden paraméterükben – eltérnek egymástól, akár a technikai megvalósításukat, akár a hatékonyságukat, vagy akár a jogi szabályozottságukat vesszük figyelembe. Annak érdekében, hogy az egyes módszereket össze tudjuk hasonlítani, először fel kell állítani egy, a vizsgálatukra megfelelő szempontrendszert. Ennek tartalmaznia kell minden olyan lényeges szempontot, amely alapján a titkos információgyűjtésre és a titkos adatszerzésre felhatalmazott szerv dönteni tud arról, hogy melyiket (melyikeket) kívánja megvasalósítani és munkájában felhasználni.

A módszer kiválasztásakor a következő szempontokat célszerű a törvényes ellenőrzésre felhatalmazott szervezeteknek megvizsgálnia, így a felállítandó vizsgálati szempontrendszernek tartalmaznia:

- *Az egy időben ellenőrizhető célszemélyek száma:* Ebben a kérdéskörben nem elsősorban a tényleges számadatot kell megvizsgálni, hanem azt, hogy egyedi vagy tömeges ellenőrzést tesz-e lehetővé a módszer.
- *Az ellenőrző eszköz működési módja:* Fontos kérdés, hogy az eszköz aktív vagy passzív módon működik-e. Ennek ugyanis meghatározó jelentősége van egyrészt az ellenőrzés célszemély általi felfedezhetőségében (dekonspiráció), másrészt a módszer alkalmazására, alkalmazhatóságára vonatkozó jogi háttér vizsgálatakor (meglévő törvényi szabályozás keretei).

- *A módszer jogi hátterének rendezettsége:* Ennek keretében kell megvizsgálni, hogy az adott módszer egyáltalán alkalmazható-e az adott ország jogrendszere szerint, és ha igen, milyen keretek között. Az is elképzelhető, hogy bizonyos ellenőrzési metódusokra – annak újszerűsége miatt – sem kizáró, sem engedélyező szabályozó sincs a jogrendben.
- *Az ellenőrző eszköz célszemélyhez való közelsége:* A dekonspiráció veszélyének a felméréséhez meg kell vizsgálni, hogy telepítéskor, működés közben, leállításkor és eltávolításkor (törvényes ellenőrzés megszüntetésekor), milyen távolságban (jobban érzékeltetné a problémát, a távolság helyett a közelség megfogalmazás) kell lenni a célszemélytől, hogy a módszert alkalmazni lehessen.
- *A módszer alkalmazásának technikai problémái:* Itt a telepítéskor, működés közben, leállításkor és eltávolításkor (törvényes ellenőrzés megszüntetésekor) felmerülő technikai problémákat kell számba venni.
- *A hozzáférhető adatok köre:* A döntés szempontjából lényeges elem, hogy az adott módszerrel milyen információkhoz (csak az online átfolyó vagy a tárolt adatok is) jut hozzá az törvényes ellenőrzést végző szervezet.
- *Online kommunikációhoz való hozzáférés teljes körűsége:* Fontos tényező, hogy a célszemély online forgalmát teljes egészében vagy csak részlegesen biztosítja az adott módszer. Ennek a kérdésnek a vizsgálatakor nem vesszük figyelembe, hogy a kommunikáció titkosított-e vagy sem, csak azt, hogy a célszemély minden kommunikációja összes bitjének elfogását biztosítja-e az adott módszer.
- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén:* Az ellenőrzési módszer hatékonyságát nagymértékben befolyásolja, hogy képes-e, és ha igen, milyen esetekben és mértékben a titkosított kommunikációból az eredeti tartalmat (pl. üzeneteket, képeket, beszédet stb.) biztosítani a titkos információgyűjtést végző szerv számára.
- *Beruházási igény:* Az sem elhanyagolható szempont, hogy az adott módszer alkalmazásához szükséges eszközrendszer mennyibe kerül.
- *Egyéb költségek:* Olyan egyéb járulékos költségek is fellépnek, felléphetnek, amelyekkel komolyan számolni kell az alkalmazást megelőzően. Ilyenek lehetnek pl. az együttműködőknek fizetendő díjak, a betanítás vagy éppen speciális ismeretekkel rendelkező (pl. hacker) szakemberek (tovább)képzési vagy megvásárlási költségei.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* Lényeges kérdés az is, hogy a célszemély adataihoz a törvényes ellenőrzést végző szolgálat munkatársain kívül ki fér, férhet még hozzá. Ez ugyanis nagymértékben növelheti a dekonspiráció veszélyét. (Itt nem vizsgáljuk az eszköz alkalmazása során, a működés miatt fellépő dekonspirációt, azaz azt, amikor a célszemély, vagy annak közvetlen környezete szerez tudomást az alkalmazásról. Ebben az esetben kizárólag harmadik fél hozzáférését (pl. szolgáltató szakemberei) vizsgáljuk.)

A fenti szempontok szerint megvizsgálva az egyes, korábban említett törvényes ellenőrzési módszereket, a titkos információgyűjtésre felhatalmazott szerv már nem csak az adott módszer bevezetéséről, rendszeresítéséről képes dönteni, hanem arról is, hogy majd adott ügyben a körülményeknek megfelelően melyik ellenőrző metódus használata a legcélravezetőbb.

A TÖRVÉNYES ELLENŐRZÉS MÓDSZEREINEK VIZSGÁLATA

Vizsgáljuk meg tehát a korábban leírt négy módszert a fenti kritériumrendszer alapján.

Aktív támadó eszköz (kémprogram vagy online házkutatás):

- *Az egy időben ellenőrizhető célszemélyek száma:* egyedi ellenőrzést tesz lehetővé.
- *Az ellenőrző eszköz működési módja:* aktív módszer, a dekonspiráció veszélye magas.
- *A módszer jogi hátterének rendezettsége:* a módszerre nincsenek mindenki által elfogadott jogszabályok, több ország most próbálja a felhasználás, alkalmazás pontos jogi kereteit kialakítani.
- *Az ellenőrző eszköz célszemélyhez való közelsége:* a vizsgált módszerek közül a legközelebb működik a célszemélyhez.
- *A módszer alkalmazásának technikai problémái:* a közelség okán a telepítés, újratelepítés nehézkes lehet, az online kapcsolat megszakadásakor az eszköz „eltűnik” az ellenőrzést végző szervek elől, kikerül a felügyeletük alól.
- *A hozzáférhető adatok köre:* nemcsak az online forgalomhoz, hanem az adott eszközön tárolt minden fájlhoz elérést biztosít, sőt további ellenőrzési lehetőségeket (pl. web kamerával képkészítés) is kínál.
- *Online kommunikációhoz való hozzáférés teljes körűsége:* nem ad teljes körű hozzáférést, hiszen csak azon az eszközön bonyolított kommunikációt képes elfogni, amelyikre feltelepítették.
- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén:* a kommunikációt a titkosítást megelőzően képes elfogni, így a felhasznált titkosítástól függetlenül ellenőrizhetővé teszi a kommunikációt.
- *Beruházási igény:* közepes, az alkalmazott eszközök, a bejuttatáshoz esetleg használt un. „0 day” sebezhetőségek költségesek.
- *Egyéb költségek:* magas, a módszer alkalmazásához speciális (hacker) tudással rendelkező szakemberek szükségesek.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* ennek lehetősége minimális.

Közbeékelődéses támadás (Man in the Middle):

- *Az egy időben ellenőrizhető célszemélyek száma:* egyedi ellenőrzést tesz lehetővé.
- *Az ellenőrző eszköz működési módja:* aktív módszer, a dekonspiráció veszélye magas.
- *A módszer jogi hátterének rendezettsége:* a módszerre nincsenek mindenki által elfogadott jogszabályok.
- *Az ellenőrző eszköz célszemélyhez való közelsége:* a módszer kizárólag a célszemély (infokommunikációs eszközének) közvetlen közelében működik.
- *A módszer alkalmazásának technikai problémái:* az alkalmazás teljes időtartamában kötelezően a célszemély (infokommunikációs eszközének) közelében kell tartózkodni. Ez pedig az egész alkalmazást nehézkessé, esetlegessé teszi, teheti.
- *A hozzáférhető adatok köre:* csak az online forgalomhoz biztosít elérést.
- *Online kommunikációhoz való hozzáférés teljes körűsége:* nem ad teljes körű hozzáférést, hiszen csak azon az eszközön bonyolított kommunikációt képes elfogni, amelyik forgalma „átfolyik” az ellenőrző (ábrán: támadó) eszközön.
- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén:* kis szerencsével és a célszemély figyelmetlenségével párosulva bizonyos titkosított forgalmaknál is lehetővé teszi a közlemények megismerését.

- *Beruházási igény:* alacsony, az ellenőrzés gyakorlatilag kommersz eszközökkel megvalósítható.
- *Egyéb költségek:* magas, a módszer alkalmazásához speciális (hacker) tudással rendelkező szakemberek szükségesek.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* ennek lehetősége minimális.

Mély csomagvizsgálat (Deep Packet Inspection (DPI)):

- *Az egy időben ellenőrizhető célszemélyek száma:* tömeges ellenőrzést tesz lehetővé.
- *Az ellenőrző eszköz működési módja:* passzív módszer, a dekonspiráció veszélye alacsony.
- *A módszer jogi hátterének rendezettsége:* a módszerre a hagyományos hírközlési szolgáltatókra vonatkozó jogszabályok szerint lehet eljárni.
- *Az ellenőrző eszköz célszemélyhez való közelsége:* a célszemélytől (infokommunikációs eszközeitől) távol működik.
- *A módszer alkalmazásának technikai problémái:* az óriási „átfolyó" adatmennyiség szűrése, feldolgozása nagy számítástechnikai hátteret és sok embert igényel, így gondot okozhat.
- *A hozzáférhető adatok köre:* csak az online forgalomhoz biztosít elérést.
- *Online kommunikációhoz való hozzáférés teljes körűsége:* közel teljes körű hozzáférést adhat, hiszen az ellenőrző eszköz(ök) elhelyezésétől függően a célszemély akár több eszközén, akár több szolgáltató hálózatán keresztül lebonyolított kommunikációját képes elfogni.
- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén:* az elfogott titkosított forgalmak tartalmához kizárólag a titkosítás feltörését követően lehet hozzáférni.
- *Beruházási igény:* rendkívül magas, az összes vizsgált módszer esetében messze a legmagasabb.
- *Egyéb költségek:* közepes, a módszer alkalmazásához nem kellenek külön speciális tudással rendelkező szakemberek, de külső közreműködőket, azok költségeit (pl. infrastruktúraszolgáltató beruházásai) a helyi jogszabályoknak megfelelően esetleg fizetni kell.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* ennek lehetősége minimális.

Együttműködés a szolgáltatóval:

- *Az egy időben ellenőrizhető célszemélyek száma:* tömeges ellenőrzést tesz lehetővé.
- *Az ellenőrző eszköz működési módja:* passzív módszer, a dekonspiráció veszélye alacsony.
- *A módszer jogi hátterének rendezettsége:* a módszerre nincsenek mindenki által elfogadott jogszabályok, az alkalmazásszolgáltatók általában nem hajlandóak együttműködni.
- *Az ellenőrző eszköz célszemélyhez való közelsége:* a célszemélytől (infokommunikációs eszközeitől) távol működik.
- *A módszer alkalmazásának technikai problémái:* az alkalmazásszolgáltató együttműködése esetén problémamentes.
- *A hozzáférhető adatok köre:* csak az online forgalomhoz és a szolgáltatónál tárolt adatokhoz, információkhoz biztosít elérést.
- *Online kommunikációhoz való hozzáférés teljes körűsége:* az alkalmazásszolgáltatón keresztül lebonyolított kommunikációhoz teljes körű hozzáférést ad.

- *A módszer alkalmazásának problémái titkosított adatkommunikáció esetén:* a szolgáltató által használt titkosítás ekkor nem jelent problémát, gondot kizárólag a felhasználó által esetleg használt egyedi titkosítás okozhat.
- *Beruházási igény:* alacsony, az összes többi módszernél is jelentkező feldolgozó terminálok kivételével alig igényel plusz eszközt.
- *Egyéb költségek:* közepes, a módszer alkalmazásához nem kellenek külön speciális tudással rendelkező szakemberek, de az alkalmazásszolgáltató beruházásait, vagy adott esetben az adatszolgáltatását a helyi jogszabályoknak megfelelően esetleg fizetni kell.
- *Célszemélyek adataihoz harmadik fél hozzáférése:* magas, ma még sokszor emberi beavatkozással működik az adatszolgáltatás és a kommunikáció ellenőrizhetővé tétele is, ráadásul a kérésekben foglalt érzékeny vagy akár minősített adatokhoz (pl. célszemély adatai) – általában – külföldi szolgáltató hazai biztonsági ellenőrzésen át nem esett emberei férhetnek hozzá, a kérő szerv szemszögéből kontrollálatlanul.

Annak érdekében, hogy az arra felhatalmazott szervek számára a PC/SaaS felhő alapú rendszerek törvényes ellenőrzésére jelenleg rendelkezésre álló módszereket össze tudjuk hasonlítani, célszerű azok előnyeit, hátrányit is összefoglalni. Ezt tartalmazza a következő táblázat.

Módszer	**előnyök**	**hátrányok**
aktív támadó eszköz (kémprogram vagy online házkutatás)	• nem csak az éppen folyó forgalmat, hanem a gépen tárolt minden adatot el lehet érni • titkosítás előtti elfogás – azaz felhasznált titkosítástól függetlenül ellenőrizhető a forgalom	• egyedi ellenőrzés (egy trójai, egy eszköz) • telepítés problémákba ütközhet • célszemély minden eszközére kell telepíteni a teljes körű ellenőrzéshez • aktív, ezért működése adott esetben felfedezhető • működése, működő képessége nagymértékben függ a céleszköz beállításaitól, telepített szoftvereitől (pl. vírusirtó, tűzfal) • működése azonnali utasítással nem megszakítható • alapos előkészületek ellenére a képességet egy egyszerű (pl.: vírusellenőrző) frissítés ellehetetlenítheti • jogszabályi háttere nem egyértelmű
közbeékelődéses támadás (Man in the Middle)	• bizonyos titkosított forgalmaknál is lehetővé teszi a közlemények megismerését (általában SSL, https esetén)	• egyedi ellenőrzés (egy netforgalomra) • más titkosított forgalmak problémát okozhatnak • viszonylag közel kell menni • több eszköz és netelérés esetén problémás (pl. vezetékes és mobil net) • adott esetben a tevékenység felfedezhető • csak az éppen folyó forgalmat lehet vele megismerni • titkosított forgalom esetében az alkalmazónak szükséges hiteles tanúsítvánnyal rendelkeznie • jogszabályi háttere nem egyértelmű
mély csomagvizsgálat (DPI)	• tömeges – egyszerre több célszemély forgalma is ellenőrizhető • teljesen passzív • tartalom alapú szűrést tesz lehetővé • jogszabályi háttere egyértelmű	• nagy beruházási igény • az egyre növekvő sávszélesség miatt egyre gyorsabb, nagyobb sávszélességű elfogókat kell használni • titkosítás problémákat okozhat • adott „csatornán” átfolyó forgalmat elemzi, ha nem ott megy a célszemély forgalma, nem fogja el – nem teljes körű • csak az éppen folyó forgalmat lehet vele megismerni

együttműködés a szolgáltatóval	• tömeges – egyszerre több célszemély is ellenőrizhető • teljes információkör elérhető, használt eszközöktől, neteléréstől függetlenül • nem csak az éppen folyó forgalmat, hanem a szolgáltatónál tárolt minden adatot (pl. piszkozatok) el lehet érni • szolgáltató által alkalmazott titkosítás nem probléma	• a szolgáltatók nem mindig partnerek, csak jogszabályi alapon működik (hatékonyan) • külföldi szolgáltatók felhasználóinak ellenőrzése esetén ráadásul nemzetközi jogszabályok szükségesek • célszemély adatait szolgáltató is megismeri – titoktartási, konspirációs gondot okozhat • több szolgáltatót használó célszemélyeknél mindegyikkel együtt kell működni

1. táblázat. A PC/SaaS felhő alapú rendszerek törvényes ellenőrzésére jelenleg rendelkezésre álló módszerek előnyei, hátrányai

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

A cikksorozat első része – a „Felhő alapú rendszerek törvényes ellenőrzési problémái” című cikkre alapozva – áttekintette a PC/SaaS felhő alapú rendszerek törvényes ellenőrzése kapcsán felmerült problémákat, majd – a teljesség igénye nélkül – megvizsgálta, hogy különböző országok hogyan valósítják meg, vagy legalábbis hogyan próbálják megvalósítani az említett rendszerek törvényes ellenőrzését. A nemzetközi példák bár széles, de nem teljes körű áttekintést adtak. Ennek egyrészt az az oka, hogy csak publikus információkra lehet támaszkodni, azok pedig – az ügy jellegére tekintettel meglehetősen korlátozottak, ráadásul szinte sohasem igazoltak, így nem lehetnek teljes körűek. A másrészt pedig az, hogy a törvényes ellenőrzésre felhatalmazott szervek részére rendelkezésre álló módszerek ismertetéséhez, elemzéséhez egyébként sincs szükség teljes körű áttekintésre.

A cikksorozat második része áttekintette a PC/SaaS felhő alapú rendszereket törvényes ellenőrzésre jelenleg rendelkezésre álló technikai lehetőségeket, majd felállította ezek vizsgálati, összehasonlítási szempontrendszerét. Ezt követően elvégezte a különböző módszerek vizsgálatát, megadta azok előnyeit, hátrányait, és megállapította, hogy a titkos információgyűjtésre felhatalmazott szervek az elemzést követően már nem csak az adott módszer bevezetéséről, rendszeresítéséről képesek dönteni, hanem arról is, hogy egy adott ügyben, adott körülmények között melyik ellenőrző metódus használata a legcélravezetőbb.

Összefoglalásként elmondható, hogy jelenleg több, egymástól technikailag és működés szempontjából is gyökeresen eltérő megoldás áll az arra feljogosított szervezetek rendelkezésére, hogy a PC/SaaS felhő alapú rendszerek kapcsán felmerülő törvényes ellenőrzési feladataikat végrehajtsák. Ezek a megoldások azonban annyira újak a törvényes ellenőrzés eszközrendszerében, hogy azok használata sok országban egyáltalán nincs jogilag szabályozva. Más országokban újonnan megjelenő szabályzókkal – sokszor vitatottan, vagy éles bírálatok közepette – vezetik be ezen ellenőrzési formákat, vagy legitimizálják a már működő rendszereket. Megint más országokban pedig a meglévő jogszabályokba próbálják több-kevesebb sikerrel beleérteni, beleerőltetni az új ellenőrzési formákat.

A cikksorozat alapján több következtetés is levonható:

1. A PC/SaaS felhő alapú rendszerek ellenőrzése minden ország törvényes ellenőrzést végző szervei számára kihívást jelentenek.
2. A törvényes ellenőrzést végzők számára több technikai megoldás is létezik a PC/SaaS felhő alapú rendszerek ellenőrzésére.
3. Ezen technikai megoldások jogi megítélése kétséges.
4. Nincsen olyan általánosan elfogadott jogi szabályozás a PC/SaaS felhő alapú rendszerek ellenőrzése kapcsán, amelyhez – akár Magyarországnak is – igazodni lehetne.
5. A fent leírt módszerek egyike sem nyújt teljes körű megoldást a nemzetbiztonsági és rendvédelmi szervek által törvényes ellenőrzés keretében igényelt adatok megszerzéséhez.
6. A törvényes ellenőrzésre felhatalmazott szervezeteknek – alkalmazkodva a törvényi keretekhez, a célszemély által használt eszközökhöz, szolgáltatásokhoz, a célszemély kommunikációs szokásaihoz, a műveleti helyzethez és az egyéb (pl. infrastruktúraszolgáltató által használt) technikai feltételekhez – több, esetleg minden ellenőrzési módra fel kell készülniük, és az azokhoz szükséges eszközöket be kell szerezniük.
7. Az alkalmazásszolgáltatóval való együttműködés az egyik leghatékonyabb és legköltség-takarékosabb ellenőrzési forma, így ez kikerülhetetlen, ugyanakkor ennek jogi szabályozottságában lelhető fel a legtöbb hiány. Így ma gyakorlatilag a legtöbb ország – így Magyarország – esetében is kizárólag az alkalmazásszolgáltató jóindulatán múlik, együttműködik-e az ellenőrzést végző szervekkel, és teljesíti-e – az egyébként teljesen legális, hatályos és pl. a hírközlési szolgáltatók számára (is) kötelező érvényű bírói végzésben foglaltakat.
8. 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 eljárásokat és – a várhatóan csak azt követő – 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.

Annak érdekében, hogy a PC/SaaS felhő alapú rendszerek törvényes ellenőrzési problémáit kezelni lehessen, a „Felhő alapú rendszerek törvényes ellenőrzési problémái” című cikk az összefoglalás és következtetés részben meghatározott néhány, további elvégzendő feladatot. Ezek közül jelen cikksorozat a másodikra ad választ, azaz áttekintette és összehasonlította az említett rendszerek törvényes ellenőrzésére jelenleg rendelkezésre álló technikai eszközöket és módszereket, azok előnyeivel, hátrányaival együtt. További feladatként, a jogi szabályozás kialakítása előtt, el kell végezi az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmának a definiálását. Majd ezt követően lehet meghatározni, hogy mit kell ellenőrzés alá vonni ahhoz, hogy a nemzetbiztonsági és a bűnüldözői munkát hatékonyan lehessen a támogatni, és ezek alapján célszerű a törvényi szabályozást átalakítani.

Felhasznált irodalom

[1] Chaos Computer Club analyzes government malware (2011. 10. 08.) http://ccc.de/en/updates/2011/staatstrojaner (2013.06.24.)

[2] Sergey Golovanov: Spyware. HackingTeam (2013. 04. 23.) http://www.securelist.com/en/analysis/204792290/Spyware_HackingTeam 2013.06.28.)

[3] Morgan Marquis-Boire - Bill Marczak - Claudio Guarnieri - John Scott-railton: For their eyes only (2013.05.01.) https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf (2013.06.28.)

[4] DEFINITION: spyware (2006. október) http://searchsecurity.techtarget.com/definition/spyware (2013.07.16.)

[5] Spyware http://www.spywareguide.com/term_show.php?id=12 (2013.07.16.)

[6] Chris Sanders: Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1) (2010. 03. 17.) http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html (2013.07.16.)

[7] Chris Sanders: Understanding Man-In-The-Middle Attacks – Part2: DNS Spoofing (2010. 04. 07.) http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html (2013.07.16.)

[8] Chris Sanders: Understanding Man-In-The-Middle Attacks - Part 3: Session Hijacking (2010. 05. 05.) http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part3.html (2013.07.16.)

[9] Chris Sanders: Understanding Man-In-The-Middle Attacks - Part 4: SSL Hijacking (2010. 06. 09.) http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html (2013.07.16.)

[10] Dennis Fisher: What is a Man-in-the-Middle Attack? (2013. 04. 10.) http://blog.kaspersky.com/man-in-the-middle-attack/ (2013.07.16.)

[11] Man-in-the-Middle Tutorial: Learn About Man-in-the-Middle Attacks, Vulnerabilities and How to Prevent MITM Attacks http://www.veracode.com/security/man-in-the-middle-attack (2013.07.16.)

[12] Alex Wawro: What Is Deep Packet Inspection? (2012. 02. 01.) http://www.pcworld.com/article/249137/what_is_deep_packet_inspection_.html (2013.07.19.)

[13] Ido Dubrawsky: Firewall Evolution - Deep Packet Inspection (2010. 11. 02.) http://www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection (2013.06.28.)

[14] BEREC preliminary findings on traffic management practices in Europe show that blocking of VoIP and P2P traffic is common, other practices vary widely http://berec.europa.eu/doc/2012/TMI_press_release.pdf (2013.06.28.)

[15] Alex Wawro: A simple guide to Deep Packet Inspection (2012. 02. 01.) http://features.techworld.com/security/3334780/a-simple-guide-to-deep-packet-inspection/ (2013.06.28.)

[16] Ellen Messmer : US government's use of deep packet inspection raises serious privacy questions (2013. 04. 24.) http://news.techworld.com/security/3444019/dhs-use-of-deep-packet-inspection-technology-in-new-net-security-system-raises-serious-privacy-questions/ (2013.06.28.)

[17] NSA slides explain the PRISM data-collection program (2013. 06. 29.) http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (2013.06.28.)

[18] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball: GCHQ taps fibre-optic cables for secret access to world's communications (2013. 06. 21.) http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (2013.07.05.)

Ábrák jegyzéke

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Póser Valéria, Schubert Tamás, Kozlovszky Miklós, Prém Dániel
poser.valeria@nik.uni-obuda.hu - schubert.tamas@nik.uni-obuda.hu -
kozlovszky.miklos@nik.uni-obuda.hu - prem.daniel@nik.uni-obuda.hu

SECURITY ON-DEMAND MEGOLDÁSOK AZ INFORMATIKAI INFRASTRUKTÚRÁKBAN

Absztrakt

A modern informatika egyre inkább a szükséglet-alapú megoldásokra törekszik. Nincs ez máshogy az informatikai biztonság területén sem. Napról napra jelennek meg új felhőszolgáltatások, amelyeket akár percek alatt használatba lehet venni. Ezzel kielégítve a piac azon igényét, hogy az előfizetők a lehető legtöbb és legjobb szolgáltatásokat a lehető leggazdaságosabban vehessék igénybe szükségletüknek megfelelően. Kutatásunk során megvizsgáltuk a jelenleg elérhető Security as a Service megoldásokat, majd górcső alá vettük azok On-Demand módon történő alkalmazhatóságát, támaszkodva a területen élenjáró Security On-Demand szolgáltató megoldásaira. Cikkünkben ezeket mutatjuk be, külön kitérve olyan témakörökre, mint a sebezhetőség vizsgálat, a behatolás érzékelő rendszer és a tűzfalszabályok és megfelelőség elemzése. A megvizsgált módszerek tapasztalatait pedig felhasználtuk a TÁMOP-4.2.1.B-11/2/KMR-2011-0001 "Kritikus infrastruktúra védelmi kutatások" projekt keretében a saját sérülékenység vizsgálati eszközünk fejlesztése során.

The modern information technology is seeking to use on-demand solutions. This is not different in the field of information security. Day by day appears new cloud based services, which are could be usable within minutes. With this, it satisfies the needs of the market to get the most and the best services, on the cheapest price that is possible. During our research we examined the currently available Security as a Service solutions, and we have looked at their applicability in the way of On-Demand, relying on the Security On-Demand service provider's solutions. In this paper, these solutions will be described and paying special attention to such topics as vulnerability assessment, intrusion detection systems and firewall rules and compliance assessment. The experiences of the examined methods are used in the TÁMOP-4.2.1.B-11/s/KMR-2011-0001 "Critical infrastructure protection research" project, where we develop our vulnerability analysis and assessment tool.

Kulcsszavak: *szükséglet-alapú biztonság, felhő-alapú szolgáltatások ~ Security On-Demand, Cloud Based Sevices*

BEVEZETÉS

A modern szükséglet-alapú számítási megoldás (On-Demand Computing) egyre népszerűbb a nagyvállalatok körében. Terjedésének legfőbb oka, hogy ez a technológia lehetőséget biztosít arra, hogy a számítási erőforrások akkor és olyan mértékben álljanak az ügyfél rendelkezésére, amennyire éppen szüksége van. Azaz, ez a megoldás hatékonyan képes kezelni az erőforrások keresletében bekövetkező ingadozásokat, segítségével elkerülhető, hogy egy adott vállalat informatikai rendszere kihasználatlanul működjön, vagy épp az ellenkezője következzen be, hogy erőforrás hiányában ne legyen képes kiszolgálni a megnövekedett keresletet.

Az erőforrások rugalmas kezelése, mint működési cél, a legjobb szakmai gyakorlat szerinti kritériumok közül a hatékonyságot szolgálják. Elsődleges szempont azonban mindig az intézmény stratégiai céljainak teljesítése. A legoptimálisabb olyan működési biztonság kialakítása, amely a működési célokat a stratégiai célokhoz igazítja [1].

A felhő infrastruktúrákon definiált szolgáltatások napjainkban már lehetővé teszik akár nagyvállalati adatközpontok virtualizált üzemeltetését is. A megfelelő informatikai biztonság kialakításában és fenntartásában jelentős segítséget jelenthet a felhő-alapú biztonság, mint szolgáltatás (Security as a Service - SECaaS) igénybevétele. Segítségével jelentős mennyiségű erőforrás (infrastruktúra, szakértelem, idő, stb.) takarítható meg. Az On-Demand Computing analógiáján jogosan merül fel az igény az igény-szerinti biztonság, mint szolgáltatás igénybevételére is. A SECaaS nagy előnye abban rejlik, hogy szolgáltatási modelljével képes az IT biztonság esetében elengedhetetlenül szükséges szakértelmet az IT erőforrásokkal (hardver és szoftver környezetek) kombinálva hatékonyan elosztani az ügyfelek között maximalizálva a kihasználtságot és ezáltal minimalizálva a költségeket. Ez a koncepció remekül használható nem csak nagyvállalati környezetben, hanem földrajzilag elszórt kisvállalatok esetében.

Kutatásunk során megvizsgáltuk a jelenleg elérhető Security as a Service megoldásokat, és cikkünkben bemutatjuk a legelterjedtebb, legszükségesebb megoldások On-Demand módon történő alkalmazhatóságát. A megvizsgált módszerek tapasztalatait pedig felhasználtuk a TÁMOP-4.2.1.B-11/2/KMR-2011-0001 “Kritikus infrastruktúra védelmi kutatások” projekt keretében a saját sérülékenység vizsgálati eszközünk fejlesztése során.

SZÜKSÉGLET-ALAPÚ BIZTONSÁGI SZOLGÁLTATÁSOK

A vállalatok arra törekszenek, hogy megfelelő védelemmel rendelkezzenek az informatikai rendszereiket érintő fenyegetések, a jogsértések, és a jogosulatlan hozzáférések ellen, ugyanakkor, ahogy a fenyegetések köre átalakul, a hagyományos biztonsági védekezés egyre kevésbé hatékony. Ez azt jelenti, hogy a vállalatoknak más, esetleg további biztonsági intézkedésre van szükségük, amely kiegészíti a meglévő védelmet. Az egyik legfontosabb szükséges képesség egy robusztus biztonsági ellenőrzési és irányítási képesség, amely képes integrálni a különböző biztonsági technológiákat egy olyan elterjedt decentralizált hálózaton is, ahol távol vannak egymástól a telephelyek, a távmunkások, a mobil eszközök, a csatlakoztatott üzleti partnerek.

A kialakult gazdasági válságnak is köszönhetően a vállalatok legfőbb törekvése a lehető legkevesebb ráfordítással a leghatékonyabb biztonság fenntartása. A megfelelési és kockázatkezelési előírások azonban nincsenek tekintettel a válságra, nem szabnak enyhébb követelményeket, mert a vállalatoknak kevesebb anyagi erőforrás áll rendelkezésükre a bizalmas információk védelmére. Az optimális megoldás az informatikai biztonsági funkciók részben, vagy teljes mértékű kitelepítése (outsourcing) lehet. Egyre több kis-és közepes méretű vállalkozás számára ma ez a szolgáltatás sokkal költséghatékonyabb, mintha a

szükséges biztonsági funkciókat teljesen házon belül oldanák meg. Ugyanis, ha a helyzet úgy kívánja, nem kell foglakozni az időközben feleslegessé vagy esetleg szükségessé vált infrastruktúra, vagy szakember problémával, vagy azzal a gonddal, hogy ha egy informatikai munkatársat elveszít a vállalat, akkor elveszti az ellenőrzését olyan technológiák, területek felett, amelyekért korábban az adott munkatárs felelős volt.

Gyakran az informatikai személyzet meglehetősen túlterhelt, gondot okoznak például a következő kérdések:

- személyzet és szakértelem hiánya az informatikai biztonság területén,
- biztonsági események ellenőrzése 7 x 24 órában,
- a legkülönbözőbb biztonsági technológiák kezelése és támogatása,
- teljesítmény és biztonsági naplók ellenőrzése, elemzése,
- a termékek megfelelő konfigurálásához szükséges szakértelem hiánya,
- szoftver licencek és karbantartási szerződések kezelése, stb.

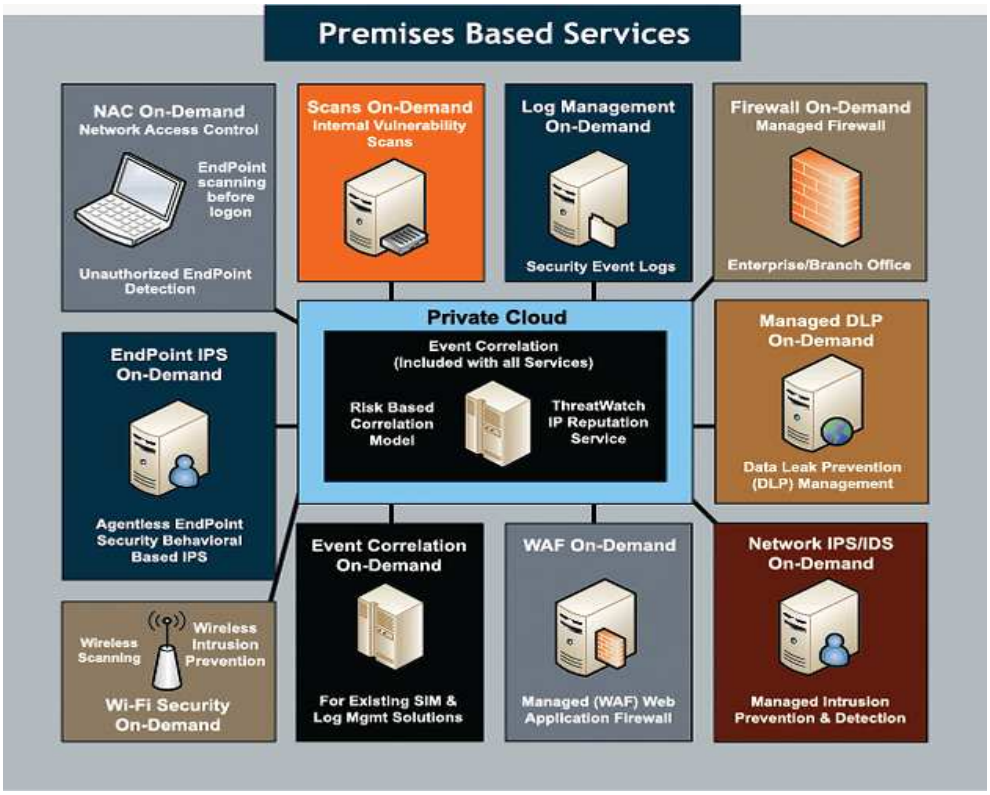
A fenti és hasonló problémák megoldására nyújthat megnyugtató és költségkímélő megoldást a biztonságnak, mint szolgáltatásnak a szükséglet-alapú igénybevétele. Ezért kutatásunk során górcső alá vettük példának okáért a Security On-Demand Társaság által kínált biztonsági megoldásokat.

Security On-Demand lehetőségek

A Security On-Demand nem más, mint a különböző biztonsági szolgáltatások az ügyfelek lehetőségeihez mért és szükségleteinek megfelelő igénybevételi lehetősége. Erre lehetőség van helyileg telepített, felhő-alapú, vagy úgynevezett kevert, vagy hibrid formában.

Telepített szolgáltatások [2]

A telepített biztonsági szolgáltatások (Premises Based Services) célja, a hálózat belső elemeinek integrálása, úgymint a végpontok, szerverek, alkalmazások, biztonsági berendezések és alkalmazások, stb.



1. ábra. Telepített szolgáltatások [2]

Az ebben a formában igénybe vehető biztonsági szolgáltatásokat az 1. ábra szemlélteti, melyek a következők:

1. *Tűzfal menedzselés (Firewall On-Demand):* Csökkenti a vállalat informatikai személyzetének terheit, mert kezel minden tűzfaljelentést, anélkül, hogy egy belső biztonsági szakértőt tartanánk fenn. Különböző megoldás létezik kis- és nagyvállalatok részére, és a különböző típusú tűzfalakat is képes támogatni (pl. Check Point, Cisco, ASA és PIX, Palo Alto tűzfalak, stb.).
   - 24x7 technikai támogatás: többszörösen tanúsított biztonsági és tűzfal mérnökökkel,
   - Compliance & Reporting: segítség a szabályozási követelményeknek való megfelelésben azáltal, hogy azonnal elérhető a tűzfal, valamint biztonsági jelentés készítése arról, amire az informatikai személyzetnek nincs ideje, gyűjtés, kezelés,
   - alacsonyabb költség: kihasználva a Security as a Service megvalósítást, csökken a kezelési és karbantartási költség,
   - ROI: a tűzfal biztonsági frissítéseinek biztosítása, rendszeres karbantartás, állandó biztonsági ellenőrzés, a biztonsági események átláthatósága és a láthatósága a tűzfalon (pl. a Security On-Demand-nál biztonságos internetes portálon naprakész, valós idejű jelentések minden forgalomról, biztonsági eseményekről).

2. *Napló menedzselés (Log Management On-Demand):* A legtöbb napló menedzsment szolgáltatás összegyűjti és összesíti az eseményeket, de valós idejű elemzést nem végez. Azon megoldások esetében, amelyek nem biztosítják ezt a képességet is, külön kell gondoskodni róla, ami jelentős mértékben növeli a költségeket és meghosszabbítja a telepítési és konfigurálási időt. Az a jó napló menedzsment, ami azonnal észleli azokat a biztonsági eseményeket, amelyeket további elemzésre kell küldeni, míg a többi naplót tömöríti archiválás céljából.

3. *Belső sérülékenység vizsgálat (Scans On-Demand):* A Scans On-Demand proaktívan vizsgálja a hálózat sebezhetőségét a belső vagy külső támadásokkal szemben. A vállalatoknak gyakran nincs idejük és erőforrásuk az összes támadási felület felderítésére, mivel a hálózati és alkalmazási környezet állandóan változik, így új támadási felületek keletkeznek. A proaktív sebezhetőség tesztelés és behatolás tesztelés segít felderíteni, hogy hol és hogyan képes a támadó olyan kritikus információkat szerezni a rendszerről, amelyek megkönnyítik a behatolást a külső védelmen keresztül. A sérülékenység menedzsment folyamata hat fontos lépcsőből áll: magában foglalja a hálózaton megtalálható eszközök teljes körű felderítését, ezek osztályozását a könnyebb menedzselhetőség érdekében, a vizsgálat folyamatát, a jelentést, amiből kiderül a kockázat, a sérülékenységek kijavítását, illetve a megfelelő kontrollok bevezetését, valamint a javítások ellenőrzését.

4. *Web Application Firewall (WAF On-Demand):* A valós idejű, folyamatos internetes alkalmazások biztonságát a környezet megfelelő védelme mellett az garantálná, hogy a tervezésük és az implementálásuk kellő körültekintéssel, a megfelelő biztonsági elemek, előírások figyelembevételével történt. Azonban az idő múlásával folyamatosan új sérülékenységek kerülnek napvilágra, amelyek az alkalmazások megszületésekor még nem is léteztek. Ezért fontos, az alkalmazások folyamatos 24x7x365 biztonsági ellenőrzése, hiszen egy új biztonsági rés komoly problémákat okozhat, amelyek akár információszivárgáshoz is vezethetnek. Egy biztonsági hiba utólagos javításának költsége sok esetben csillagászati összegeket emészthet fel, hiszen az alkalmazást akár alapjaiban is módosítani kellhet, és a biztonsági

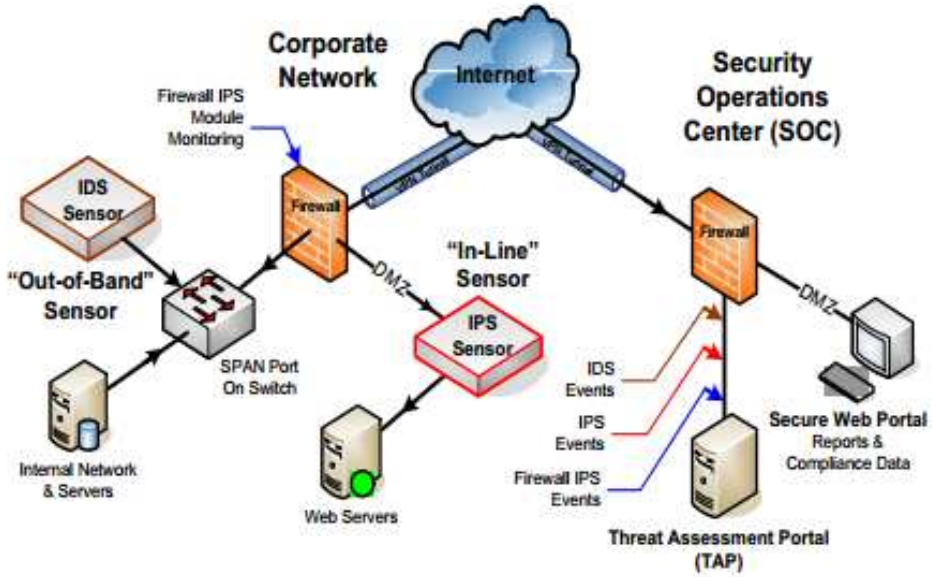
teszteléseket is újra el kell végezni. Emiatt sokkal költséghatékonyabb magoldás lehet egy Web Application Firewall alkalmazása, amelybe csak egy új szabályt kell definiálni a felmerült sérülékenységre.A legtöbb probléma, amiért, és ami ellen védekezni kell:

- a webes alkalmazások az első számú forrása a célzott hacker támadásoknak,
- a célzott alkalmazás támadások általában megkerülik vagy átmennek a tűzfalakon,
- a hálózati biztonsági szkennerek többnyire nem ismerik fel az alkalmazások hibáit, gyengeségeit,
- túl sok a kód és kevés a gyakorlott fejlesztő, aki tudja javítani azokat az alkalmazásokat, amelyek kódja sebezhető,
- az alkalmazások közötti kapcsolat általában bizonytalan.

5. *Wi-Fi biztonság (Wi-Fi Security On-Demand):* A vállalatok hálózati forgalmának egyre nagyobb része „közlekedik a levegőben", és egyre több informatikai eszköz rendelkezik WiFi képességgel, amelyek számos támadási lehetőséget jelentenek. Sok szervezet nem fordít kellő figyelmet és energiát a vezeték nélküli rendszereire, amikor biztonsági technológiát épít ki. A vezetékes hálózatoknál széleskörűen alkalmazott IPS megoldások nem védenek a vezeték nélküli támadások ellen, ezek kezelésére speciális WiFi IPS eszközökre van szükség. A vezeték nélküli behatolás védelmi szolgáltatásnak is folyamatos 24x7 biztonsági ellenőrzésnek kell lenni. A szolgáltatásnak alapos elemzést kell végeznie valamennyi vezeték nélküli csatornára, eszközre, forgalomra. Proaktívan kell azonosítani az összes lehetséges vezeték nélküli fenyegetést, köztük több száz biztonsági rést.

6. *Network Acces Control (NAC On-Demand):* A NAC számos forgatókönyvet tartalmaz a potenciális biztonsági események bekövetkezésekor végrehajtandó lépésekre, amelyek segíthetnek megoldani a valós biztonsági problémákat. Konzultációk alkalmával lehet tisztázni a biztonsági kérdéseket és célokat, amelyek a NAC-ba kerülnek, pl. milyen biztonsági politikát szeretnénk érvényesíteni, milyen megfelelőségi követelményeknek kell eleget tennünk, milyen felhasználói hitelesítés felel meg legjobban számunkra, hogyan kezelje a nem megfelelő felhasználókat, vannak-e illetéktelen hozzáférési végpontok a hálózathoz, stb.

7. *Behatolás jelző rendszer (Network IPS/IDS On-Demand):* A behatolás jelző IDS és IPS szolgáltatás célja, hogy védje a hálózatot a külső és belső támadásoktól. Ma már minden vállalatnak rendelkeznie kell vele, hiszen ez a védelem kritikus pontja. A rosszindulatú adatküldést nehéz kimutatni, mert sokszor téves riasztások is vannak. Ezért nagy szakértelem kell, az ilyen riasztások kiszűréséhez. A behatolás jelző rendszer segít kezelni az információlopás kockázatának észlelését, és meghiúsítja a támadásokat. A megoldás alapja egy 3-rétegű architektúra, amely gazdaságos, kis helyigényű a telepítés, azonban könnyen skálázható nagyszabású telepítések támogatására. Két érzékelőt telepítenek, egy IPS szenzort “in-line” és egy IDS szenzort “out-of-band”, ahogy a következő ábrán látszik.



2. ábra. 3 rétegű architektúra [3]

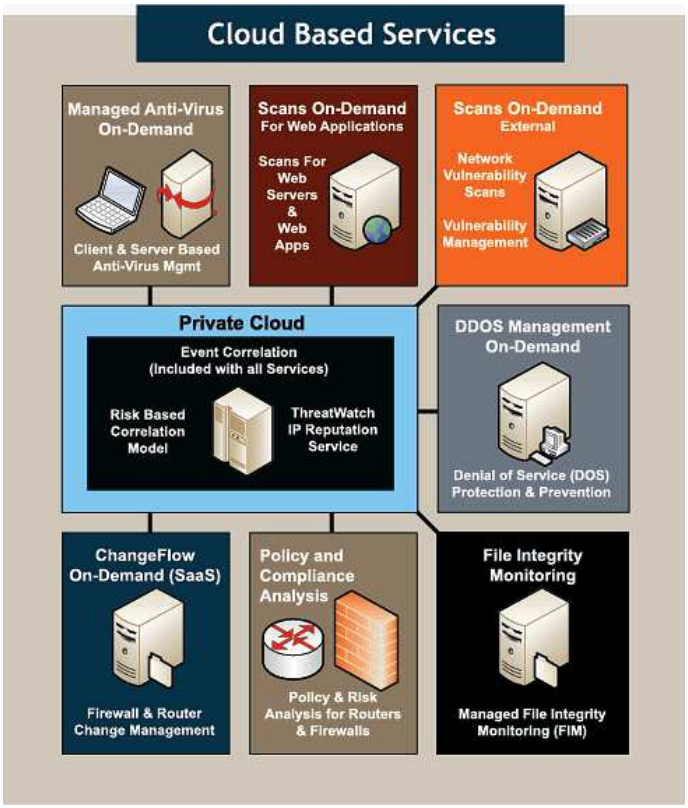
8. *Esemény menedzselés (Event Correlation On-Demand:* Az esemény menedzsment szolgáltatás az informatikai biztonság alapvető építő eleme, egy átfogó szolgáltatás, melynek segítségével csökkenthető a szervezetek üzleti kockázata és működési költsége. A SIM/SIEM rendszerek gyűjtik és elemzik az infrastruktúra, az eszközök, az alkalmazások naplóit, és ha fenyegetést, csalást, vagy visszaélést észlelnek, reagálnak azokra.

9. *Végpont IPS megoldás (EndPoint IPS On-Demand):* Érzékeli a viselkedési anomáliákat, elemzi a végpont együttműködését más rendszerekkel, milyen szolgáltatások futnak az asztalon, észleli a végpont kockázatos magatartását, és ellenőrzi az előre meghatározott végponti politikák végrehajtását. Az ismeretlen felhasználóknak megtagadhatja a hozzáférést attól függően, hogyan van beállítva. Azok a végpontok, amelyek viselkedése sérti a politikát, vagy nem egy vállalati eszköz, korlátozni lehet elkülönítés nélkül, vagy el lehet távolítani a felhasználót a hálózatról. Egyes végponti IPS megoldások képesek felismerni és szétválasztani az ismert és ismeretlen szervezet eszközeinek minden IP alapú eszközét, beleértve a laptopokat, számítógépeket, nyomtató szervereket, forgalomirányítókat, vezeték nélküli hozzáférési pontokat, vagy bármely hálózati eszközt. Előre meghatározott politika alapján az ismeretlen készülékeket vagy felhasználókat, vagy azonnal karanténba teszik, és nem engedik a hálózatra, vagy lehet vendégnek nyilvánítani és csak internet-hozzáférést biztosítani számukra.

10. *DLP megoldás (Managed DLP On-Demand):* A Data Leak Protection (DLP) megoldások egyre elterjedtebbek. Az érzékeny adatok, mint pl. a hitelkártyák, társadalombiztosítási számok, vevőlisták, egészségügyi nyilvántartások, biztosítási információk, címek és más hasonló információk véletlen szivárgásának vagy szándékos kiszivárogtatásának megakadályozására számos eszköz vehető igénybe. Minden megoldás középpontjában az adatosztályozás áll, azaz hogy képesek legyünk meghatározni, hogy milyen típusú adatokat kell megvédeni, és különbséget tenni az ügyfelek adatainak típusai között, mely alapján létre lehet hozni egy politikát a nyomon követésre és az információ szivárgás védelmére. Bár az adatok osztályozása nem elő követelmény, de egy jól definiált adatosztályozási politika kiindulási pont lehet.

Felhő-alapú szolgáltatások [4]

A felhő-alapú biztonsági szolgáltatások (Cloud Based Sevices) kiegészítik a telepített biztonsági szolgáltatásokat, céljuk, hogy integrálják a hálózat külső elemeit, mint pl. a web szerverek, tűzfalak, szerverek, alkalmazások, webes tartalom és sérülékenység elemző eszközök, ezáltal nyújtva olyan átfogó biztonsági stratégiát, amely megvédi a szervezetet az összes lehetséges támadási módszertől.



3. ábra. Felhő-alapú szolgáltatások [4]

Az ily módon igénybe vehető biztonsági szolgáltatásokat a 3. ábra szemlélteti, melyek a következők:

1. *Vírusvédelem (Managed Anti-Virus On-Demand):* Az informatikai rendszerek és azon keresztül a vállalatok zökkenőmentes működésének egyik kritikus pontja a vírusvédelem. Ha az aktuális frissítés nem töltődik le időben, abból katasztrófa alakulhat ki. A víruskereső rendszerek log adatainak gyűjtését és figyelemmel kísérését legtöbbször figyelmen kívül hagyják a szervezetek. A megoldás lényege, hogy a beépített vírusvédelemnek köszönhetően a riasztási üzenetek, figyelmeztetések a szolgáltató rendszerébe valós időben futnak be, ahol képesek megfelelően kezelni azokat. A szolgáltatás figyeli, hogy a víruskereső frissítési fájlok megfelelően letöltődtek-e, továbbá támogatja a kártevőirtókat (anti-malware), kémprogram irtókat (anti-spyware), együttműködik a helyileg telepített vírusvédelmi termékkel. Teljes nyilvántartást vezet minden riasztásról, vizsgálatról és válaszról.

2. *Webes alkalmazások sebezhetőségének vizsgálata (Scans On-Demand for Web Applications):* A felhasználók korlátozására lehet tűzfalakat használni, azonban a tipikus HTTP és HTTPS protokollokra korlátozott forgalom is hordozhat olyan kódot, amely kihasználhatja a webes alkalmazásokban lévő sebezhetőségeket. Az ilyen sebezhetőségek kihasználása vezethet adat szivárgásához, a webes oldal eltorzításához, vagy más támadásokkal akár kompromittálhatják a létfontosságú

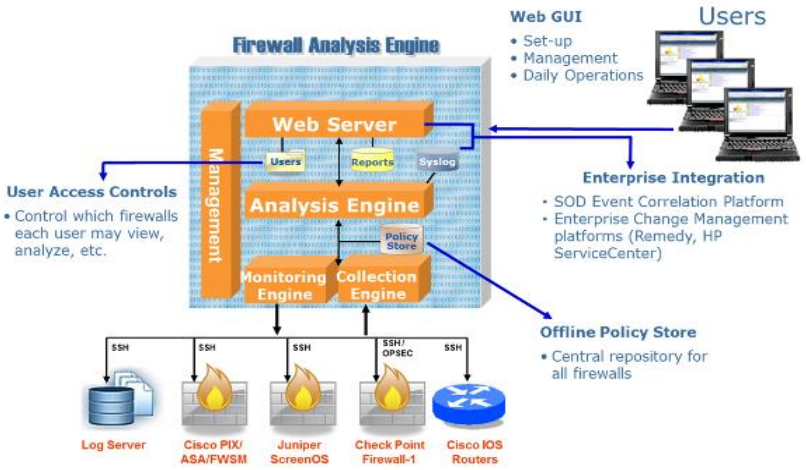
adatok integritását és titkosságát. Legyen szó bármilyen méretű vállalkozásról, ha saját magunk üzemeltetjük a webes alkalmazásainkat, nem árt biztosítanunk a weboldalainkat az alkalmazás szintű fenyegetettségek ellen. A Scans On-Demand for Web Applications szolgáltatás a webes alkalmazásokat és webhelyeket távolról értékeli, a sérülékeny pontokat azonosítja, majd blokkoló szabályokat hoz létre a Web Application Firewall-on (WAF) a feltárt sebezhető pontok alapján.

3. *Hálózati sérülékenység menedzsment (Scans On-Demand External):* A szolgáltatás segítségével proaktív módon azonosíthatók és kiküszöbölhetők a hálózat és összetevőinek sérülékenységei. Korrelálja a sérülékenység vizsgálati adatokat, valós időben elemzi a különböző forrásokból érkező biztonsági eseményeket, beleértve a hálózatot alkotó gépek, szerverek, hálózati eszközök, alkalmazások, adatbázisok, stb. biztonsági naplóit.

4. *DDoS támadás elleni védelem menedzselése (DDoS Management On-Demand):* A DDoS támadás például úgy keletkezik, hogy egy automatizált eszköz (alkalmazás) felkutatja az internetre kapcsolódó sebezhető számítógépeket. Amikor talál olyat, melyet képes megfertőzni, feltelepít egy rejtett támadóprogramot, melynek segítségével távolról vezérelhetővé válik egy „mester" gépről (a támadó gépéről). Ha elég gépet fertőzött meg a támadóprogrammal a „mester" állomás jelt ad a „zombiknak", hogy kezdjék meg a támadást a kiszemelt célpont vagy célpontok ellen. Ekkor az összes „zombi" egyszerre elindítja a támadást, és bár egyenként kis mennyiségű adattal dolgoznak, mégis több száz, vagy akár százezer támadó gép esetén a sok kis adatcsomag eredménye hatalmas adatáramlás, mely a megtámadott gép, vagy rendszer ellen irányul. Ha a DDOS Management eszközök visszaélést fedeznek fel, azonosítják a támadót, és kiejtik a támadó forgalmat, állomást vagy tartományt.
5. *Fájl integritás monitorozása (File Integrity Monitoring):* Ez a szolgáltatás a napló menedzsment része, azoknak az eseményeknek a felderítésére szolgál, melyeket a hagyományos napló menedzsment, vagy monitorozó rendszerek, mint a SIM/SIEM rendszerek nem képesek felderíteni. A rendszer konfiguráció, a fájlok, könyvtárak változását monitorozza.

6. *Tűzfalszabályok és megfelelőség elemzés (Policy and Compliance Analysis On-Demand):* Egyedi tűzfalak, tűzfal csoportok, vagy Cisco IOS alapú forgalomirányítók esetében a biztonsági politikák beállításainak ellenőrzésére szolgál. Az elemzés offline módon történik. Átfogó, jól méretezhető, egyszerűen telepíthető és használható szolgáltatás, ami támogatja az elérhető jelentősebb nagyvállalati tűzfal platformokat.

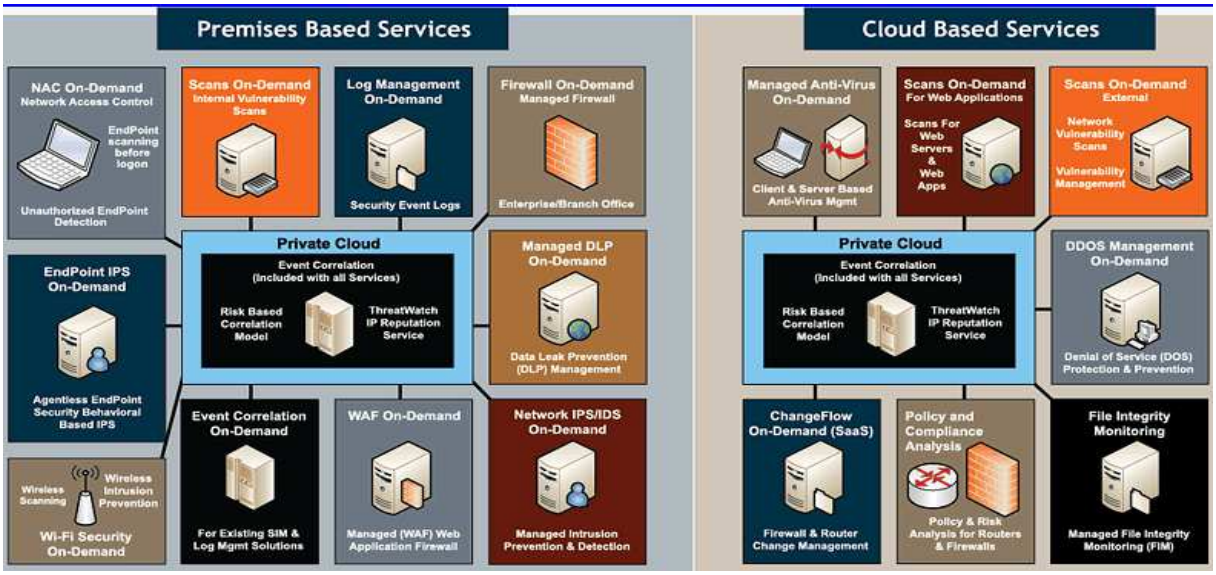
7. *Változás menedzselés (ChangeFlow On-Demand):* A szolgáltatás tűzfalak és forgalomirányítók automatizált változás menedzsment eszköze.



4. ábra. Policy and Compliance Analysis [5]

Hibrid biztonsági architektúra [6]

A hibrid vagy kevert biztonsági architektúra (5. ábra) kihasználja mindkét biztonsági architektúrának (telepített és felhő-alapú) az előnyeit.



5. ábra. Hibrid biztonsági architektúra [6]

A két szolgáltatás típus együttes alkalmazása biztosítja a legjobb telepíthetőséget, szállíthatóságot, és menedzselhető mind a szolgáltató, mind az ügyfél oldalon. Az eredmény egy rendkívül jól méretezhető hibrid biztonsági architektúra, amely nem igényel tőkebefektetést, és enyhíti az informatikai személyzet terheit, 24x7 lefedettséget és menedzsmentet biztosít.

A SECURITY ON-DEMAND MEGOLDÁS ELŐNYEI, ALKALMAZHATÓSÁGA

Az On-Demand felhő-alapú biztonsági szolgáltatások előnyeinek jelentős része a Security as a Service megoldásból származik, és csak bővíti az előnyök körét, hogy ezen szolgáltatások igénybevétele kivitelezhető úgy is, hogy a szolgáltatás díját csupán a valós szükségletnek és lehetőségeknek megfelelően kell megfizetni.

A legfontosabb előnyök tehát:

- *Megszünteti a technológiai tanulási görbét:* egy tipikus szervezet, amikor saját eszközökbe és rendszerekbe fektet be, gyakran tapasztal meredek tanulási görbét a tervezés, a végrehajtás, a konfiguráció terén. Azáltal hogy a szolgáltatás igénybe vétele megszünteti, vagy jelentős mértékben csökkenti az alkalmazottak tanulási görbéjét, a szervezet támogatására, az üzleti műveletekre tudnak összpontosítani.
- *Telepítés gyorsasága:* a technológia kiépítése, az informatikai környezet integrálása meglehetősen költséges. Általában a szolgáltatás teljes telepítése és hangolása kevesebb, mint 30 nap, így felgyorsítja a befektetések megtérülését az ügyfél számára.
- *Költségek (beruházások, szolgáltatási színvonal fenntartása, licencek):* jelentős összeget és folyamatos ráfordítást vesz igénybe a szükséges környezet, az infrastruktúra kialakítása és folyamatos karbantartása, fejlesztése. Számos szervezet nem is rendelkezik kellő anyagi forrással, és nem is lenne gazdaságos a biztonsági szolgáltatások saját kivitelezése. A Security On-Demand biztosítja és fenntartja az összes hardver, szoftver, licencek támogatását, ezek beszerzésére, beüzemelésére, karbantartására, fejlesztésére nem kell erőforrásokat allokálni.
- *Csökkenti a technológiai kockázatot:* költséges technológia beszerzése azzal a kockázattal jár, hogy nem elégíti ki maradéktalanul az elvárásokat. Ekkor a váltás is igencsak költséges. A Security On-Demand megszünteti ezt a kockázatot, minimalizálja a beruházást, az ügyfél a szolgáltatói szerződés megkötése előtt kipróbálhatja a biztonsági technológiát. Ezen kívül lehetőség van a megállapodás megváltoztatására, átalakítására, vagy megszüntetésére, ha a szolgáltatás nem felel meg az elvárásoknak.
- *Személyzeti és biztonsági szakértelem:* nem szükséges vagy lényegesen kisebb mértékben szükséges a megfelelő szaktudású munkatársak alkalmazása, kiképzése. A Security On-Demand kiküszöböli a fluktuáció veszélyét, és megszünteti a képzés költségeit, garantálja a szolgáltatás folyamatosságát.
- *Rugalmas kapacitás tervezés:* lehetővé teszi, hogy az ügyfél csak a ténylegesen igénybe vett szolgáltatásokért fizessen, a körülményekben bekövetkezett változások, legyen az növekedés vagy visszafejlődés, a szolgáltatások köre és mértéke rugalmasan változtatható.
- *Lefedettség:* csak a legnagyobb vállalatok engedhetik meg maguknak, hogy biztonsági szakemberek a nap 24 órájában készenlétben legyenek a biztonságot érintő események figyelésére és az incidensek elhárítására. Ennek hiányában a szervezetek vagy figyelmen kívül hagyják azokat a biztonsági eseményeket, amelyek nem munkaidőben keletkeztek, vagy az informatikai személyzet osztályozza a biztonsági eseményeket, és órák után kerülnek a figyelmeztetések továbbításra. Mindkét stratégia jelentős kockázatot jelent a szervezetnek azáltal, hogy nagy a munkaidőn kívüli lefedetlen idő rés. A Security On-Demand redukálja ezt a kockázatot, a szolgáltatások igény esetén 24x7x365 elérhetőségűek.

A Security On-Demand alkalmazhatósági területei:

- *Kis- és közepes méretű vállalkozások:* A technológia ebben a szektorban alkalmazható leginkább, mivel az általa biztosított szolgáltatások itt biztosítják költséghatékonyan a megfelelő biztonságot (szakértelem hiány megszüntetése, rugalmas, igényekhez igazodó infrastruktúra és szolgáltatás igénybevételi lehetőség, stb.)

- *Pénzügyi szolgáltatók:* Talán ebben a szektorban a legjelentősebb a különböző szabályozásoknak való megfelelés. Vannak azonban többszörös és egymást átfedő szabályozó testületek, szabványok, irányelvek, jogi követelmények és közzétett iránymutatások, amelyek között esetenként nincs szinkron. Ilyen előírások és követelmények beépítésével az On-Demand biztonsági szolgáltatások közé, jelentősen megkönnyíthető e szervezetek biztonságos működése.
- *Egészségügy és kapcsolódó vállalatok:* A Security On-Demand az egészségügyi ágazatban a következőképpen néz ki: Biztonságosan elérhetővé teszi a létfontosságú IP alapú egészségügyi felszereléseket és számítástechnikai eszközöket, védi a külső és belső hálózatot a jogosulatlan használattól vagy a hozzáféréstől. Segíti a megfelelést a HIPAA követelményeknek. Visszajelzést ad a vállalati adatvagyon jogosulatlan elérési kísérletekor. Észleli a rosszindulatú programokat, beleértve a nulladik napi (zero day) fenyegetéseket, botneteket, keyloggereket, trójaiakat, férgeket és vírusokat.
- *Kormányzati kritikus infrastruktúrák és oktatás:* A kormányzati és más közintézmények is egyre nagyobb mértékben szembesülnek biztonsági fenyegetésekkel, azonban gyakran itt áll rendelkezésre a legkevesebb forrás a megfelelő védelem kialakítására, fenntartására. A kritikus infrastruktúrák sok esetben egységesített, illetve ezeken felüli speciális biztonsági megfelelősségekkel rendelkeznek. Ezek központosított, megfelelő szakmai színvonalú ellenőrzése költséghatékonyságot és magasabb minőséget eredményezhet. Azonban a technológia még viszonylag gyerekcipőben jár, nem kellő mértékű szabályozottsága, és nem utolsó sorban az adatok határokon átnyúló akár csak ideiglenes tárolása (esetleg más szabályozás van érvényben) óvatosságra int ebben a szektorban.

ÖSSZEGZÉS

A vállalatok, szervezetek számára a felhő technológiák alkalmazása nem csak költségvetési szempontból előnyös, hanem az informatikai rendszereik biztonsági előírásoknak, szabványoknak való megfelelőségi szintje is jelentősen javul. Nagyobb mértékben tudnak az alapvető üzleti tevékenységeikre koncentrálni, mivel kihelyezhetik azokat a rutinfeladatokat, amelyek csak megterhelik a költségvetést, de nem hoznak többletértéket, és így biztosak lehetnek abban, hogy valamennyi törvényi, megfelelőségi előírásnak eleget tesznek. A szolgáltatásokat biztosító szolgáltató szervezetek megbízhatóságának garantálása az egyik sarkalatos pontja a biztonsági feladatok kihelyezésének, virtualizálásának. A szolgáltató működésének megfelelő átláthatósággal, ellenőrizhetőséggel kell rendelkeznie, melyeket szigorú, folyamatosan ellenőrzött tanúsítványokkal kellene igazolni.

KÖSZÖNETNYILVÁNÍTÁS

A szerzők ezúton mondanak köszönetet a TÁMOP-4.2.1.B-11/2/KMR-2011-0001 „Kritikus infrastruktúra védelmi kutatások” projektnek a cikkhez végzett kutatások anyagi támogatásáért. A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Felhasznált irodalom

[1] K. Szenes: Operational Security - Security Based Corporate Governance, in Proc. of IEEE 9th International Conference on Computational Cybernetics, July 8-10, 2013 Tihany, Hungary, pp. 375-378, IEEE Catalog Number: CFP13575-USB (pendrive); CFP13575-PRT (printed), ISBN: 978-1-4799-0061-9 (pendrive); 978-1-4799-0060-2 (printed)

[2] Security On-Demand: Premises-Based Security Services, http://www.securityondemand.com/Services/PremisesSecurity/index.htm, 2013.05.16

[3] Security On-Demand: Intrusion Monitoring On-Demand, http://www.securityondemand.com/images/datasheets/IM.pdf, 2013.06.06

[4] Security On-Demand: Cloud-Based Security, http://www.securityondemand.com/Services/CloudSecurity/index.htm, 2013.06.23

[5] Security On-Demand: Firewall Policy and Compliance Analysis http://www.securityondemand.com/Services/CloudSecurity/PolicyAndCompliance.htm, 2013.07.15

[6] Security On-Demand: Security Architecture Overview http://www.securityondemand.com/SolutionCenter/SecurityArchitecture.htm, 2013.07.15

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Rajnai Zoltán
rajnai.zoltan@uni-nke.hu

EGY KIKÜLÖNÍTETT, SPECIÁLIS FELADATTAL ELLÁTOTT VEGYI-BIOLÓGIAI CSOPORT KÉP-, HANG- ÉS ADAT-KOMMUNIKÁCIÓJÁNAK LEHETŐSÉGEI

Absztrakt

A Nemzeti Közszolgálati Egyetem konzorciumban a Honvédelmi Minisztérium Elektronikai, Logisztikai és Vagyonkezelő Zrt.-vel (a továbbiakban HM EI Zrt.) kapta azt a feladatot, hogy tervezze meg és készítse el a Telepíthető Gyorsdiagnosztikai Laboratórium (röviden: TGYDGL) átfogó külső és belső kommunikációs és informatikai moduljait, rendszertervét, valamint azokat az eljárásokat modellezze és tesztelje, melyek alkalmazhatók a projekt keretében. A munka első szakaszában (2008-2010) összeállította illetve meghatározta a külső és belső kommunikációs platformmal szembeni funkcionális követelményeket és az egységes megvalósítási koncepciót. A második szakasz első felében (2010-2011) elkészült a belső kommunikációs és informatikai rendszer koncepciója, mely alapvetően a biológiai kontroll-konténer külső információs kapcsolataihoz szükséges rendszer kialakításához kell. Jelen szakaszban (2012. június hó 13. napján hatályba lépett 13. számú szerződésmódosításban foglaltak alapján) a labor külső kapcsolatainak elemzése, modellezése tekintetében szükséges vizsgálni a kikülönítésre kerülő vegyi-biológiai csoport kommunikációját és információs rendszerének összetételét.

The National University of Public Service was given the task to design and prepare a Biological Control Laboratory comprehensive communication and information system design, test and model the context of the project. The project schedule, at the first phase (2008-2010) set out requirements and implementation approach to external and internal communications platform. The first part of the second phase (2010-2011) created the concept of internal communication and information systems. At this part (based on 13th amendments of contract) are the analysis of the laboratory's external communication and modeling field of chemical biology group communication system.

Kulcsszavak: *biológiai, laboratórium, infokommunikáció ~ biological, laboratory, infocommunication*

KIINDULÓ ÁLLAPOT, KÖRÜLMÉNYEK MEGHATÁROZÁSA

A biológiai kontroll feladatokat ellátó laboratórium (továbbiakban: biolabor) külső és belső infokommunikációs rendszerének vizsgálatához fontos meghatározni az alkalmazhatóság, alkalmazás, vezetés és irányítás legfontosabb paramétereit. Az infokommunikációs rendszer szempontjából ugyanis nem elhanyagolható tény, hogy a biolabor hazai vagy külföldi területen kerül „bevetésre", vezetését hazai vagy nemzetközi törzs végzi. Mindezek más-és más követelményeket, kommunikációs platformokat követelhetnek a helyi és csatlakozó hálózatok kialakítására.

A vizsgálat és modellezés tehát kiterjed a csoport munkáját segítő-irányító biolabor vezetőjének felelősségi körébe tartozó, a vezetés-irányítást biztosító hang (beszéd) kommunikációra, a csoport gyakorlati feladat végrehajtását ellenőrizhető képi (mozgó- és állóképi) kommunikációra, valamint a szakmai munkát segítő, a mért adatok gyors eljuttatását biztosító adatkommunikációra. A tanulmány kitér a megvalósíthatóság előnyeire és hátrányaira is. Jelen modellezés elsősorban a kisebb távolságra kiküldött csoport infokommunikációját vizsgálja, egy további tanulmány segíti a nagyobb távolságon dolgozó csoport infokommunikációs rendszerének kialakítását.

Az értékelés módszere

A publikáció értékelő része az infokommunikációs infrastruktúra szolgáltatás-igényű elemzését, az ehhez alkalmazható hálózati elemek felkutatását, vizsgálatát, majd infokommunikációs hálózatba szervezését tartalmazza. Értékelő része összehasonlítja a rendszerelemek, részmodulok és a komplex infrastruktúra szolgáltatásait a kialakítandó kapcsolatok érdekében, javaslatot fogalmaz meg a konkrét megvalósításra.

KIINDULÓ KÖVETELMÉNYEK, ALKALMAZÁSI KÖRÜLMÉNYEK

Amennyiben a biolabor környezetéből kikülönített csoport(ok), járőrök, vegyi vizsgáló (felderítő-analizáló) csoportok kiküldése szükséges, úgy azok kommunikációját két szinten is szükséges biztosítani. Egyrészt kapcsolatot kell tartani a konténer vezetésével hang- adat és kép formában, másrészt biztosítani kell a megfelelő minőségű kommunikációt a csoport tagja(i), vagy más csoportok között. Ehhez szükség van a járőr-tagokat megfelelő kommunikációs eszközökkel felszerelni.

Figyelembe véve, hogy a szakmai feladatokat végrehajtó járőr-tagok védőruhában látják el feladataikat, a felszerelésük közé nem célszerű harcászati rádiókat integrálni azok nagy mérete. Súlya és bonyolult kezelhetősége miatt.

A felszerelésbe integrálható eszközök kialakításánál célszerű figyelembe venni:

- - a kommunikációs eszközök szolgáltatásait,
- - az eszközök súlyát, fizikai dimenzióit,
- - a könnyű, egyszerű kezelhetőséget,
- - a komplex, egyidejű infokommunikációs kiszolgálást.

Az infokommunikációs eszközök alkalmazása során figyelembe kell venni azokat a korlátozó tényezőket is, melyek a járőr-tagok védőruházata okozhat. Így:

- - a védőkesztyű alkalmazása,
- - beszélőkészletek védőruha alatti elhelyezése,
- - adás-vételre kapcsolás nehézségei,
- - „szabad kéz" elve: a járőrtagok kezüket szakfeladataik (pl.: mintavételezés) használják,
- - nincs lehetőség, vagy korlátozottan frekvencia-, üzemmód-, stb. váltására.

Az alkalmazási körülményeket és lehetőségeket vizsgálva fontos kiemelni a környezet-alkalmazhatóság-szolgáltatás hármas elvrendszerét.

1. ábra. A hármas elvrendszer egymásra épülése

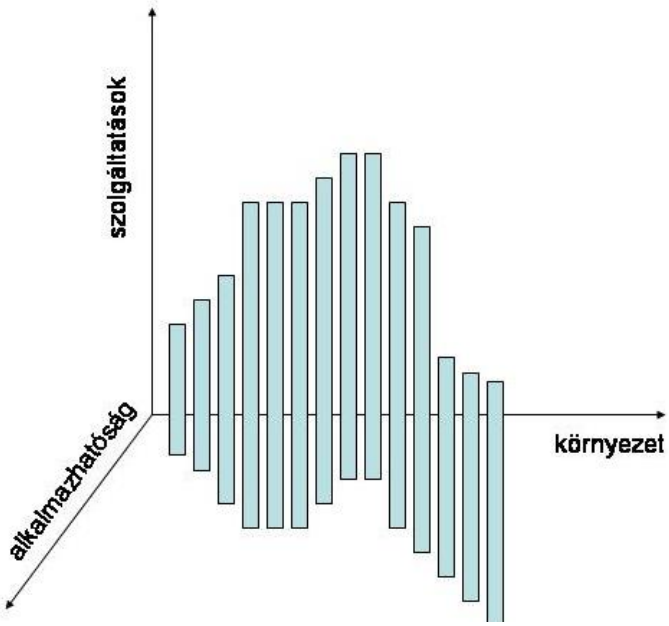
A környezet:
Bonyolult körülménynek, környezetnek számít a járőr tevékenységi területe, feladata, mely befolyásolja az infokommunikációs eszközöket és azok alkalmazását. Amennyiben a járőr előre nem látható környezetben folytat tevékenységet, a *legnagyobb veszély elve* alapján használja egyéni védőeszközeit. Ennek hatása, hogy az infokommunikációs eszközöket csak korlátok között képes a járőr-tag használni.

Az alkalmazhatóság:
Az infokommunikációs eszközök alkalmazhatósága az eszközök külső körülményekhez, környezethez történő adaptálását jelenti, melyeknek összhangban kell lenniük a bonyolult környezeti hatásokkal, és az eszközök által biztosított szolgáltatásokkal. A bonyolult környezet a legegyszerűbb kezelést, ugyanakkor a bonyolultság a legtöbb szolgáltatási igénybevételt indikálja.

A szolgáltatás
A hármas elvrendszer egyik legbonyolultabb eleme. A szolgáltatások rendszere a környezeti hatások függvényében jelenik meg. Minél bonyolultabb körülmények között alkalmazzuk az infokommunikációs eszközöket, annál több, bonyolultabb szolgáltatást rendelünk a felhasználókhoz. A vegyi-biológiai járőr minél bonyolultabb környezetben dolgozik, annál több szolgáltatásra van szüksége. Egy ismeretlen, kiemelten veszélyes környezetben nem csak a beszédkapcsolatra, hanem szükség esetén képtovábbításra, sőt alkalmanként akár adatbázis cserére is igénye lehet a felhasználóknak.

Ez a hármas rendszer tehát csak komplexen kezelhető, nem szabad egyik elemet sem figyelmen kívül hagyni. A környezeti bonyolultság és szolgáltatás mellett az alkalmazhatósági tényezők közösen befolyásolják az eszközök kiválasztását, ételét. Ezek az eszközök ugyanakkor visszahatnak a szolgáltatások jellegére, hiszen az eszközök és az azokból összeállított rendszer rendelkezik azokkal a szolgáltatási lehetőségekkel, melyek alkalmazásra kerülhetnek a járőr bevetése során.

Mindezeket figyelembe véve megállapítható, hogy egyetlen eszközrendszer nem lehet kielégítő a komplex és változó környezethez, ezért egy átlagos környezeti hatásra kialakított rendszer vizsgálatára és modellezésére lehet csak javaslatot kidolgozni opcionális lehetőségek megjelölésével, melyek a környezeti hatásoktól függően fokozzák, vagy csökkentik az alkalmazott eszközök és szolgáltatások körét.



2. ábra. Az alkalmazhatóság-könyezet-szolgáltatás eloszlás ábrázolása

A HANG (BESZÉD) KOMMUNIKÁCIÓ SZERVEZÉSI ÉS TERVEZÉSI ALAPELVEI ÉS ALAPKÖVETELMÉNYEI

A beszédkommunikáció a vegyi csoport és a konténer közötti információcsere alapvető erőforrása, amelyben az információ megszerzésére, továbbítására, feldolgozására, tárolására, rendelkezésre bocsátására és hasznosítására kiemelt figyelmet szükséges fordítani. A hatékony vezetés és feladat végrehajtás érdekében a mindkét csoport híradó és informatikai rendszere kialakításának, működtetésének és alkalmazásának alapelveit a végrehajtandó feladat tervezésének, szervezésének és végrehajtásának teljes időszakában érvényre kell juttatni.

A híradó és informatikai rendszer elemeket, összeköttetéseket, szolgáltatásokat és a logisztikai támogatást minden esetben a feladat jellegének megfelelő szolgáltatások szerint kell megszervezni és biztosítani a járőr és a vezetők (konténer) között.

A híradó és informatikai rendszer kialakítása és működtetése során az alábbi alapelveket, alapkövetelményeket és alapképességeket szükséges érvényesíteni: rendelkezésre állás, szabványosság, reagáló képesség, rugalmasság, manőverező képesség, hitelesség, modularitás, skálázhatóság, vezethetőség, biztonság és védelem, felhasználhatóság, prioritás, információ megosztás, gazdaságosság, adatkonzisztencia.

A *rendelkezésre állás* vagy *megbízhatóság* a rendszernek az a tulajdonsága, hogy meghatározott körülmények között és követelmények alapján képes a híradó és informatikai szolgáltatások folyamatos biztosítására.

A *szabványosság* olyan elv és követelmény, amely a híradó és informatikai rendszerek és berendezések összekapcsolhatóságának és helyettesíthetőségének érdekében az illesztési felületek és berendezések egységesítését irányozza elő. A rendszerek és berendezések szabványossága a kompatibilitás, az interoperabilitás, a felcserélhetőség és az azonosság szintjein valósul meg.

- A *kompatibilitás* egy rendszer vagy berendezés két vagy több elemének, darabjának vagy alkatrészének azon képessége, amely biztosítja, hogy ugyanabban a környezetben való telepítésük, működtetésük egymást nem zavarja.
- Az *interoperabilitás* a híradó és informatikai rendszer azon képessége, hogy szolgáltatásokat tud biztosítani más híradó és informatikai rendszerek számára;

valamint szolgáltatást képes igénybe venni más híradó és informatikai rendszerek részéről..

- A *felcserélhetőség* a híradó és informatikai rendszer azon képessége, amelynek jellemzője, hogy két vagy több rendszer, berendezés fizikai és funkcionális tulajdonsága kivitelben és működésben egyenértékű egymással, maga a rendszer vagy a berendezés – a szabályozás kivételével – átalakítás, módosítás nélkül felcserélhető egymással.
- Az *azonosság* a hasonló és a felcserélhetőség jellemzőivel bíró rendszerekre és berendezésekre vonatkozó minőségi mutató, amely lehetővé teszi, hogy más rendszerekre és berendezésekre kiképzett személy kiegészítő képzés nélkül képes azokat üzemeltetni, üzemben tartani, továbbá azonos javítóanyagok használhatók fel a különböző rendszerek, berendezések számára.
- A *reagálóképesség* vagy *szilárdság* a híradó és informatikai rendszerek azon képessége, amelynek révén a normális működési környezet és körülmények változása esetén - előre prognosztizálható eseményeknek megfelelően - a működés átszervezésével, tartalékok bevonásával és erőforrások átcsoportosításával biztosíthatók a vezetés követelményeinek megfelelő híradó és informatikai szolgáltatások.
- A *rugalmasság* vagy *manőverező képesség* a híradó és informatikai rendszerek azon képessége, amelynek köszönhetően a rendszernek a változó körülményekhez történő megfeleltetése *minimális idő és erőforrás ráfordításával* valósítható meg. A rugalmasság elérhető az eszközfajták és szoftverek számának csökkentésével, az eszközök szabványosításával és csereszabatosságuk biztosításával, alternatív eszközök felhasználásával, a rendszer gondos, előrelátó tervezésével, az eszközök és hálózatok konfigurálásában a szoftveres módszerek alkalmazásával, (lehetőség esetén) a távfelügyelet és távvezérlés alkalmazásával, a polgári hírközlési rendszerek kiegészítésként történő felhasználásával, mobil, szállítható híradó és informatikai rendszerek alkalmazásával vagy előre telepített, aktivizálható rendszerelemekkel.

A hitelesség

- *Alapszinten:* a híradó és informatikai rendszer azon tulajdonsága, amelynek révén képes biztosítani az információk átalakítása, továbbítása, kezelése és tárolása során az információtartalom változatlanságát. A hitelesség alapszintű biztosításának eszközei az előírásoknak megfelelő híradó csatornák biztosítása, ellenőrző és hibajavító berendezések, eljárások és szoftverek alkalmazása, a fontosabb információk többféle híradó eszközön történő egyidejű továbbítása, ugyanazon információ különböző eszközökön történő párhuzamos kezelése és több példányban végrehajtott mentése, információvédelmi eljárások és eszközök alkalmazása.
- *Felsőszinten:* a híradó és informatikai rendszer azon tulajdonsága, amely technikai úton képes biztosítani,
    a) hogy az információt fogadó személy (vezető) meggyőződhessen arról, hogy az információ forrása azonos-e azzal a személlyel, akitől a vezető az információt várja,
    b) hogy az információt fogadó vezető meggyőződhessen arról, hogy az átvitel és kezelés során az információtartalomban módosulás nem következett be. A hitelesség felsőszinten történő biztosítása alapvetően hitelesítési eljárások, módszerek és eszközök révén valósul meg.

A *modularitás* elvének alkalmazása egyes rendszerek, hálózatok vagy berendezések vonatkozásában azt jelenti, hogy

a rendszerelemek és csatlakozásaik szabványosak, valamint funkcionális, kivitelezési, műszaki és logisztikai szempontból egymástól jól elkülöníthetők, ezért hasonló vagy azonos elemmel történő cseréjük egyszerűen és gyorsan végrehajtható.

A *skálázhatóság* elve, illetve képessége

- *alap szinten:* a rendszerelemek szabványosak, és a rendszertől függetlenül maguk is képesek önálló rendszerként hatékonyan hasznosulni alacsonyabb szintű vagy kisebb méretű szervezet (járőr-csoport) feladatainak végrehajtása érdekében egyes alkotórészek elhagyásával, vagy kapacitásuk, funkcióik hardver úton történő korlátozásával.
- *felső szinten:* a rendszer alkotóelemeinek funkciója, működése és kapcsolódási felülete szabványos, amely szoftveres módszerrel paraméterezhető és változtatható, ezért a rendszerelemek szükség esetén egymással helyettesíthetők, felcserélhetők, illetve különböző szintű, méretű és funkciójú rendszerek érdekében hatékonyan alkalmazhatók.

A *vezethetőség* a híradó és informatikai rendszer azon tulajdonsága, hogy a híradásért és informatikai támogatásért felelős vezető a mindenkori helyzetnek megfelelően képes folyamatos ráhatást gyakorolni a híradó és informatikai rendszer üzemeltetésére, az alárendeltek tevékenységére, a híradó és informatikai erők és eszközök célszerű alkalmazására. A híradó és informatikai rendszer vezethetősége feltételezi a rendszerek előrelátó tervezését, a tervek és okmányok naprakészségét, a változásokkal kapcsolatos intézkedések végrehajtókhoz történő időbeni eljuttatását, a rendszermegtervezésében résztvevők célszerű munkamegosztását, céltudatos elemző és ellenőrző tevékenységét, a híradással és informatikai támogatással kapcsolatos nyilvántartások pontos vezetését, a feladathoz megfelelő berendezések rendelkezésre állását, a híradás és informatikai támogatás vezetéséhez szükséges szolgálati összeköttetések biztosítását.

A biztonság és védettség képessége

- *híradó rendszerek esetében:* olyan rendszabályok és eszközök összessége, amelyek alkalmazásával megakadályozható vagy jelentősen csökkenthető az rendszer elleni felderítés és rádióelektronikai zavarás hatékonysága, valamint saját berendezéseink kölcsönös zavarása. A rendszer biztonsága és védettsége a híradó eszközök és az átviteli csatornák fizikai védelmén túl feltételezi a felderítés elleni védelem, a rádiózavarás elleni védelem, és a kölcsönös rádiózavarás elleni védelem megszervezését és rendszabályainak komplex alkalmazását.
- *informatikai rendszerek esetében* olyan rendszabályok, módszerek és eszközök összessége, amelyek alkalmazásával biztosítható az informatikai rendszerek biztonságos és védett működése, amely magában foglalja:
  a) az informatikai rendszerekbe történő illetéktelen behatolás, a rendszer működésének megzavarására vagy bénítására irányuló kísérlet megakadályozását
  b) a szándékos behatolás vagy behatolási kísérlet felfedését, a behatolás következményeinek azonosítását, hatásának lokalizálását és minimalizálását,
  c) a felhasználók nem szándékos, nem előírásszerű tevékenységének káros következményei elleni védelmet
  d) az informatikai rendszerben tárolt adatok illetéktelenek által történő törlésének, módosításának vagy kinyerésének megakadályozását, az idegen, megtévesztő adatok rendszerbe történő juttatásának megakadályozását,

e) az informatikai rendszerelemek és az azt kiszolgáló infrastruktúra fizikai védelmét, a fizikai megsemmisülés következtében fellépő rendszerhiba, működésképtelenség vagy adatvesztés minimalizálását,

A *felhasználhatóság* olyan elv, amelynek alkalmazása a híradó és informatikai rendszer működtetése során biztosítja, hogy az információk a hatékony felhasználásukhoz szükséges helyen, időben, formában és tartalomban kerüljenek rendelkezésre bocsátásra.

A *prioritás* elvének alkalmazása azt jelenti, hogy a tevékenység fontosságának és prioritásának megfelelően kerülnek a híradó és informatikai rendszerek, eszközök és erőforrások átcsoportosításra, alkalmazásra és felhasználásra. A feladat fontosságát és prioritását a vezetés határozza meg.

Az *információ-megosztás* elve azt jelenti, hogy mindazon információt, amelyek konténer szakállománya, kezelői részére meghatározott feladatok végrehajtásához szükségesek - a szükséges mértékben - meg kell osztani függetlenül attól, hogy az a szervezeti hierarchiában és feladatmegosztásban hol foglal helyet.

Az *adatkonzisztencia* elve azt jelenti, hogy kezelőállomány tagjai a tevékenységükhöz szükséges ugyanazon adatokat a híradó és informatikai rendszerből ugyanarról a helyről nyerik. Másként fogalmazva: Ugyanazon adat vagy adatkapcsolat több helyen, több adatgazda felügyelete alatt történő rögzítése, tárolása és rendelkezésre bocsátása kerülendő, hacsak azt a műveleti követelmények szükségessé nem teszik.

A *gazdaságosság* elve azt jelenti, hogy a híradó és informatikai erőket és eszközöket úgy kell meghatározni, csoportosítani és alkalmazni, hogy az a híradó és informatikai támogatás követelmények szerinti megvalósítása a lehető legalacsonyabb munkaidő, erőforrás és költség ráfordítással, a lehető legkevesebb humán, anyagi és eszköz felhasználással kerüljön végrehajtásra.

HÍRADÓ, INFORMATIKAI INFRASTRUKTÚRA

A konténer-*infrastruktúra* kialakítása olyan szolgáltatások nyújtását irányozza elő, amely a felhasználók széles körét érinti tevékenységük jellegétől függetlenül, és sokszor attól függetlenül, hogy az infrastruktúra által nyújtott szolgáltatásokat a felhasználók milyen konkrét cél megvalósítása érdekében kívánják igénybe venni. Ebből kiindulva létezik energetikai infrastruktúra, távközlési infrastruktúra, informatikai infrastruktúra, oktatási infrastruktúra, stb. Az infrastruktúrák általános jellemzője, hogy szabványos kapcsolódási felületen keresztül, viszonylag egyszerűen lehet hozzájuk kapcsolódni, és az általuk nyújtott - korlátozott számú, egységesített - szolgáltatások közül választani, és azt meghatározott paraméterek és minőségi követelmények alapján igénybe venni. Az infrastruktúrák által biztosított szolgáltatásokra támaszkodva speciális, a szervezetek konkrét, speciális igényeit is ki lehet elégíteni, de ez többnyire fejlesztést, vagy kiegészítő tevékenységeket igényel.

A konténer rendszereinek vonatkozásában:

A *híradó és informatikai infrastruktúra* egyrészt biztosítja a szaktevékenységekhez, funkciókhoz rendelt speciális híradó és informatikai alkalmazói szolgáltatások (célrendszerek) működési környezetét, azok műszaki és szoftver alapjait, másrészt fenntartja, működteti és a felhasználók széles köre számára elérhetővé teszi azokat az általános híradó és informatikai szolgáltatásokat, amelyek a konténer és a személyzet számára napi tevékenységük során szervezeti hovatartozásuktól függetlenül szükségesek (informatikai alkalmazások, elektronikus levelezés, telefon, fax stb.).

A *híradó infrastruktúra* a stacioner telepítésű, állandó jellegű híradó rendszer elemeiből – *átviteli csatornák, rendezők, jelformálók, multiplexerek, modemek, mikrohullámú állomások, stacioner műholdvevők, kapcsoló berendezések, adatátvitelt felügyelő berendezések és*

szoftverek, távbeszélő és fax készülékek stb. – tevődik össze. A híradó infrastruktúra alapját képezi a honi területen megvalósított híradó szolgáltatások biztosításának, a nagytávolságú hang, kép és adatátvitelnek, valamint felcsatlakozási lehetőségek biztosításának lehetősége a kitelepített konténer híradó rendszere számára.

Az *informatikai infrastruktúra* tartalmazza az informatikai rendszerszolgáltatásokat, az általános célú alkalmazói szolgáltatásokat, az operációs rendszereket, az informatikai hálózat-felügyeleti eszközöket, a webkiszolgálókat, adatbázis-kezelő rendszereket, a közös felhasználású számítógép szervereket, a számítógép munkaállomásokat, a perifériákat és háttértárolókat, az általános elektronikus biztonsági szolgáltatásokat, valamint az általános alkalmazói szolgáltatásokhoz kapcsolódó, és a felhasználók döntő része által igénybe vett szoftvereket, úgy mint az office-t, vagy a fájlkezelő programokat.

ÖSSZESSÉGÉBEN

A biolabor infokommunikációs környezetét, viszonylatait az alkalmazás, a vezetés és irányítás feladatait végző szervezetek rendszereinek ismeretében célszerű kialakítani. Mielőtt az infokommunikációs csatlakozási felületek kifejlesztése megtörténik vizsgálni szükséges a legfontosabb technológiákat, „versenyeztetni" kell azok szolgáltatás-jellegét, melyek segíthetik a fejlesztési eredményeket. Fontos terület lehet a csatlakozó rendszerekhez történő illesztés, az adat-, kép- és beszédkommunikáció csatornáinak kialakítása kihelyezett művelet időszakában.

A biolabor infokommunikációs rendszerének kialakításán dolgozó kutatócsoport (6-7 fő) feladatát e rendszerben végzi, javaslataival, szakmai véleményalkotásával, tanulmányokkal és publikációkkal segíti a fejlesztést végző szakemberek munkáját.

"A PROJEKT A MAGYAR KORMÁNY TÁMOGATÁSÁVAL, A NEMZETI FEJLESZTÉSI ÜGYNÖKSÉG KEZELÉSÉBEN, A KUTATÁSI ÉS TECHNOLÓGIAI INNOVÁCIÓS ALAP FINANSZÍROZÁSÁVAL VALÓSUL MEG."

Projektazonosító: TGYDGL09

A projekt címe: „Telepíthető gyorsdiagnosztikai laboratórium"

Irodalomjegyzék:

[1] Allen L. Wyatt: Az Internet alapjai, Kossuth Könyvkiadó,-1996 ATM alapismeret:MATÁV jegyzet

[2] Convery, Sean, Miller, Darrin: SAFE: Wireless LAN Security in Depth, Cisco Systems, Inc., San Jose, USA, 2001. pp. 1-48.

[3] Czeiner Antal: A távközlés üzemeltetése 2. Fogalmak és meghatározások. Távközlési Könyvkiadó, 1994.

[4] Daróczy Sz.-Hoványi D-Kováts G: Az IP alapú távbeszélő szolgáltatások menedzselése MAGYAR TÁVKÖZLÉS 2000/2 (XI. évfolyam 2. szám)

[5] Daróczy Sz.-Hoványi D-Kováts G-Szabó R.: A VoIP lehetőségei , MAGYAR TÁVKÖZLÉS 2000/2 (XI. évfolyam 2.szám)

[6] Digital Communications – S. Hankin, Wiley & Sons Inc, New York 1994

[7] Digital Mobile Communications and the TETRA system – John Dunlop & James

[8] Ervine, Wiley & Sons Inc. New York 2001

[9] Farkas Károly: IPv6 – A jövő Internet protokollja? Híradástechnika LX. Évfolyam 2005/10.

[10] Farkas Tibor: A válságreagáló műveletek vezetését és irányítását támogató híradó- és informatikai rendszer megszervezése a Magyar Honvédség többnemzeti műveleteinek tükrében, Doktori (PhD) értekezés, ZMNE, 2010

[11] Fekete Károly: A Magyar Honvédség állandó hírrendszere továbbfejlesztésének lehetőségei, ZMNE:A kommunikáció (híradás) helye és szerepe a vezetés rendszerében, 2000.

[12] Fekete Károly: A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei, doktori (PhD) értekezés ZMNE, 2003.

[13] Fekete, Karoly: IP solutions in the military communications and information systems, „A katonai kommunikációs rendszerek fejlődési irányai –kihívások és trendek a XXI. században", Nemzetközi Szakmai Tudományos Konferencia, Budapest, 2001. november 28.

[14] Fekete, Karoly: Network Enabled Capability with regard to WLAN, „Robot Warfare" Nemzetközi Tudományos Konferencia, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2004. november 24.

[15] Fekete, Karoly: New possibilities in the field of WAN-WLAN military communications, Kommunikáció 2004 Jubilleumi Nemzeközi Szakmai Tudományos Konferencia Különkiadvány, pp. 97-10, ISBN 963 86441 5 X, 2004.

[16] Fekete, Karoly: Personal Military Communications System, Kommunikáció 2002 Nemzeközi Szakmai Tudományos Konferencia Különkiadvány, pp. 55-62, ISBN 963 86229 2 X, 2002.

[17] Fekete, Karoly: Towards a new generation of WLAN in military communications, Kommunikáció 2005 (Communications 2005) tudományos kiadvány, Budapest, 2005, ISBN 963 7060 11 1, Feltalálási hely: Országos Széchenyi Könyvtár, Zrínyi Miklós Nemzetvédelmi Egyetem Tudományos Könyvtár, pp. 334-340.

[18] Fekete, Karoly: VoIP in Military Communications System, A katonai kommunikációs rendszerek fejlődési irányai –kihívások és trendek a XXI. században, Nemzetközi szakmai tudományos konferencia Különkiadás, Zrínyi Miklós Nemzetvédelmi Egyetem, Zrínyi M. kiadó, Budapest, 92-98 oldal, ISBN 963 00 8819 3, 2001.

[19] Földes András, Reich György, Zimányi István: Angol betűszavak feloldó szótára, Távközlési könyvkiadó, 1996.

[20] Kapsch Telecom Kft. A NortelNetworks Pasport 4400 multiszolgáltatású kapcsolója (oktatási anyag) 1999.

[21] Géher Károly: Híradástechnika, Bp., Műszaki könyvkiadó,1993

[22] Grünzweig T.-Sziklai A: Intelligens szolgáltatások IP hálózaton, MAGYAR TÁVKÖZLÉS 2000/5 (XI. évfolyam 5. szám)

[23] Dr. Kovács Oszkár: A keskenysávú ISDN kézikönyve, Távközlési könyvkiadó, 1997.

[24] Kónya László: Számítógép- hálózatok (2 kiadás), LSI

[25] www.nokia.com
[26] www.nokia.hu/halozat/tetra.html
[27] www.tetramou.com
[28] www.etsi.org
[29] www.tetraforum.hu

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Rajnai Zoltán
rajnai.zoltan@uni-nke.hu

A SPECIÁLIS FELADATOT VÉGZŐ BIOLÓGIAI KONTROL-CSOPORT HÁLÓZATÁNAK SZOLGÁLTATÁSAI, HANG- ÉS ADATKOMMUNIKÁCIÓS MEGOLDÁSAI

Absztrakt

A Nemzeti Közszolgálati Egyetem konzorciumban a Honvédelmi Minisztérium Elektronikai, Logisztikai és Vagyonkezelő Zrt.-vel (a továbbiakban HM EI Zrt.) kapta azt a feladatot, hogy tervezze meg és készítse el a Telepíthető Gyorsdiagnosztikai Laboratórium (röviden: TGYDGL) átfogó külső és belső kommunikációs és informatikai moduljait, rendszertervét, valamint azokat az eljárásokat modellezze és tesztelje, melyek alkalmazhatók a projekt keretében. A HM EI ZRt. a projekt ütemtervének megfelelően, a munka első szakaszában (2008-2010) összeállította illetve meghatározta a külső és belső kommunikációs platformmal szembeni funkcionális követelményeket és az egységes megvalósítási koncepciót. A második szakasz első felében (2010-2011) elkészült a belső kommunikációs és informatikai rendszer koncepciója, mely alapvetően a biológiai kontroll-konténer külső információs kapcsolataihoz szükséges rendszer kialakításához kell. Jelen szakaszban a labor külső kapcsolatainak elemzése, modellezése tekintetében szükséges vizsgálni a kikülönítésre kerülő vegyi-biológiai csoport kommunikációját és információs rendszerének összetételét. Cél, hogy a munkaszakasz végére kialakuljon a kikülönített csoport hang-, kép-, és adatkommunikációjának rendszere.

The National University of Public Service was given the task to design and prepare a Biological Control Laboratory comprehensive communication and information system design, test and model the context of the project. The project schedule, at the first phase (2008-2010) set out requirements and implementation approach to external and internal communications platform. The first part of the second phase (2010-2011) created the concept of internal communication and information systems. At this part (based on 13th amendments of contract) are the analysis of the laboratory's external communication and modeling field of chemical biology group communication system.

Kulcsszavak: *biológiai, laboratórium, infokommunikáció ~ biological, laboratory, infocommunication*

A BIOLÓGIAI KONTROL FELADATOKAT ELLÁTÓ KONTÉNER (BIOLABOR) HÍRADÓ ÉS INFORMATIKAI RENDSZEREINEK SZOLGÁLTATÁSAI

A *híradó és informatikai szolgáltatást nyújtó rendszer* a biolabor külső és belső infokommunikációját biztosítja, mely nemcsak a konténerben dolgozók beszéd- és adatcseréjét adja, hanem illeszkedik a környezetében fellelhető (a konténer részére kijelölt) infokommunikációs hálózatokhoz, melyek lehetnek zárt célú hálózatok, vagy akár polgári felhaználású rendszerek is. A szolgáltatások célja a kezelő állomány eltérő feladatainak végrehajtása érdekében alkalmazható olyan egységes információs képesség biztosítása, amelynek alkalmazásával a feladatokat rövidebb idő alatt, kevesebb erőforrás bevonásával és jobb minőségben hajthatók végre, mint a szolgáltatás igénybe vétele nélkül.

A híradó és informatikai szolgáltatás alapvető tulajdonsága, hogy az általa biztosított információs képességeket nem egyetlen személy, vagy kisebb csoport, hanem a konténer állományának meghatározott csoportjai is alkalmazhatják, és annak függvényében, hogy miként történik a szolgáltatás igénybe vételének megszervezése és végrehajtása, a szolgáltatás más-más jellegű szaktevékenységek végrehajtását teszi hatékonyabbá.

A biolabor híradó és informatikai szolgáltatása egy proaktív tevékenység, amelynek eredményei az alkalmazás céljából kiajánlásra kerülhetnek más csatlakozó kormányzati, helyi politikai-katonai, vagy együttműködő szervezet, csoport részére. A szolgáltatások fejlesztésével kapcsolatos követelmények általánosan jellemző információfeldolgozási folyamatok elemzéséből kerülnek meghatározásra az alkalmazók és a híradó-informatikai szakfeladatokat ellátók együttműködése eredményeként, míg a fejlesztési folyamat a híradó-informatikai szakállomány szakmai felügyeletével és operatív irányításával kerül végrehajtásra.

A híradó-informatikai szolgáltatások igénybe vételéről és annak módjáról általános esetben az alkalmazók maguk döntenek, azonban a működési hatékonyság növelése érdekében – *integrált, számítógéppel támogatott információs rendszerek kialakítása céljából, egységes alkalmazási elvek alapján* – elrendelhető számukra egyes szolgáltatás kötelező alkalmazásba vétele, vagy tiltása. A híradó-informatikai szolgáltatások - *azok funkciója alapján* – alkalmazói szolgáltatásra (rövidítve: szolgáltatásra) és rendszerszolgáltatásra tagozódnak.

Az *alkalmazói szolgáltatások* közvetlenül alkalmazható információs képességet biztosítanak a konténer állománya részére, ilyen többek között az elektronikus levelezés, a távbeszélő szolgáltatás, a fájlszerver szolgáltatás, a hálózatba szervezett irodai alkalmazások, a hálózati nyomtatás és szkennelés, a böngészés, a csoportmunka, a videokonferencia szolgáltatás és a faxszolgáltatás. Központi szolgáltatásnak hívják azokat a szolgáltatásokat, amelyek a konténer állományának többsége részére kerülnek biztosításra, és központi híradó és informatikai üzemeltető szervezet biztosítja. Helyi szolgáltatások területi alapon, a funkcionális szolgáltatások alkalmazói tevékenységi jelleg alapján, a szervezeti szolgáltatások a szervezeti hovatartozás függvényében bocsátanak a híradó-informatikai szakállomány rendelkezésére.

A *rendszerszolgáltatások* egyrészt a különböző alkalmazói szolgáltatások részére nyújtanak közös felhasználású híradó-informatikai képességeket és erőforrásokat (nagytávolságú adatátvitel, transzporthálózati szolgáltatás, szerver-kapacitás, háttértár-kapacitás, mentés-archiválás, biztonsági szolgáltatások, hitelesítési szolgáltatás, hálózati erőforrás megosztás stb.), másrészt az alkalmazók speciális feladatainak érdekében működtetett informatikai célrendszerek részére nyújtják ugyanezt. A rendszerszolgáltatások alapvető tulajdonsága, hogy képesek ugyanazokkal az erőforrásokkal és üzemeltetési eljárásokkal integrált módon különböző alkalmazói szolgáltatások és célrendszerek igényeit párhuzamosan kiszolgálni, amely az eszközök, szoftverek és üzemeltetési tevékenységek optimális, hatékony kialakítását és felhasználását teszik lehetővé.

A rendszerszolgáltatások a híradó-informatikai infrastruktúra részét képezik, amelynek alapvető technikai elemei többek között az állandó jellegű híradó rendszer adatátviteli csatornái, csatornaképző és kapcsolóeszközei, a számítógép-szerverpark, a biztonsági és hitelesítő eszközök és szoftverek, a hálózati operációs rendszer, és a közös felhasználású adatbázis-kezelő szoftverek.

A híradó és informatikai szolgáltatásokat központi híradó és informatikai üzemeltető szervezetek nyújtják a szakállomány részére. Ez a szolgáltatási tevékenység tartalmazza a szolgáltatáshoz kapcsolódó üzemeltetési tevékenységek végrehajtását, a változáskezelést, a kapacitásmenedzsmentet, az incidenskezelést, a problémakezelést, a felhasználók részére történő támogatást és segítségnyújtást, a szolgáltatás műszaki fejlesztésének kezdeményezését és felügyeletét, a szolgáltatás-biztosítás humán, képzési, műszaki, logisztikai, pénzügyi követelményeinek és igényeinek megfogalmazását és képviseletét, a felhasználói állománynak a szolgáltatás igénybe vételére történő felkészítését, a képzés megszervezését.

Az alkalmazói és rendszerszolgáltatásokat szolgáltatáskatalógusban kell nyilvántartani, specifikálni és a felhasználók részére kiajánlani. A szolgáltatás specifikációjának tartalmaznia kell a szolgáltatás leírását, tulajdonságait, rendelkezésre állását, biztonsági paramétereit, hozzáférését, a szolgáltatás nyújtás és szolgáltatás igénybevétel határfelületét, a szolgáltatást nyújtó és az azt igénybe vevő személy felelősségét, feladatait. Amennyiben valamely híradó-informatikai üzemeltető szervezet részéről rendszerszolgáltatás biztosítására kerül sor, úgy a szolgáltatás paramétereit és a feleket terhelő kötelezettségeket írásban szükséges rögzíteni.

KÜLSŐ SZOLGÁLTATÁS IGÉNYBE VÉTELE

Híradó szolgáltatások

A *híradó szolgáltatások* polgári szolgáltató szervezetektől történő igénybe vétele a vezetés érdekében objektumok közötti átviteli csatornák és eszközök bérlésével, esetenkénti üzemeltetés-támogatási, karbantartási szolgáltatás igénybe vételével, illetve komplex távközlési szolgáltatások igénybe vételével valósulhat meg. Ilyen lehet pl.: a kormányzati rádiótelefon rendszer (EDR) szolgáltatás igénybe vétele.

Informatikai szolgáltatások

Erősödik a tendencia az úgynevezett *felhő alapú* informatikai szolgáltatás igénybe vételére, vagyis az adatok jelentős részét adattárolás, feldolgozás szempontjából nem helyileg, hanem a világ egy másik pontján végzi azt helyette valamelyik informatikai szolgáltató vállalkozás (*informatikai infrastruktúra, informatikai alkalmazói szolgáltatás*), katonai, vagy kormányzati szervezet.

Ez utóbbi a konténer szempontjából – *ha az kormányzati, vagy honvédelmi célú feladatot hajt végre* - az információs rendszerek esetében nem megengedhető, mert a rendelkezésre állásra, hitelességre, biztonságra és védelemre vonatkozó követelmények eltérnek a polgári szervezetek követelményeitől, illetve az üzleti alapon - *sok esetben más országban* - működő szolgáltatók eltérő érdekek mentén a kormányzati, vagy honvédelmi célú informatikai rendszer működésébe beavatkozhatnának, működését béníthatnák, adatait torzíthatnák, amely a vezetés egészének eredményes tevékenységét – *különösen különleges jogrend alkalmazásának idején* – jelentős mértékben veszélyezteti, szélsőséges esetben lehetetlenné teszi.

HANG- ÉS ADATKOMMUNIKÁCIÓS MEGOLDÁSOK

A hang- és adatkommunikáció szervezéséhez szükséges néhány kiinduló állapot meghatározása. Mivel a konténer alkalmazási, alkalmazhatósági körülményei sokrétűek, így egyetlen, minden körülmény közötti alkalmazhatóság nem határozható meg. Ezért a munkacsoport részére meghatározott alkalmazási körülményt vettem figyelembe. Ennek megfelelően a kitelepített konténertől akár több 10-100 km-re kitelepülő vizsgáló csoporttal számolunk.

Ennek megfelelően feltételezzük, hogy a csoport tagjai között kommunikációs-informatikai szakállomány nem áll rendelkezésre. Ennek azért van jelentősége, mert a készülékek és alkalmazások beállítását a konténertől indulás előtt kell végrehajtani, illetve csak olyan szolgáltatást szabad az elemző csoport tagjai részére biztosítani, melyek egyszer, a személyzet által elvégezhető feladatokat jelent.

„A" VÁLTOZAT: AZ ELEMZŐ CSOPORT TAGJAI KÖZÖTTI KOMMUNIKÁCIÓ:

A hang- és adatkommunikációhoz csoporton belül az egyéni felszerelésbe tartozó könnyű, egyszerűen kezelhető, az URH tartományban üzemelő, hordozható kivitelű, headset-tel rendelkező készülékeket célszerű alkalmazni, mely egyrészt biztosítja a kezelő kommunikációját a kezek használata nélkül, másrészt lehetőséget ad védőöltözetben is jó minőségű hangkommunikáció biztosítására. Megoldási javaslatra a rádiós hozzáférési technológiák közül célszerű választani. Ez a kommunikáció egyszerű alkalmazást, szabad kezeket biztosít a csoport tagjainak. Ilyen eszköz szabad frekvencia felhasználási tartományban üzemel. Elemzéshez a *Kenwood* TK-2180E eszközt találtam legalkalmasabbnak.

A készülék jellemzői:

A beépített 5 hangú jelzésrendszer 12 különböző formátum használatát teszi lehetővé: ZVEI, ZVEI2, CCIR, EIA, EEA, PZVEI, DZVEI, PCCIR, PDZVEI, Natel, AP-369 és a Kenwood saját formátuma. Lehetőség van 6 vagy 7 hangú jelzésrendszer használatára és egyedi többszörös 5 hangú sorozatok küldésére és fogadására is. A felhasználó által egyedileg beállítható adás / vétel formátumok korlátok nélküli jelzésrendszer használatot eredményeznek.

FleetSync® Digitális Jelzésrendszer (adatkommunikáció):
A TK-2180/3180-as rádiók kompatibilisek a Kenwood által kifejlesztett és szabadalmaztatott FleetSync® digitális jelzésrendszerrel, amely alkalmas digitális rádióazonosításra, adatátvitelre és különböző vészhelyzeti működésre. A FleetSync® rendszer további funkciója a státusz üzenetküldés, egyedi vagy csoportos szelektívhívás, rövid / hosszú üzenetküldés és teljes körű GPS kezelés. A 250 férőhelyes szelektívhívó/státusz memória a felhasználó által szabadon particionálható. A készülék alkalmas "FleetSync-II" üzemmódú működésre is, mely esetben az adatátvitel biztonságosabb Forward Error Correction rendszerű hibajavítással egészül ki. Lehetőség van az 5 hangú jelzésrendszer és az FFSK jelek együttes alkalmazására is: a FleetSync rendszer a rövid/hosszú üzenetek küldésére vagy GPS pozíciójelentésre, míg az 5 hang a szelektív hívásra használható.

Transzparens Adatátvitel
A Kenwood által kifejlesztett transzparens adatátviteli módszer lehetővé teszi, hogy a készülékhez soros porton (RS232) keresztül csatlakoztatott személyi számítógépek vagy más terminálok a rádiós csatornán keresztül adatot cseréljenek egymással. Opcionálisan lehetőség van RTS/CTS funkciókkal bővített transzparens adatátvitelre is. A transzparens adatátvitel több új alkalmazás használatát teszi lehetővé pl.: távérzékelés, távvezérlés, mobil okmány ellenőrzés, stb…

Alfanumerikus üzenetküldés (SDM)
A Kenwood által kifejlesztett SDM üzenet a GSM telefonoknál használt SMS üzenetek URH rádiós megfelelője. A készülékhez csatlakoztatott opcionális KMC-36 mikrofon segítségével a felhasználó szabadon írhat üzenetet bármely rádiókészüléknek vagy a diszpécserközpontnak. Az üzenetküldés 5 hangú szelektívhívással is használható funkció.

Beépített inverziós titkosító
A beépített inverziós titkosító használatával megnövelt biztonsági szint érhető el a beszédalapú adások esetén. Az audió jel harmadik személyek számára érthetetlenné válik és csak a csoporton belüliek értik tisztán a közleményeket.

Beépített VOX
Ez a kéz nélküli üzemmód a beépített VOX funkcióval. A funkció használatához az opcionális KHS-14 vagy KHS-15-OH fejszerelvény szükséges. A VOX érzékenysége 10 szinten állítható.

Voting (Intelligens csatornakeresés)
Egy többcsatornás rendszerben a voting funkció megkeresi és kiválasztja a legjobb térerővel vett átjátszót és azt használja. Az intelligens csatornakereséssel a felhasználó mindig a legjobb minőségben tudja a rendszerét használni kompromisszumok nélkül.

Kettős prioritás csatorna és Keresés funkciók
A kettős prioritás funkció használatával a rádió két fontos csatorna forgalmát ellenőrzi folyamatosan, mialatt a normál csatornakeresés funkció aktív. A rádiók széleskörűen paraméterezhető keresési funkciókkal rendelkeznek, így a felhasználók minden igényét kielégítik.

Egyedül dolgozó funkció
Az egyedül dolgozó (Lone worker) funkció biztonságot és védelmet nyújt az egymagában munkát végző személyek részére. Amennyiben a dolgozó vészhelyzetbe kerül a rádió az előre

beállított vészhelyzeti funkcióra vált és jelzéseket küld a vészhelyzetről. Kompatibilitás az MPT1327-es trönkölt szabvánnyal (opció), a TK-2180/3180-as rádiók MPT1327 szabványú trönkölt rendszerekben is üzemeltethetők. A használathoz a rádióban belső programot kell cserélni, mely a Kenwood szervizekben történik.

Több nyelvű kijelző

Az összes kijelzőn megjelenő üzenet és funkció elnevezés az adott ország nyelvén jeleníthető meg. A rádióhoz használt számítógépes beállító program segítségével minden felhasználó maga is beállíthatja, hogy az adott funkció milyen néven jelenjen meg a kijelzőn.

Általános jellemzők:

Kompakt és könnyű szerkezetű. Az ergonómiai szempontok szem előtt tartásával tervezett TK-2180/3180 tökéletesen illeszkedik a felhasználó kezéhez. Súlya csak 400 g Lithium-Ion akkuval (KNB-33L) és 460 g Ni-Cd akkuval. Szélessávú működésre alkalmas készülék. A TK-2180/3180 széles működési frekvenciatartománya előnyös a több csatornás rendszereket üzemeltető felhasználóknak: 38 MHz sávszélesség VHF tartományban (136-174 MHz) és 70 MHz sávszélesség UHF tartományban (400-470 MHz).

Programozható csatorna távolság 12.5/20/25 kHz közötti. A TK-2180/3180 rádiók programozható csatorna távolsággal rendelkeznek. A 25 kHz, 20 kHz vagy 12.5 kHz csatornánként beállítható. A készülékek különösen nagy, 512 férőhelyes memóriával rendelkeznek, mely minden jelenlegi és jövőben várható csatornaszám igényt kielégít.

A TK-2180/3180 rádiók adóteljesítménye 1 - 5 Watt között állítható. Az UHF sávon is 5 Whasználható! A észülék alfanumerikus pont-matrix kijelzője nagy felbontású, 12 karakteres, alfanumerikus, a felhasználó egyszerűen leolvashat minden működtetéshez szükséges információt. A kijelző a felhasználó által szabadon beállított nyelvű szövegek megjelenítésére is alkalmas. A felhasználó rendelkezésére áll még a 3 karakteres csatornaszám, vagy zóna kijelző is. Akkumulátora könnyű, KNB-33L (Li-Ion) akku 10 óra üzemidőt biztosít. A KNB-31A (Ni-Cd) akkumulátor alacsony hőmérsékletű alkalmazások esetén jó megoldás, míg a nagyteljesítményű KNB-32N (Ni-MH) 14 óra üzemidőt biztosít.

Segélyhívó gomb

A jól látható és tapintható segélyhívó gomb a készülék tetején került elhelyezésre. A gombhoz rendelt funkciókat a felhasználó a számítógépes programban szabadon beállíthatja. A kiváló minőségű hangszóró (500 mW) audió teljesítménye még a zajos ipari környezetben is kifogástalan érthetőséget garantál.

Zajszűrő funkció KMC-25 mikrofonnal

A TK-2180/3180 beépített hangszóró 500 mW-os Az opcionálisan vásárolható KMC-25 mikrofon használatával még kifejezetten zajos környezetben is tisztán érthető marad a készülék adása. A beépített zajcsökkentő áramkörnek köszönhetően a rádiók hangminősége keskeny vagy széles csatorna használata esetén is kifogástalan. A funkció csatornánként ki–be kapcsolható.

Programozható funkciógombok

A TK-2180/3180 rádión 7 funkciógomb található, melyeket a felhasználó a számítógépes beállító program segítségével szabadon programozhatja különböző funkciók végrehajtására. Az opcionális KMC-25 mikrofonon 2 szabadon programozható funkciógomb található. Programozható mikrofon erősítés szabadon programozható alacsony vagy magas értékre, hogy a felhasználás módjától és a rendszertől függően mindig a legjobb minőséget adja.

Jelszavas védelem (PIN kód)

A rádiók védelmét 3 szintű jelszavas (PIN kódos) védelem szavatolja. A három szint a következő:

- *"Rádió jelszó"* a készülék illetéktelen használatát akadályozza meg;
- *"Kiolvasási jelszó"* a rádióban tárolt adatok és információk kiolvasását akadályozza meg; - "Felülírási jelszó" a rádió programozását akadályozza meg.

Belső opciós port

A rádiók belsejében egy 26 pólusú opciós port található, ahová egyszerűen illeszthetők az opcionális kiegészítők. Pl.: VGS-1 hangrögzítő panel, VGS-1 Hang és adatrögzítő panel (opció). Az opcionális VGS-1 panel több új funkcióval bővíti a rádió lehetőségeit:

- *"Hang információ"* a rádió angolul bemondja a választott csatorna számát vagy a ki-be kapcsolt funkciókat.
- *"Hang rögzítés"* a készülék maximum 300 másodperc terjedelemben rögzíthet bejövő üzeneteket, elmulasztott hívásokat, valamint használható diktafonként és üzenetrögzítőként is. A készülék hívás esetén bemondja az előre rögzített szöveget, majd ezt követően a hívó üzenetet hagyhat a rádión.

További funkciók:

- 3 szinű LED (zöld, piros, sárga)
- QT / DQT / DTMF adás és vétel
- Minimum és maximum hangerő beállítási lehetőség
- Felhasználó által beállítható és szerkeszthető jelzőhangok
- Digitális 5 hangú jelzésrendszer ZVEI és VDEW beépítve
- Kézi GPS csatlakozatási lehetőség
- Valós idejű óra a készülékben, időbélyegző funkcióval
- Vételi térerő kijelzése a kijelzőn (RSSI)
- Akkumulátor töltöttségi állapot kijelzése a kijelzőn
- Alacsony akkufeszültség jelzése
- Kenwood ESN (Elektronikus Gyári szám)
- Jelszóval védett rádióazonosító üzenet
- Távletiltás és engedélyezés
- Windows alapú programozás és hangolás

MINŐSÉGBIZTOSÍTÁS ÉS KÖRNYEZETÁLLÓSÁG

A TK-7180/8180 rádiók már megfelelnek az EU RoHS és WEEE előírásainak. ISO 9001 Minőségbiztosítású a TK-2180 és TK-3180 rádió. A TK-2180/3180-as rádiókészülékek megfelelnek a legszigorúbb IP54-es és IP55-ös előírásoknak. Azon berendezések, melyek az IP54 és IP55 szabványnak megfelelnek, a legszélsőségesebb körülmények között is biztonsággal üzemeltethetők. (MIL-STD 810 C/D/E/F)

A TK-2180/3180 rádiók teljese mértékben megfelelnek az Amerikai Védelmi Minisztérium környezeti behatások elleni védelemre vonatkozó előírásainak a MIL-STD 810 C/D/E/F szabvány szerint:

- Alacsony nyomás, magas hőmérséklet
- Alacsony hőmérséklet, hőmérséklet sokk
- Napsugárzás, eső (vezetett eső is)
- Pára, sós köd, por, rázkódás, ejtés

Általános adatok a TK-2180-ról:

- Működési frekvencia tartomány 136-174 MHz 400-470 MHz
- Csatornaszám Max. 512 csat. (max. 128 csoport)
- Csatornatávolság 12.5 / 20 / 25 kHz
- PLL csatorna léptetés 5, 6.25 kHz
- Antenna impedancia 50 ohm
- Működési feszültség 7.5VDC±20%
- Akku élettartam (5-5-90) KNB-31A 9 óra
- KNB-32N 14 óra
- KNB-33L 10 óra
- Működési hőmérséklet tartomány -30C +60C között
- Méret (Szélesség x Hossz x Magasság)
- KNB-33L akkuval 58 x 33 x 136 mm
- Súly KNB-33L akkuval 400 g
- Szabványok EN 300 086, EN 300 113, EN 301 489, EN 300 279, IP54, IP55

A készülékek a csoport tagjainak védőöltözetén belül, málhamellényben, vagy derékszíjra rögzítve használhatók. A hozzá kapcsolt vezeték nélküli beszélőkészlet teszi lehetővé a szabadkezes kommunikációt.

ÖSSZEHASONLÍTÁS MÁS RÁDIÓS HOZZÁFÉRÉSI TECHNOLÓGIÁKKAL. AZOK JELLEMZŐI

A szélessávú vezetéknélküli kommunikáció technológiai szintjén két fő fejlődési irány ismert. Az egyik az IP alapú vezetéknélküli technológiák képességeit egészíti ki költséghatékonyabb, nagyobb területi lefedés lehetőségével és a mobilitás támogatásával. A WLAN mellet 2006-ban vált elérhetővé a WiMAX (Worldwide Interoperability of Microwave Access) rendszer fix változata. Ebben az anyagban a WiMAX-ot a felhasználók szempontjából egy hálózati hozzáférést nyújtó megoldásnak tekintjük. A másik fő irányvonal technológiái a 3GPP szabványcsaládba tartoznak, és ezek az EDGE (Ehanced Data rate for Global Evolution), az UMTS (Universal Mobile Telecommunication System) és annak továbbfejlesztett változata a HSPA (High Speed Packet Access).

Jellemző	EDGE /3GPP/	UMTS - Rel. 99' /3GPP/	UMTS / HSPA /3GPP/	WiMAX (fix: 802.16.a/g, mobile: 802.16.e) /IP/	WLAN (802.11.a, b) /IP/
Hozzáférési mód	TDMA – FDD	WCDMA – FDD	WCDMA – FDD	OFDM(A) – TDD (mobil), FDD	DSSS, OFDM
Moduláció	GMSK / 8PSK	QPSK	QPSK, 16QAM	QPSK, 16QAM, 64QAM	BPSK, QPSK, 16QAM, 64QAM
Max. felhasználói adatsebesség le / fel (indikatív értékek)	200 / 100 kbit/s	384 / 64 kbit/s	3.0 (10) Mbit/s / 384 kbit/s (5 Mbit/s)	20 / 5 Mbit/s	6, 3 / 6,3 Mbit/s
Működési frekvenciák [MHz] (tervezett)	900, 1800	2000, (900, 1800, 2500)	**2000**, (900, 1800, 2500)	Mobile: 2300, 2500, Fix: **3500**, (5800)	2400, 5400-5800
Frekvenciasáv engedélyköteles-sége (Magyarországon)	Igen	Igen	Igen	Mobil: nem áll rendelkezésre 3500 MHz: igen	Nem
Mobilitás támogatása	Igen	Igen	Igen	Mobil verzió 2007/2008 -tól	Korlátozott
Nagy területek lefedésére alkalmas	Igen	Igen	Igen	Igen, de városi környezetben inkább a mobil változat	Nem
Jövőállóság (1-3)	1	1	3	3	3
Érettség (1-3)	3	3	2	1	3
Támogatott felhasználói módok	M	M	F, N, M	F, N, M	F, N

Rádiós hozzáférési technológiák főbb jellemezői

„B” VÁLTOZAT: WIMAX KOMMUNIKÁCIÓ

A felsorolt jellemzők alapján, hosszabb távon a WiMAX alkalmas nagyterületű hozzáférés biztosítására és a felsorolt felhasználási módok mindegyikének lefedésére. Természetesen nem szükségszerű az összes felhasználói mód kiszolgálása, de ez a tulajdonság növeli a technológia alkalmazási lehetőségeit.

A lényegesebb eltérések a hozzáférés módja, a támogatott modulációk fajtái, a támogatott működési frekvenciák, illetve a technológiák jelenlegi érettségében mutatkozik meg.

A WiMAX jelenleg magasabb rendű modulációs módok támogatása miatt nagyobb hálózati kapacitásra és felhasználó szintű adatsebességre képes. Azonban napjainkban csak a fix változat tekinthető érettnek, alkalmasnak a piaci bevezetésre. Ezen felül a technológiai korlátok következtében a MAN szintű használata limitált. A mobil változat a mobilitás támogatása mellett, olyan megoldásokkal rendelkezik – *az UMTS/HSPA-hoz hasonlóan és a fix változattal szemben* – amelyekkel képes lesz nagyvárosi területek spektrum hatékony lefedésére is.

Az UMTS/HSPA előnye a technológia érettsége, alkalmazhatósága

Bár jelenleg kevésbé gyors átvitelt támogat, annak mértéke nagy valószínűséggel kielégíti majd az összes szolgáltatás által igényelt szintet. A táblázatban lévő adatátviteli sebességek a jelenre vonatkoznak, és elsősorban a különbségeket érzékeltetik. A valós hálózati környezetben tapasztalható minőség függ a szolgáltató állomás távolságától, a hálózat terheltségétől, a zaj és az interferencia szintjétől, az alkalmazott terminál képességeitől egyaránt.

Rádiós hozzáférés esetén a rendelkezésre álló sávszélesség, a nagy területek költség-hatékony ellátása, valamint a mobilitás támogatása a legfőbb ismérvek. A technológiai adottságok alapján az EDGE és az UMTS inkább a mobil típusú, a WLAN inkább a nomád típusú, míg a WiMAX és az UMTS/HSPA mindhárom módra egyaránt alkalmas. Fontos megjegyezni, hogy a várhatóan kevésbé fogják mozgás közben igényelni a szélessávú szolgáltatásokat, viszont azokhoz számos helyről szeretnének majd hozzáférni. A táblázatból az is kiolvasható, hogy mindkét technológiai irányvonal egyaránt alkalmas lehet az ADSL kiváltására, azzal megegyező szolgáltatási minőség nyújtására.

A könnyen rögzíthető kültéri antennák telepítése szakértelmet nem igénylő, gyors rögzítést biztosító kell, hogy legyen. A gyors telepítés érdekében – *különösen akkor, ha a csoportban híradó felkészültségű személy nincs* – az is biztosítható, hogy az árboc felszerelt kültéri egységekkel kerüljön szállításra.

WiMAX technológiával kiváló minőségű Pont Multipont (PMP) rádiós hozzáférési rendszer alakítható ki. A kikülönített csoport gépjárművének környezetében elhelyezkedő mobil felhasználók forgalmát egy árbocon elhelyezett WiMAX szabványú rádiós hozzáférési hálózat gyűjti össze. A járőrök esetében hordozható, akkumulátoros üzemre is alkalmas végponti egység (CPE) biztosítása szükséges. A rendszerrel a mobil labor központjából lehetővé válik a felhasználóktól álló vagy mozgókép továbbítása is a vezetési pontból (a gépjárműtől 3-8 km-es körzetében). Ehhez a gépjármű oldalára erősített, 1,5-2 méter magas

antenna árboc szükséges, melyre akár 3 darab 120 fokos szektorsugárzó antennát lehet rögzíteni, így a körkörös lefedettség is biztosítható. A kültéri egységek nem foglalnak helyet a bázisállomás belteréből a külső felszerelés miatt. A járőrök felszerelését ki kell egészíteni hordozható akkumulátoros üzemre is alkalmas végponti egységgel (CPE), mely lehetővé teszi a mobil felhasználók részére álló vagy mozgókép továbbítását a vezetés részére a gépkocsi 3-8 km-es körzetében. Ehhez szükséges minimálisan egy négycsatornás bázisállomás kültéri egységekkel, melyek az antenna árboc alján kerülhetnek elhelyezésre a három kültéri egységgel és a három darab, árbocra szerelt 120°-os szektorantennával. A bázisállomás csatlakozva a kültéri rádiós egységhez képes kiszolgálni végpontok százait, a spektrumhatékonyságot szem előtt tartva, minden irányban váltakozó modulációs sémát célszerű használni (QPSK–64QAM), hogy mindig a megfelelő sávszélességű és minőségű szolgáltatást nyújtson a felhasználók részére. Ez a megoldás akár 45 km-re lévő távoli helyek rendszerbe kötésére is alkalmas lehet Pont-Pont szélessávú kapcsolat kialakítására, kiváló minőséggel, kiküszöbölve a felesleges repeater állomások költségét.

A rendszer előnyei

- költség-hatékony szélessávú megoldás;
- ideális megoldás a TDM alapú távközlésről a VoIP-re történő migrációnál;
- távoli végpontok is hatékonyan a rendszerbe köthetők;
- a nagy sávszélesség adta előny ideálissá teszi gerinchálózati megoldásokra;
- az alacsony késleltetési idő miatt valós idejű alkalmazásokra kiváló;
- nagyon könnyű és gyors telepíthetőség.

Nagyobb kapacitás

- nagy sávszélesség (max. 70Mbps) a rádiós interfészen, max. 45Mbps Ethernet interfészen gerinchálózati és nagy sávszélességű elosztóhálózati megoldásra;
- alacsony késleltetési idő (<10 ms) kiválóan alkalmas gerinchálózati és több "hop"-ból álló hálózati alkalmazásra, valamint real-time szolgáltatásokra, mint ang, video és interaktív alkalmazások.

Nagy megbízhatóság és biztonság

- a redline szabadalmaztatott adaptív modulációs és kódolási technikája biztosítja a 10^{-9} BER-t, megfelelve a "carrier-class" megbízhatósági igényeknek is;
- a hat különböző modulációs séma (QPSK 64 QAM) mindig a rádiós csatorna minőségéhez, jel/zaj viszonyához igazodik;
- ARQ (Automatic Repeat Request) algoritmus a fejlett hibajavító eljárással 99,999% rendelkezésre állás biztosítható;
- 802.16 szabvány által definiált "Service class"-ok használatával biztosítható a megfelelő QoS szolgáltatások a kiemelt feladatot ellátóknak is;
- magas MTBF mutató garantálja a "carrier class" megbízhatóságot;
- AES/3DES titkosítási algoritmus megfelelő védelmet nyújt a rádiós interfészen.

A JÁRŐR FELSZERELÉSE A KOMMUNIKÁCIÓS LEHETŐSÉGEK BIZTOSÍTÁSÁRA

Képmegjelenítő kamera

A képmegjelenítő kamera

A járőr részére a vezetési pontról történő írásos üzenetek, képek, adatok megjelenítésére az egyik szem elé miniatűr képmegjelenítő (microdisplay) szükséges. Ez a kezelőt a szabad látásban nem gátolja, ugyanakkor segítséget ad a feladatok végrehajtásának támogatására. A kamerát a kommunikációs kapcsolatot biztosító rádió után a BodyLan elemeként a hordozható számítógéphez, PDA-hoz kell csatlakoztatni. A járőr feladatának végrehajtásához szükség van a „szabad kéz” elvűségre, ezért a beszédkommunikáció alapvetően head-settel valósul meg. Az eszköz kiválasztásánál fontos szempont a kényelmes viselhetőség és a kellő érzékenység. Nem célszerű a fülbe dugható megoldás a rögzítetlenség miatt (kicsúszhat, kényelmetlen lehet). A kommunikációs terminál csatlakozó felületein USB 2.0 csatlakozók elérése szükséges, melyeken keresztül akár a kijelző, vagy más adatbeviteli eszköz csatlakoztatható.

Bluetooth-os és vezetékes fejhallgató mikrofonnal

Integrált kép- és hangcsatlakozás

A két eszköz integrálása a feladat jellegétől függően meg is történhet, vagyis a kijelző és a fejhallgató egy eszközbe integráltan „kevésbé katonai kivitelben” is alkalmazható.

Rádiókommunikáció, BodyLan:
A járőr tevékenységét segítő legfontosabb elem, mely biztosítja a folyamatos kép-, adat- és hangkommunikációt. A készülék hordozható, akkumulátoros kivitelű kell, hogy legyen, hosszabb időn keresztül (10-12 óra) biztosítson autonómiát a felhasználó részére. A rádió frekvenciatartományát a mobil konténerre rögzített WiMAX hálózathoz kell illeszteni. A BodyLan-t biztosító személyi számítógépbe CPE egység (a WiMAX hálózathoz) szükséges.

A képen látható rádió esetében UHF-R vezetéknélküli platform rendszerét használja, és szoftverrel konfigurálható. 60 - 75 MHz-es tartományban működik, 25 kHz-es lépésekben állítható, összesen 3000 választható frekvencia áll rendelkezésre. Választható 10mW vagy 50mW-os teljesítmény, akár 9 órás működési idő, szintkijelzés és LCD háttér-világítású.

Mikrokamera

Mikrokamera sisakra erősítve

Amennyiben a járőr tagjainak szükséges a képrögzítés, képbejátszás a vezetési pontra (konténerbe), úgy a fejre szerelhető kamerák alkalmazása célszerű. Ezek a jó felbontású, színes képek felvételére, továbbítására alkalmas eszközök biztosíthatják a járőr tevékenységének kontrollálását, másrészt a későbbi elemzés lehetőségét. Ugyanakkor a továbbított mozgóképek elemzéséből utasítások adhatók a járőr részére akár hang, akár adat vagy kép formájában a mikrokijelzőre.

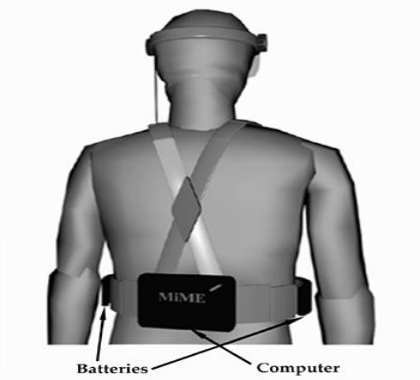
Személyi számítógép
A személyi hálózatok, a PAN-ok (Personal Area Network) olyan számítógép-hálózatok, amelyet személyi felszereléskénti fejlesztettek ki, általában a testfelületen, vagy a testre rögzített viselésre szántak. Hatótávolsága alapján megközelítőleg10 méter körüli kiterjedést képes biztosítani elsődlegesen a testfelület és a testre rögzített (hordozható) eszközök kommunikációs szintű összekapcsolására (ideális körülmények esetén a 100 méter is elérhető).

Nadrágszíjra erősített PAN

Ezeket a PAN-okat piconet-nek is nevezhetjük, ami legfeljebb 8 aktív berendezés master-slave típusú összekapcsolását teszi lehetővé ("parkoló" módban legfeljebb 255 berendezés csatlakoztatható). A piconet hálózatban az első Bluetooth berendezés a vezérlő, a "master", és az összes többi berendezés "slave" módon kommunikálhat a "master"rel. A BodyLan hálózat lelke a személyi számítógép, mely lehet egy erre a célra speciálisan kifejlesztett, vagy a feladatra a COTS termékek közül kiválasztott számítógép, PDA. Ennek meghatározása a feladat jellegétől, a gépre kapcsolt eszközök számától és a futtatható programok jellegétől függ. Jelenleg ennek típusa, képessége nem meghatározható; a készülékek széles skálája biztosítja a szükséges eszköz integrálását, de előtte a szakmai feladatok meghatározása szükséges. A járőrt olyan PAN számítógéppel célszerű ellátni, mely képes vezetés-irányítási rendszer adatokat továbbítani automatikusan, és információkat a rendszerben fogadni. Ezzel megvalósítható a járőr tényleges helyzetének pontos meghatározása, nyomon követése (blueforce tracking).

Vezetés-irányítási adatok továbbítása

A BodyLan eszközök tápellátását a testre rögzített nagykapacitású (6-9 óra üzemidőt biztosító) akkumulátorokkal kell biztosítani. Erre új generációs tölthető lithium-ion (Li-ion) akkumulátorcsoport használata célszerű. A technikai eszközöket viselhető formában úgy kell kábelezni és felszerelni, hogy azok akár „egyszerűbb” védőfelszerelés viselése közben, akár védőöltözetben komfortosan tudja használni a járőr.



Az akkumulátor elhelyezése

A BodyLan eszközök tápellátását a testre rögzített nagykapacitású (6-9 óra üzemidőt biztosító) akkumulátorokkal kell biztosítani. Erre *új generációs tölthető lithium-ion (Li-ion) akkumulátorcsoport használata célszerű.* A technikai eszközöket viselhető formában úgy kell kábelezni és felszerelni, hogy azok akár „egyszerűbb" védőfelszerelés viselése közben, akár védőöltözetben komfortosan tudja használni a járőr.

ÖSSZEGZÉS

Összegezve a kikülönített csoport kommunikációját megállapítható, hogy a szolgáltatások tárháza nagyon szertágazó. Minimálisan azonban megfogalmazható, hogy a rádiókommunikáció a csoporton belül elsődleges és szükséges! Ennek szolgáltatásai az igények függvényében bővülhetnek képi és adatszolgáltatásokkal.

A Publikáció összefoglalta a kiterjesztett szolgáltatásokat, melyek közül a felhasználó a csoport feladata és a kommunikáció megjelenési formájának igénye szerint választhat, bővíthet.

A vizsgált és javasolt eszközök felhasználhatósága nagyban függ az alkalmazás helyétől, a terep jellegétől, és a csoport munkavégzési környezetétől. Ezekre is választ ad a cikk.

"A PROJEKT A MAGYAR KORMÁNY TÁMOGATÁSÁVAL, A NEMZETI FEJLESZTÉSI ÜGYNÖKSÉG KEZELÉSÉBEN, A KUTATÁSI ÉS TECHNOLÓGIAI INNOVÁCIÓS ALAP FINANSZÍROZÁSÁVAL VALÓSUL MEG."

Felhasznált irodalom

[1] Farkas Tibor: A válságreagáló műveletek vezetését és irányítását támogató híradó- és informatikai rendszer megszervezése a Magyar Honvédség többnemzeti műveleteinek tükrében, Doktori (PhD) értekezés, ZMNE, 2010

[2] Géher Károly: Híradástechnika, Bp., Műszaki könyvkiadó,1993

[3] Grünzweig T.-Sziklai A: Intelligens szolgáltatások IP hálózaton, MAGYAR TÁVKÖZLÉS 2000/5 (XI. évfolyam 5. szám)

[4] Dr. Kovács Oszkár: A keskenysávú ISDN kézikönyve, Távközlési könyvkiadó, 1997.

[5] Kónya László: Számítógép- hálózatok (2 kiadás), LSI

[6] Magyarné Kucsera Erika: A hálózatfelügyelet és lehetőségei a Magyar Honvédség híradó szolgálatánál ZMNE TDK 2001

[7] Márkus Szabolcs: Az IP technológián alapuló beszédkommunikáció alkalmazási lehetőségei az MH stacioner hálózatának modernizációja során (ZMNE. Diplomamunka, 2007)

[8] Dr. Molnár S: IP hálózatok forgalmi méretezése, MAGYAR TÁVKÖZLÉS 2000/9 (XI. évfolyam 9. szám)

[9] Motorola Dimetra rendszer leírások

[10] Mobil távközlés – Dr. Dárdai Árpád, Nap Kiadó, 1999.

[11] Nagy Sándor: Internet és Intranet IntraNetware hálózaton, ComputerBooks Kiadói, Szolgáltató és Kereskedő Kft.-1997

[12] Network Centric Warfare, Appendix A: Information Technology Trends and the Value-Creation Potential of Networks, pp. 249., http://dodccrp.org/NCW

[13] Pahlavan, Kaveh: Trends in Wireless LANs, Second IEEE Workshop on Wireless LAN, Worchester Politechnic Institute, Worchester, MA 01609.

[14] Papp S.-Réthy Gy.-Balogh T.-Horváth T.-ISDN műszaki ismeretek I.-MATÁV OKTIG

[15] Pándi Erik: A magyar kormányzati távközlés egységesítésének hatása a rendvédelmi-, katonai-, és közigazgatási kommunikációs rendszerek megszervezésére és irányítására, ZMNE, doktori (PhD) értekezés

[16] Rajnai Zoltán: A tábori alaphírhálózat vizsgálata és digitalizálásának lehetőségei egyes NATO országok kommunikációs rendszereinek tükrében, doktori (PhD) értekezés ZMNE, 2001.

[17] SIEMENS Rt.: HICOM 300 E Rendszerleírás (oktatási anyag), 1998

[18] SIEMENS Rt.: HICOM 300 E Alkalmazások (oktatási anyag), 1998

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Harald Pöcher

REDUCTION OF PERSONNEL AND HEAVY WEAPON-SYSTEMS IN EUROPE BETWEEN 1990 AND 2010

Abstract

Since the end of World War Two in 1945 until 1990 the European security environment has been shaped by the powerful military alliances North Atlantic Treaty Organization (NATO)[i] and Warsaw Pact (WAPA)[ii]. While Eastern-Europe (Poland, former German Democratic Republic, former Czechoslovakia, Hungary, Romania, Bulgaria) was controlled by Soviet Union, the most of West- and Shout-Europe (Great Britain, Norway, Denmark, Netherlands, Belgium, Island, Luxemburg, France, Germany, Italy, Spain, Portugal, Greece) was under a loose control by the most powerful NATO member-states USA, Great Britain and France. Besides the military alliances a handful neutral and non-aligned countries (Sweden, Finland, Austria, Switzerland, Albania, Yugoslavia and Ireland) played in the strategic game of both superpowers only a secondary role. One of the most important strategy in the so-called "Cold War"[iii] period was "the arms race"[iv] which led to be always read for fight to over-manned and over-equipped armed forces.

Keywords: *security, NATO, Cold War ~ biztonság, NATO, Hidegháború*

THE WAY TO DISARMAMENT

In 1990 the Warsaw-pact member-state "German Democratic Republic" collapsed overnight and the Berlin Wall was demolished afterwards. Like a house of cards, the domino effect brought other former member-states of WAPA to collapse and in 1991 the Warsaw Pact treaty was cancelled. As a result the former member-states of WAPA changed their political and economic system and became member-states of NATO in 1999 respectively 2004 and member-states of European Union[v] in 2004 respectively 2007.

After the collapse of the bipolar[vi] world, in a period of nearly 20 years the former member-states of WAPA restructured their armed forces fundamentally. Nearly all the countries changed their recruitment system from conscription to a volunteer system and reduced thereby also their arsenal of weapon systems.

Figure 1[vii] shows the reduction of personnel and heavy weapons systems in Europe (without former Soviet Union) between 1990 and 2010 in detail. The brief summary looks as follows:

Personnel	40.7 %
Reserves	75.5 %
Battletank	59.5 %
Armoured infantry fighting vehicle	45.8 %
Armoured personnel carrier	54.1 %
Artillery-towed	61.1 %
Artillery-SP	24.9 %
Fighter Aircraft	59.2 %
Transport aircraft	34.4 %
Helicopter	18.4 %
Large Fighting Ships	5.1 %

Figure 2[viii] shows the reduction of personnel and heavy weapons systems in the successor states of former Soviet Union and of US Forces in Europe between 1990 and 2010 in detail. The brief summary looks as follows:

Successor states of former Soviet Union		**US Forces Europe**	
Personnel	67.6 %	Personnel	73.9 %
Reserves	50 %	Battletank	96 %
Battletank	54.9 %	Armoured infantry fighting vehicle	86 %
Armoured infantry fighting vehicle	20.3 %	Armoured personnel carrier	80 %
Armoured personnel carrier	69.3 %	Artillery-towed and SP	92 %
Artillery-towed	51.1 %	Fighter Aircraft	71 %
Artillery-SP	-	Transport aircraft	
Fighter Aircraft	35.3 %	Helicopter	
Transport aircraft	30 %	Large fighting ships	No figures available
Helicopter	41 %		
Large fighting ships	72 %		

As both figures show within a period of 20 years most of the countries in Europe reduced their personnel and reserve personnel as well as their heavy weapon systems. Therefore on the market for armament goods in Europe exists an over supply of second hand armament goods.

Meanwhile, there exists a long list of examples which kind of used weapons found a new owner. The Austrian Armed forces which had always manage the forces with little money

bought used Leopard 2 battle tanks from the Netherlands, Hercules transport aircraft and self propelled artillery systems M 109 from Great Britain, Jaguar tank destroyer from Germany (meanwhile withdrawn from service) and nearly as good as new Typhoon fighter aircraft[ix]. The purchase of used weapon systems leads always to many problems, for example upgrading and the purchase of spare parts could become extremely expensive during the whole life cycle of operation. But, in lack of money for armed forces, the purchase of used weapons is the only possibility for many states to equip their armed forces with nearly modern technology.

Used weapons which had served its time had to be scrapped by specialists. Because of large accumulated amount of old worn out weapons this business became an important branch of industry in Europe. Valuable raw materials can thereby be recycled and used for the production of new civilian and military goods.

The reduction of personnel and heavy weapon systems went hand in hand with reduction of defence expenditure on most of European countries. See in detail the figure 3[x] which shows the reduction of defence expenditure between 1990 and 2010 of selected European countries. In sum all the European countries spent less than 33.5 billion US$ in 2010 than in 1990. As the listing shows, the greatest reduction in absolute figures happened in reunited Germany (30 percent), Swiss (42.8 percent) and in most of the former member-states of Warsaw Pact respectively their successor states, i.e. in Hungary (50 percent), Romania (50 percent) and in the successor-states of former Czechoslovakia (63 percent). A larger increase of defence expenditure only happened in Finland (33 percent), Portugal (33 percent), Poland (25 percent), Greece (25 percent), Turkey (23 percent) and Norway (18.6 percent). A moderate increase in defence expenditure happened in Great Britain (8.6 percent), Denmark (2.2 percent), Spain (6.6 percent) and Italy (5 percent). The reduction of defence expenditure influenced economic activity in different ways. On the one hand side it has due to decreasing demand on armament goods an influence on the national defence industry and on the other hand side saving money for armed forces can reduce the budget deficit if the reduction of defence expenditure were real savings and weren't reallocated to other public expenditure, i.e. education, social security or health.

THE CONSEQUENCES OF DISARMAMENT IN EUROPE

Europe as a continent nowadays indulges in reminiscences and the continent has no imagination how mighty the whole Europe could be in the world. When we look at the economic figures, Europe is a powerful continent with a prospering economy as a strong base. But in comparison with the military machine of USA Europe is a weak continent. European countries operate no large aircraft carriers and no long range military transport aircraft. Both are important requirements to be a real world wide acting superpower. As history has shown, an overall powerful continent needs not only a strong economy but also a strong military machine. Remember the times when Great Britain rules the waves and the mighty Royal Navy won nearly all sea-battles during their glorious times at the heydays of the British Empire. Or remember the glorious days of France as a superpower which controlled most of West-Africa.

The First World War sounded the bell for decline of the continent Europe as a superpower. After the World War One the USA became stronger and stronger and during the heydays of the Second World War, USA with the advantage to be a power which has the monopoly of nuclear weapons became the most important superpower. Shortly after the war Soviet Union joint USA as second power which was able to produce nuclear weapons.

To loose further importance, after the Second World War the most powerful Western-European countries founded the European Communities (EC)[xi], nowadays the European Union (EU). Within the European Union the Common Security and Defence Policy (CSDP)[xii] is one important task of policy. Until now the CSDP stayed a stepchild of EU policy. Too

strong is NATO in Europe and there is obviously no need for duplication of military installations like organization structure. Within NATO the European member-states behave like free-riders and spend a smaller amount of money for their defence as USA and Peoples Republic of China (see figure 3: Defence expenditure). The result is a lack of strategic air and sea transportation systems, for example aircraft carriers and military long range transport aircrafts. The current situation of ESDP gives the impression that the Europeans rely heavily on the capabilities of USA and get therefore in a dangerous strategic offside position.

An important outcome to be a real strategic power is the possibility to send troops in missions with different intensity around the world and to control all the important sea-lanes. Though the European countries showed in the past that it is possible to lead missions abroad without extensive help by USA, for example in Chad before the door of Europe, it is not easy for European organize, lead and supply missions abroad far away from Europe. Therefore European contingents are only part of US-leaded Missions, for example in Afghanistan.

The current situation leads not only to great influence on the strategic position of Europe in the World but has also influence on the European armament Industry. A lack on demand of armament goods leads to a steadily decline of leading European armament enterprises. In the final end the firms earn less profit and had to reduce their organization which leads in short-time works or firing employees.

THE WAY OUT OF THE DILEMMA

As shown above, CSDP, compared with other fields of politics, lives a life of nicheness. Therefore it is necessary to start a process to raise awareness of importance of strong forces in a security environment which becomes more and more instable. If Europe will play an important role in world politics in the future, all the European Countries shall follow the way of the USA to adhere to a policy to maintain strong well equipped forces which could deployed in every corner of the world immediately in the best possible condition.

Land		1990	2010	Reduction	
				In absolut figures	In percent
Austria (neutral)	Personnel	44.000	27.300	16.700	37.9
	Reserves	242.000	65.000	177.000	73.1
	Battletank	159	114	45	28.3
	Armoured infantry fighting vehicle	-	112	-	-
	Armoured personnel carrier	460	352	108	23.4
	Artillery-towed	136	105	31	22.7
	Artillery-SP	54	189	-	-
	Fighter Aircraft	54	37	17	31.4
	Transport aircraft	2	3	-	-
	Helicopter	64	67	-	-
Hungary (Former WAPA) (NATO since 1999)	Personnel	86.500	29.450	57.050	65.9
	Reserves	210.000	44.000	166.000	79
	Battletank	1.482	30	1.453	98
	Armoured infantry fighting vehicle	502	164	338	67.3
	Armoured personnel carrier	1.261	164	1.097	86.9
	Artillery-towed	591	16	575	97.2
	Artillery-SP	171	152	19	11.1
	Fighter Aircraft	111	39	72	64.8
	Transport aircraft	16	5	11	68.7
	Helicopter	122	29	93	76.2

Land		1990	2010	Reduction	
				In absolut figures	In percent
Belgium (NATO since 1949)	Personnel	85.450	38.450	47.000	55
	Reserves	234.000	2.040	231.960	99.1
	Battletank	334	40	294	88
	Armoured infantry fighting vehicle	514	24	490	95
	Armoured personnel carrier	1.421	232	1.189	83.6
	Artillery-towed	21	24	-	-
	Artillery-SP	207	-	207	100
	Fighter Aircraft	144	60	84	58.3
	Transport aircraft	22	20	2	9
	Helicopter	60	33	27	45
	Large Fighting Ships	4	2	2	50
Bulgaria (Former WAPA) (NATO since 2004)	Personnel	107.000	34.975	72.025	67.3
	Reserves	472.500	302.500	170.000	35.9
	Battletank	2.149	362	1.782	82.9
	Armoured infantry fighting vehicle	243	185	58	23.8
	Armoured personnel carrier	1.998	1.290	708	35.4
	Artillery-towed	716	152	564	78.7
	Artillery-SP	761	329	432	56.7
	Fighter Aircraft	266	62	204	76.6
	Transport aircraft	22	17	5	22.7
	Helicopter	84	47	37	44
	Large Fighting Ships	7	4	3	42.8
Czechoslovakia (Former WAPA) (Czech Republic NATO since 1999, Slovakia NATO since 2004) (2010: Add-up figures for successor-states Czech Republic and Slovakia)	Personnel	154.000	33.001	121.000	78.5
	Reserves	495.000	11.445	483.555	97.6
	Battletank	3.200	420	2.780	86.8
	Armoured infantry fighting vehicle	1.560	805	755	48.3
	Armoured personnel carrier	1.900	210	1.690	88.9
	Artillery-towed	1.849	51	1.798	97.2
	Artillery-SP	518	298	220	42.4
	Fighter Aircraft	297	70	227	76.4
	Transport aircraft	30	18	12	40
	Helicopter	181	104	77	42.5
Denmark (NATO since 1949)	Personnel	29.000	26.585	2.415	8.3
	Reserves	72.700	53.507	19.193	26.4
	Battletank	499	65	434	86.9
	Armoured infantry fighting vehicle	-	29	-	-
	Armoured personnel carrier	595	372	223	37.4
	Artillery-towed	317	-	317	-
	Artillery-SP	76	24	52	68.4
	Fighter Aircraft	79	48	31	39.2
	Transport aircraft	6	7	-	-
	Helicopter	42	34	8	19.4
	Large Fighting Ships	3	2	1	33.3
Finland (neutral)	Personnel	31.800	22.550	9.250	29
	Reserves	700.000	350.000	350.000	50
	Battletank	120	100	20	16.6
	Armoured infantry fighting vehicle	72	180	-	-
	Armoured personnel carrier	460	920	-	-
	Artillery-towed	630	354	276	43.8
	Artillery-SP	-	90	-	-
	Fighter Aircraft	90	64	26	28.8
	Transport aircraft	3	10	-	-
	Helicopter	7	24	-	-
	Large Fighting Ships	2	8	-	-

Land		1990	2010	Reduction	
				In absolut figures	In percent
France (NATO since 1949)	Personnel	453.100		100.379	22.1
	Reserves	419.000	352.721	411.970	98.3
	Battletank	1.349	7.030	712	52.7
	Armoured	817	637	108	13.2
	infantry fighting	3.700	709	-	-
	vehicle	399	3.894	301	75.4
	Armoured	371	98	281	75.7
	personnel carrier	950	90	670	70.5
	Artillery-towed	263	280	136	51.7
	Artillery-SP	905	127	731	80.7
	Fighter Aircraft	51	174	18	35.2
	Transport aircraft		33		
	Helicopter				
	Large Fighting Ships				
Germany (NATO since 1955)	Personnel	476.300		225.687	47.3
	Reserves	1 Mio.	250.613	838.188	83.8
	Battletank	7.000		5.615	80
	Armoured	3.254	161.812	1.210	37.1
	infantry fighting	10.327	1.385	7.927	76.7
	vehicle	1.486	2.044	1.409	94.8
	Armoured	1.263	2.600	570	45.1
	personnel carrier	638	77	335	52.5
	Artillery-towed	252	693	156	61.9
	Artillery-SP	1.032	303	542	52.5
	Fighter Aircraft	14	96	-	-
	Transport aircraft		490		
	Helicopter		15		
	Large Fighting Ships				
Great Britain (NATO since 1949)	Personnel	300.100		124.420	41.4
	Reserves	347.200	175.680	147.920	42.6
	Battletank	1.314		928	70.6
	Armoured	945	199.280	370	39.1
	infantry fighting	3.590	386	872	24.2
	vehicle	345	575	179	51.8
	Armoured	367	2.718	189	51.4
	personnel carrier	575	166	288	50
	Artillery-towed	102	178	36	35.2
	Artillery-SP	795	287	269	33.8
	Fighter Aircraft	48	66	23	47.9

Land		1990	2010	Reduction	
				In absolut figures	In percent
Greece	Personnel	158.500	156.600	1.990	1.2
(NATO since 1952)	Reserves	406.000	237.500	168.500	41.5
	Battletank	1.879	1.688	191	10.1
	Armoured infantry fighting vehicle	96	377	-	-
	Armoured personnel carrier	2.000	2.105	105	52.5
	Artillery-towed	875	412	463	52.9
	Artillery-SP	299	348	-	-
	Fighter Aircraft	375	242	133	35.4
	Transport aircraft	97	39	58	59.7
	Helicopter	180	195	-	-
	Large Fighting Ships	18	17	1	5.5
Italy	Personnel	361.400	293.302	68.098	18.8
(NATO since 1949)	Reserves	584.000	41.867	542.133	92.8
	Battletank	1.220	320	900	73.7
	Armoured infantry fighting vehicle	-	254	-	-
	Armoured personnel carrier	3.879	2.367	1.512	38.9
	Artillery-towed	967	164	803	83
	Artillery-SP	283	164	119	42
	Fighter Aircraft	449	207	242	53.8
	Transport aircraft	63	91	-	-
	Helicopter	535	126	409	76.1
	Large Fighting Ships	34	26	8	23.5
Netherlands	Personnel	101.400	46.882	54.518	53.7
(NATO since 1949)	Reserves	152.400	3.339	149.061	97.3
	Battletank	913	60	853	93.4
	Armoured infantry fighting vehicle	984	224	760	77.2
	Armoured personnel carrier	2.232	70	2.162	96.8
	Artillery-towed	165	-	165	100
	Artillery-SP	298	169	129	43.2
	Fighter Aircraft	181	87	94	51.9
	Transport aircraft	16	10	6	37.5
	Helicopter	112	106	6	5.3
	Large Fighting Ships	15	6	9	60
Norway	Personnel	32.700	24.025	8.675	26.5
(NATO since 1949)	Reserves	285.000	45.000	240.000	84.2
	Battletank	211	72	13	65.8
	Armoured infantry fighting vehicle	53	104	-	-
	Armoured personnel carrier	150	390	-	-
	Artillery-towed	274	-	274	100
	Artillery-SP	126	90	36	28.5
	Fighter Aircraft	85	57	28	32.9
	Transport aircraft	12	4	8	66.6
	Helicopter	33	44	-	-
	Large Fighting Ships	5	3	2	40
Poland	Personnel	305.000	69.670	245.330	80
(Former WAPA)	Reserves	507.000	371.000	136.000	26.8
(NATO since 1999)	Battletank	2.850	946	1.904	66.8
	Armoured infantry fighting vehicle	1.391	1.508	-	-
	Armoured personnel carrier	928	239	689	74.2
	Artillery-towed	883	-	883	100
	Artillery-SP	599	608	-	-
	Fighter Aircraft	506	122	384	75.8
	Transport aircraft	25	39	-	-
	Helicopter	208	104	104	50
	Large Fighting Ships	6	8	-	-

Land		1990	2010	Reduction	
				In absolut figures	In percent
Portugal (NATO since 1949)	Personnel	61.800	44.340	17.460	28.2
	Reserves	190.000	210.900	-	-
	Battletank	146	225	-	-
	Armoured infantry fighting vehicle	-	-	-	-
	Armoured personnel carrier	255	353	-	-
	Artillery-towed	142	135	7	4.9
	Artillery-SP	6	20	-	-
	Fighter Aircraft	83	19	64	77.1
	Transport aircraft	37	45	-	-
	Helicopter	45	35	10	22.2
	Large Fighting Ships	10	12	-	-
Romania (Former WAPA) (NATO since 2004)	Personnel	200.800	73.500	127.300	63.3
	Reserves	626.000	45.000	581.000	92.8
	Battletank	2.875	299	2.576	89.6
	Armoured infantry fighting vehicle	156	26	130	83.3
	Armoured personnel carrier	2.575	1.089	1.486	57.7
	Artillery-towed	1.583	390	1.193	75.3
	Artillery-SP	32	24	-	-
	Fighter Aircraft	465	49	416	89.4
	Transport aircraft	26	12	14	53.8
	Helicopter	120	64	56	46.6
	Large Fighting Ships	9	7	2	22.2
Spain (NATO since 1982)	Personnel	257.400	128.013	129.387	50.2
	Reserves	2,4 Mio.	319.000	2,1 Mio.	87.5
	Battletank	838	498	340	40.5
	Armoured infantry fighting vehicle	-	144	-	-
	Armoured personnel carrier	1.742	1.465	277	15.9
	Artillery-towed	722	296	426	59
	Artillery-SP	156	130	26	16.6
	Fighter Aircraft	247	179	68	27.5
	Transport aircraft	120	107	13	10.8
	Helicopter	269	181	88	32.7
	Large Fighting Ships	20	13	7	35
Sweden (neutral)	Personnel	63.000	13.050	49.950	79.2
	Reserves	709.000	200.000	509.000	71.7
	Battletank	785	280	505	64.
	Armoured infantry fighting vehicle	-	336	-	-
	Armoured personnel carrier	600	687	-	-
	Artillery-towed	990	49	541	54.6
	Artillery-SP	30	24	6	20
	Fighter Aircraft	470	165	305	64.8
	Transport aircraft	30	16	24	80
	Helicopter	92	47	45	48.9
	Large Fighting Ships	31	5	26	83.8
Swiss (neutral)	Personnel	21.500	22.058	-	-
	Reserves	625.000	174.041	450.959	72
	Battletank	870	351	519	59.6
	Armoured infantry fighting vehicle	625	154	471	75.3
	Armoured personnel carrier	725	945	-	-
	Artillery-towed	900	-	900	100
	Artillery-SP	473	348	135	28.5
	Fighter Aircraft	289	87	202	69.8
	Transport aircraft	18	20	-	-
	Helicopter	107	56	51	47.6

Land		1990	2010	Reduction	
				In absolut figures	In percent
Turkey (NATO since 1952)	Personnel	579.200	510.600	68.600	11.8
	Reserves	1,1 Mio.	378.700	721.300	65.5
	Battletank	3.783	4.503	-	-
	Armoured infantry fighting vehicle	-	650	-	-
	Armoured personnel carrier	3.560	3.643	-	-
	Artillery-towed	1.724	685	939	54,4
	Artillery-SP	528	868	-	-
	Fighter Aircraft	530	426	104	19.6
	Transport aircraft	88	77	11	12.5
	Helicopter	330	340	-	-
	Large Fighting Ships	20	23	-	-
Yugoslavia (non-aligned) (Slovenia is NATO member since 2004 and Croatia is NATO member since 2009) (2010: Add up figures of successor states –Slovenia, Bosnia Hercegovina, Croatian, Serbia, Montenegro, Macedonia)	Personnel	188.000	74.341	113.659	60.4
	Reserves	510.000	56.316	453.684	88.9
	Battletank	1.850	868	982	53
	Armoured infantry fighting vehicle	490	727	-	-
	Armoured personnel carrier	500	700	-	-
	Artillery-towed	1.934	336	1.598	82.6
	Artillery-SP	120	160	60	50
	Fighter Aircraft	489	110	379	77.5
	Transport aircraft	44	19	25	56.8
	Helicopter	185	145	40	21.6
	Large Fighting Ships	4	2	2	50

Sum total			Sum total of reduction	
	1990	2010	In absolute figures	In percent
Personnel	4.097.550	2.426.316	1.671.234	40.7
Reserves	11.460.700	3.206.818	8.657.882	75.5
Battletank	32.646	13.210	19.436	59.5
Armoured infantry fighting vehicle	11.606	6.284	5.322	45.8
Armoured personnel carrier	44.858	17.430	27.428	54.1
Artillery-towed	15.196	3.510	11.686	61.1
Artillery-SP	6.662	4.997	1.665	24.9
Fighter Aircraft	6.924	2.820	4.104	59.2
Transport aircraft	1.294	848	446	34.4
Helicopter	3.642	2.971	671	18.4
Large Fighting Ships	291	276	15	5.1

1. figure. Reduction of personnel and selected weapon systems in Europe (without former Soviet Union) between 1990 and 2010 [xiii]
Scource: Institute for Strategic Studies-The Military Balance – 1990/1991 and 2010 and Janes Group

Land	1990		2010		Reduction	
					In absolut figures	In percent
Soviet Union (In column 2010 add up figures of successor states of former Soviet Union)	Personnel	3.4 Mio.	Personnel	1.1 Mio.	2.3 Mio.	67.6
	Reserves	5.2 Mio.	Reserves	2.6 Mio.	2.6 Mio.	50
	Battletank	54.400	Battletank	29.875	25.525	54.9
	Armoured infantry fighting vehicle	28.000	Armoured infantry fighting vehicle	22.296	5.704	20.3
	Armoured personnel carrier	50.000	Armoured personnel carrier	15.348	34.652	69.3
	Artillery-towed	33.000	Artillery-towed	15.982	17.018	51.1
	Artillery-SP	9.000	Artillery-SP	10.814	-	-
	Fighter Aircraft	4.340	Fighter Aircraft	2.805	1.535	35.3
	Transport aircraft	620	Transport aircraft	434	186	30
	Helicopter	4.600	Helicopter	2.713	1.887	41
	Large fighting ships	218	Large fighting ships	61	157	72
US-Forces Europe	Personnel	303.100	Personnel	79.000	224.100	73,9
	Battletank	5.000	Battletank	200 to 300	as much as 4.800	96
	Armoured infantry fighting vehicle	2.200	Armoured infantry fighting vehicle	300 to 400	as much as 1.900	86
	Armoured personnel carrier	3.500 bis 5.000	Armoured personnel carrier	1.000 to 1.500	as much as 4.000	80
	Artillery-towed and SP	2.420	Artillery-towed and SP	200 to 300	as much as 2.250	92
	Fighter Aircraft	657	Fighter Aircraft	NA	Though there are no figures available, the figures of reduction could be similar to the reduction of heavy weapon systems	
	Transport aircraft	26	Transport aircraft	NA		
	Helicopter	293	Helicopter	NA		
	Large fighting ships	13	Large fighting ships	NA		

2. figure. Reduction of personnel and selected weapon systems in successor states of former Soviet Union and US-Forces in Europe between 1990 and 2010
Source: Institute for Strategic Studies-The Military Balance 1990/1991 and 2010, Homepage of US Forces Europe.

Country	1990	2010	Change in absolute figure	Change in percent
Austria	3.5	3.4	- 0.1	- 2,8
Hungary	3.2	1.6	- 1.6	- 50
Albania	0.268	0.2	- 0.068	- 22
Belgium	8.3	5.7	- 2.6	- 31
Bulgaria	3.6	1	- 2.6	- 72
Czechoslovakia	10.8	3.9	- 6.9	- 63
Denmark	4.7	4.8	+ 0.1	+ 2,2
Finland	2.7	3.6	+ 0.9	+ 33
France	70	66	- 4	- 5,7
Germany	71	49	- 22	- 30
Great Britain	58	63	+ 5	+ 8.6
Greece	7	8.8	+ 1.8	+ 5
Ireland	1	1.3	+0.3	+ 30
Italy	36	38	+ 2	+ 5
Netherlands	13.5	12	- 1.5	- 11
Norway	5.9	7.0	+ 1.1	+ 18.6
Poland	7.4	9.3	+ 1.9	+ 25.6
Portugal	3.9	5.2	- 1.3	+ 33
Romania	4.6	2.3	- 2.3	- 50
Spain	15	16	+ 1	+ 6.6
Sweden	8.4	6.7	- 1.6	- 19
Swiss	8.4	4.8	- 3.6	- 42.8
Turkey	13	17	+ 3	+ 23
Yugoslavia	4.4	3.4	- 1	- 22
Soviet Union	290	80	- 210	- 70
USA	527	720	+ 193	+ 36

3. figure. Defence Expenditure of selected countries in Billion US$ (constant 2011)
Source: Institute for Strategic Studies-The Military Balance 1990/91 and 2010, SIPRI-database
Remarks: Figures 2010 for Czechoslovakia, Yugoslavia and Soviet Union add-up figures of successor states

References

[i] The North Atlantic Treaty Organization (NATO; *Organisation du traité de l'Atlantique Nord (OTAN)*), also called the (North) Atlantic Alliance was founded in April 1949 by Great Britain, France, Netherlands, Belgium, Luxembourg, United States, Canada, Portugal, Italy, Norway, Denmark and Iceland. Meanwhile, after some Steps of enlargement NATO includes 28 member states. 12 founders and Greece, Turkey, Germany, Spain, Czech Republic, Hungary, Poland, Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovenia, Slovakia, Albania and Croatia. Within NATO exists the „Partnership for Peace- Program (PfP)". Further 22 states are member of PfP: Armenia, Azerbaijan, Russia, Ukraina, Belarus, Georgia, Kazakhstan, Moldava, Tajikistan, Turkmenistan, Usbekistan, Bosnia and Hercegovina, Republic of Macedonia, Montenegro, Serbia, Austria, Ireland, Sweden, Finland, Malta, Switzerland. Cyprus and Kosovo are aspiring members. There exists also a co-operation with other states in the NATO-program for global partners. In this co-operation are included Republic of Korea, Japan, Australia, New Zealand, Mongolia, Pakistan, Afghanistan, Iraq and Colombia. Another interesting program is the Mediterranean Dialogue which includes Algeria, Egypt, Israel, Marocco, Jordan, Mauritania and Tunisia.

[ii] The Treaty of Friendship, Co-operation, and Mutual Assistance, more commonly referred to as the Warsaw Pact was founded in May 1955 by Bulgaria, Czechoslovakia, East Germany (withdrew in September 1990, before German Unification), Hungary, Poland (withdrew on January 1, 1990), Romania, Albania (formally withdrew in 1968) and Soviet Union. On 25 February 1991, the Warsaw Pact was declared disbanded at a meeting of defense and foreign ministers from Pact countries meeting in Hungary. On 1 July 1991, the Warsaw Treaty Organization of Friendship, Cooperation, and Mutual Assistance formally ended.

[iii] The so-called period of "Cold War" dated from 1947 to 1991 and was a state of political and military confrontation between powers in the Western Bloc, dominated by the USA and NATO, and powers in the Eastern Bloc, dominated by the Soviet Union along with the Warsaw Pact.

[iv] The phrase "arms race" means a competition between two or more parties to have the best armed forces. Each party competes to produce larger numbers of weapons, greater armies, or superior military technology. The arms race leads to a technological escalation.

[v] The European Union (EU) is an economic and political union of 28 member states. The members are: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden United Kingdom. One important field of politics in the EU is the Common Foreign and Security Policy (CFSP). The CFSP sees the NATO responsible for the territorial defence of Europe and "peace-making". However, since 1999, the European Union is also responsible for implementing missions, such as "peace-keeping" and policing of treaties, etc..

[vi] Bipolarity is a distribution of power in which two states have the majority of economic, military, and cultural influence internationally or regionally. For example, in the Cold War, most Western and capitalist states would fall under the influence of the USA, while most Communist states would fall under the influence of the Soviet Union.

[vii] The data for figure 1 were taken from "The Military Balance" which is The International Institute for Strategic Studies' (IISS) annual assessment of the military capabilities and defence economics of 171 countries worldwide. It is an essential resource for those involved in security policy-making, analysis and research.

"The Military Balance", 1990-1991 Brassey's UK, Limited, 1990 and "The Military Balance" 2010 and 2011, Routledge 2010 and 2011.

[viii] The data for figure 2 were taken from "The Military Balance", 1990-1991 Brassey's UK, Limited, 1990 and "The Military Balance" 2010 and 2011, Routledge 2010 and 2011.

[ix]The data for figure 3 were mostly taken from the "Stockholm International Peace Research Institute (SIPRI) military expenditure database" gives consistent time series on the military spending of 172 countries since 1988, allowing comparison of countries' military spending: in local currency, at current prices; in US dollars, at constant prices and exchange rates; and as a share of GDP. Some data were taken from Institute for Strategic Studies-The Military Balance 1990/91 and 2010.

[x] See http://en.wikipedia.org/wiki/Leopard_2#Operators (Retrieved 30 August 2013), http://www.airpower.at/flugzeuge/herkules/index.html (Retrieved 30 August 2013), http://de.wikipedia.org/wiki/Jaguar_(Jagdpanzer) (Retrieved 30 August 2013) http://ciar.org/ttk/mbt/armor/armor-magazine/armor-mag.1998.ma/2austria98.pdf (Retrieved 30 August 2013) http://en.wikipedia.org/wiki/Eurofighter_Typhoon#Operators (Retrieved 30 August 2013)

[xi] The European Communities (sometimes referred to as the European Community or EC) were three international organisations that were governed by the same set of institutions. These were the European Coal and Steel Community (ECSC), the European Economic Community (EEC) and the European Atomic Energy Community (EAEC or Euratom).

[xii] The Common Security and Defence Policy (CSDP), formerly known as the European Security and Defence Policy (ESDP), is a major element of the Common Foreign and Security Policy of the European Union (EU) and is the domain of EU policy covering defence and military aspects, as well as civilian crisis management. The ESDP was the successor of the European Security and Defence Identity under NATO, but differs in that it falls under the jurisdiction of the European Union itself, including countries with no ties to NATO.

[xiii] Since 2010 further reduction of personnel and weapon-systems have happened. For example Austria reduced artillery SP (from 189 to approx.50) and armoured personnel carrier (from 353 to 0) and batteltanks from 114 to approx. 6 and Hungary reduced all the artillery SP weapons to 0 and figfhter aircraft to 14.

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Kassai Károly
karoly.kassai@hm.gov.hu

AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI KÉRDÉSEK MEGJELENÉSE A MAGYAR HONVÉDSÉG HÍRADÓ-INFORMATIKAI SZABÁLYZATBAN

Absztrakt

A híradó és informatikai szabályzásnak le kell fednie minden területet a stratégiai szintű műveletektől a harcászati szintű műveletekig itthon és külföldön támogatva a vezetési és irányítási képességeket a minősített vagy nem minősített adatkezelés érdekében a parancsnokok követelményei szerint. A másik kritikus tényező a híradó és informatikai rendszerek támogatása és az információbiztonsági szempontok közötti összehangolás. A szerző szándéka a biztonsági követelmények beillesztésének támogatása a tervezett új híradó és informatikai szabályzatba, valamint a stratégiai szinten az alapvető biztonsági filozófia megértésének segítése.

The CIS regulation has to cover all issues from strategic level to tactical level operations at home and abroad, supporting C2 capabilities to handle classified and unclassified information according to the requirements of commanders. The other critical factor is the coordination between CIS support and the CIS security point of view. The intention of the author is to support the implementation of security requirements into the planned future CIS regulation and to help to understand the basic security philosophy at strategic level.

Kulcsszavak: *információbiztonság, elektronikus információbiztonság, kiberbiztonság, szabályozás ~ information security, electronic information security, cyber security, regulation.*

ELŐZMÉNYEK

A Magyar Honvédségnél (MH) a híradó és informatikai kérdések szabályozása több, korábban kiadott szabályzat és alacsonyabb szintű belső rendelkezés feladata.[1]

A jelenlegi rend szerint az informatikai szakterület első számú szabályozója az 1993-ban kiadott MH Informatikai Szabályzat [1], mely az akkori szervezeti kultúrának megfelelően keretet adott az informatikai szakkérdések kezelésének, benne az elektronikus információbiztonságra vonatkozó alapvető követelményeket is megfogalmazva.

Vezérkar főnöki intézkedésben megtörtént a szakterületi kérdések korszerű szabályzatban történő kidolgozásának elrendelése a közelmúltban, így a jól felépített, logikus – de már korszerűtlen – „kis zöld" helyett jövőre kiadásra kerül a Magyar Honvédség Híradó-informatikai Szabályzata (továbbiakban: Szabályzat), melynek kidolgozása a 2013. július 29-én egyeztetett, jóváhagyásra felterjesztett szinopszissal megkezdődött. [2]

A kidolgozás tartalmi elemeiről hírt adni ilyen rövid idő elmúltával nem lehetséges, de a téma fontossága és az elektronikus információbiztonsági szakterülettel való szoros kapcsolat szükségessé teszi e szabályozási feladat kapcsán néhány elektronikus információbiztonsági szempont vizsgálatát.

A legelső szembeötlő változás maga a cím, ami jelzi, hogy a korábbi szakterületi elkülönülést a szakmai feladatok vezetéséért felelős HM szerv és a szakfeladatokat végrehajtó szervezetek a továbbiakban nem kívánják fenntartani. Ez a törekvés szinkronban van a világban történő eseményekkel, hadtudományi és egyéb szakterületi megállapításokkal. Napjaink egyre jobban digitálissá váló életünkben már egyre nehezebb az analóg vagy digitális átviteli út, vagy adat és hangkommunikáció – esetleg más szempontok – szerint „híradó" és „informatika" területekre osztani a világot.

A Szabályzat másik érdekessége – ami egyben a megoldandó feladat nehézségét is jelzi–, hogy a híradó és informatikai szakterületeken definiáltan még nem alakult ki az szabályozási hierarchia, ami az „általánostól az egyedi felé" elv alapján tartalmazza, hogy a szakmapolitika – általános, központi követelmények – rendszer vagy funkcionális alapon kiadott alacsonyabb szintű és szűkebb hatókörű szakutasítások rendjében milyen szabályozót, belső rendelkezést kell kialakítani. A kidolgozás így magában hordozza azt a kihívást, hogy már meglévő szabályozót kell módosítani, vagy meglévő (esetleg kialakulás alatt álló) értékes szabályozó elemeket kell megbontani annak érdekében, hogy később kialakítandó alacsonyabb szintű szabályozóba tartozó, részletesebben megfogalmazott követelmények ne kerüljenek be a központi Szabályzatba.

A Szabályzat szinopszisa szakmai egyetértés alapján jóváhagyott kiindulási pont, de a kidolgozás menete során értelemszerűen változhat, formálódhat, ami miatt nem célszerű elemzése, értelmezése. Érdekes kérdésnek csak az mutatkozhat, hogy a híradó és informatikai szakterületek mennyire tartják fontosnak a nemzetközi, nemzeti szabványok és „bevált gyakorlat" körébe tartozó ajánlások alkalmazását. A szabványkövetés kérdése figyelmet érdemel, mert a nemzetközi szakirodalomban az elektronikus információbiztonságra vonatkozó irányadó szabványok illeszkednek a katonai terminológia szerint „híradó és informatikai" szabályozáshoz, így könnyen elkerülhető a „keresztbe szabályozás" vagy egyéb szakterületi összehangolatlanságot okozó probléma. E miatt elektronikus információ biztonság szempontjából (is) fontos kérdés a híradó és informatikai szakterület szabványkövetésre vonatkozó döntése, ami a kidolgozásról szóló döntés során sikeresen meg is született. A kérdés érdekessége és a kidolgozók felelősségét, a szabályozási munka nehézségét jelzi, hogy az MH-ra is érvényesíthetően az informatika, vagy távközlés területén teljes körű, jogszabályban

[1] A szerző korábbi cikke – az elektronikus információbiztonságra koncentrálva – átfogó jelleggel azonosította a szabályozókat: Az elektronikus információvédelem szabályozási kérdései a közelmúltban, Hadmérnök, VIII. évfolyam 1. szám, 2013. március, p. 203-214.

megfogalmazott követelmények, kötelezően alkalmazandó szabványok vagy ajánlások nem azonosíthatók (még a kormányzati célú hálózatokról szóló jogszabály sem azonosít ilyen követelményeket). [3] E mellett az elektronikus információbiztonság területén a NATO és EU követelmények mellett törvény és kormányrendelet szabályozza a minősített adatkezelésre vonatkozó követelményeket, illetve 2013. július elsejétől az állami és önkormányzati szervezetek elektronikus információbiztonságáról is jogszabály rendelkezik (Ibtv.) **Hiba! A hivatkozási forrás nem található.**, ami jelzi a szakterületek közötti összehangolás fontosságát.

Az előzményekhez tartozóan utolsó kérdésként meg kell említeni a tervezett Szabályzat és az elektronikus információbiztonság szakterületi kapcsolatát, illetve azt a kérdést, hogy tervezett Szabályzat tartalmazzon-e az elektronikus információbiztonságra – illetve tágabban: információbiztonságra – vonatkozó részeket (és milyen mértékben), vagy nem.

A kidolgozásért felelős híradó és informatikai szakterületi képviselők állásfoglalása szerint az elektronikus információbiztonsági kérdések szabályozással e Szabályzat kidolgozása nem ütközhet a már meglévő biztonsági területű szabályozókkal. Ezzel együtt híradó és informatikai szakterületi igényként fogalmazódott meg, hogy elektronikus információbiztonságra – illetve tágabban: információbiztonságra – vonatkozó fejezetet kell a Szabályzatnak tartalmaznia. Az információbiztonsági fejezetben meg kell fogalmazni a fizikai, személyi, adminisztratív és elektronikus információbiztonsággal[2] kapcsolatosan azokat az alapkérdéseket, melyek *általános követelmények szintjén iránymutatást adnak a híradó és informatikai szakállománynak és megfogalmazásával segítik, hogy milyen információbiztonsági területű szabályozót „kell kézbe venni" az adott kérdés megoldása érdekében*, vagy *milyen irányon kell segítséget kérni*, ha technológiai váltás vagy nem szabályozott kérdés miatt eddig ismeretlen helyzetet kell megoldani.

A cikk a továbbiakban a Szabályzatban megjelenítendő elektronikus információ biztonsági részek előkészítését szolgálja. Cél, hogy az elektronikus adatfeldolgozás támogatása érdekében a rendszerek, szolgáltatások teljes életciklusán keresztül látható legyen az a biztonsági szemléletmód, amely biztosítja az adatok és rendszerek szükséges mértékű biztonságát. Az elektronikus adatfeldolgozás területén ez az elektronikus információbiztonsági keretrendszer egyaránt tartalmazza a minősített és nem minősített adatok körét, valamint a NATO, EU és más két vagy többoldalú szerződés védelme alatt álló, vagy nemzeti adatot.

A HADMŰVELETI KÖVETELMÉNYEK, FELHASZNÁLÓI IGÉNYEK BIZTONSÁGI SZEMPONTJAI

Az elektronikus adatkezelő rendszerek, képességek biztonsága szempontjából az egyik legfontosabb kérdés az első lépések, döntések és szerepük fontosságának tisztázása. *Új szolgáltatásokat biztosító elektronikus adatkezelő rendszerek kialakítása, vagy meglévő rendszerek változtatása csak jóváhagyott követelmények alapján történhet.* Ez a követelmény gyakran azért kerül ki a nézőpontból, mert túlnyomórészt meglévő rendszerek módosításai, fejlesztései képezik a változások zömét, melynek során gyakori a rendszer meglévő tartalékaira való támaszkodás, vagy racionalizálásból adódó erőforrás felhasználásra történő hivatkozás, mely lehetőségek elvonják a figyelmet az erőforrások biztosításának szükségességéről.

A „hadműveleti követelmények" és a „felhasználói igények" kapcsolata izgalmas vizsgálandó kérdés, mert az egyéni felhasználói igények nem írhatják felül a vezetési és irányítási képességekre vonatkozó magasabb szintű központi követelményeket.

[2] A kérdés szakmai kihívásnak tekinthető, mert jogszabály jelenleg csak a minősített adatok kezelése területén azonosít fizikai, személyi és adminisztratív jellegű követelményeket, [5][6] így az MH esetében e szabályokat a szervezetre vonatkozóan, önállóan kell megalkotni. E területen változtatást fog jelenteni az Ibtv. végrehajtását célzó NFM rendelet megjelenése, bár jelenleg még pontosan nem azonosítható a rendelet tervezet hatóköre.

Nemzeti viszonylatban a hadműveleti szakterület feladata az MH összes szervezetére meghatározni és jóváhagyatni a békeidőszakra vonatkozó vezetési és irányítási rendet, lefektetni az alapokat a különleges jogrendben szükséges vezetési és irányítási képességek meghatározása érdekében. *Ez a nemzeti keretrendszer csak a NATO és EU követelményekkel összhangban alakítható ki*, mivel a missziós kötelékek, vagy a NATO felajánlott erők kategóriájába tartozó képességeknek rendelkeznie kell a szövetséges előírások szerinti elöljárói, együttműködő és adminisztratív támogató kapcsolatokkal.

A vezetési képességekre vonatkozóan a feladat jellege, a környezet és egyéb változók miatt a kötelező jellegű szolgáltatásokon belül – vagy azok kiegészítéseként – megjelenhetnek szervezeti vagy egyéni igények, melyek a kiegészítéshez vagy módosításhoz szükséges erőforrások megléte és a biztonsági feltételrendszer kialakíthatósága esetén módosíthatják a szolgáltatások körét, a szolgálati vagy magáncélú adatkezelési lehetőségeket. E területen kritikus fontosságú annak tudatosítása, hogy *az erőforrások ideális esetben a központi hadműveleti követelményeknek megfelelően kialakítottak. Az esetleges változások, kiegészítések erőforrás szempontjából nem csak eseti kiadásokat vagy feladatokat jelentenek, hanem a további életciklus szakaszok alatt is erőforrásokat igényelnek*, melyek hiánya esetén az adott szolgáltatás csak ideig-óráig lesz elérhető.

A hadműveleti követelményeknek, felhasználói igényeknek tartalmaznia kell a biztonsági követelmények meghatározásához szükséges alapadatokat. A minimálisan meghatározandó adatok:

- a felhasználói kör és a szükséges személyi biztonsági követelmények;
- a kezelt adatok típusa (hang, adat, kép stb.), formátuma és a szükséges adatkezelő szolgáltatások, beleértve a más rendszerek felé történő egyoldalú vagy kölcsönös adatcsere igényeket;
- a kezelt adatok biztonsági osztálya, minősítési szintek és kezelési utasítások, hozzáférési korlátozások;
- adatkezelési helyszínek;
- a rendelkezésre állásra vonatkozó követelmények és prioritások (szolgáltatás, adat).

Az elektronikus adatkezelő rendszerre vonatkozó hadműveleti követelmények változtatása, pontosítása során vizsgálni kell a kockázatokat, és azok vezetésre és irányításra kifejtett biztonsági hatásait. Az elfogadható kockázatokat, illetve a változás okán keletkező, de erőforrások igénybevételével ellensúlyozható kockázatokat jóvá kell hagyatni. Ez a rendszabály azt célozza, hogy a követelményeket meghatározó vezető kapja meg a változást okozó döntések következményeivel járó információkat, rendelje el a változások okozta védelmi rendszabályok módosítását és tudatosan vállalja az információs kockázatokat.

A BIZTONSÁGI SZEMPONTOK ÉRVÉNYESÍTÉSE A TERVEZÉS, KIALAKÍTÁS, ÜZEMELTETÉS ÉS FEJLESZTÉS SORÁN

Nagy gyakorlatot igényel annak helyes mérlegelése, hogy mely tervezési, tesztelési vagy üzemeltetési feladat igényel elektronikus információbiztonsági támogatást, és melyek azok az esetek, amikor egy gyors konzultáció vagy dokumentálás kielégíti a biztonsági szempontú megfelelőséget.

Az elektronikus adatkezelő rendszerek tervezésekor a legkorábbi szakaszban meg kell jeleníteni és érvényesíteni kell a biztonsági szempontokat.

Az elektronikus adatkezelő rendszerek tervezési, fejlesztési, kialakítási és üzemeltetési fázisaiban azonosítani kell a szakfeladatokért való felelősségeket, és azokat úgy kell összehangolni, hogy a felelősség pontosan azonosítható legyen. A biztonsági követelmények, védelmi rendszabályok bedolgozása érdekében azonosítani kell a biztonságért felelős személyt

(személyeket). A tervezésért, szervezésért, szakfeladatokért – így a biztonságért – felelős személyek feladatait meg kell határozni.

A tervezés, kialakítás, üzemeltetés során ismétlődő jelleggel azonosítani kell az elektronikus adatkezelő rendszert érintő fenyegetettségeket, sebezhetőségeket. A vizsgálat alapján meg kell határozni és jóvá kell hagyatni az elfogadható mértékű kockázatokat.

Az elfogadható mértékű kockázatok figyelembe vételével a kialakítás vagy változtatás fázisaihoz igazodó biztonsági követelményeket kell kialakítani és jóváhagyatni.

A biztonsági követelmény teljesülése érdekében az elektronikus adatkezelő rendszert biztonsági osztályba kell sorolni. A biztonsági osztályon belül a védelmi rendszabályok specializálása, az adatkezelő funkciókhoz történő illesztés érdekében csoportok alakíthatók ki. A biztonsági osztályokra vonatkozó általános követelményeket a honvédelmi tárca információ biztonságpolitikája határozza meg.[3] [7] Az adatok bizalmasságának, sértetlenségének vagy rendelkezésre állásának változásából, vagy az adatok mennyiségének változásából adódó halmozódási hatásból (aggregation effect) adódó kockázatokat a biztonsági osztály vagy csoport átsorolással kell ellensúlyozni.[4]

Az adatkezelő szervezeteket az alkalmazott biztonsági osztályok figyelembe vételével a jogszabályi követelménynek megfelelően szervezeti biztonsági szintekbe kell sorolni. [4] A biztonsági osztályokra és a szervezeti biztonsági szintekre vonatkozó besorolásokat időszakonként felül kell vizsgálni.

A biztonsági követelmények alapján az elektronikus adatkezelő rendszer kialakítási vagy változtatási fázisaihoz igazodóan ki kell dolgozni és jóvá kell hagyatni a védelmi rendszabályokat tartalmazó biztonsági dokumentumokat (üzemeltetés biztonsági szabályzat, elektronikus információbiztonsági szabályzat). [6] [4] Fontos adminisztratív kérdés a kétfajta szabályozás összhangjának biztosítása, mivel a NATO, EU követelmények szerinti Üzemeltetés Biztonsági Szabályzat struktúrája valószínűleg eltér a másik szabályozótól. Ugyanígy szükség van a nemzeti és a NATO, EU minősített adatok szabályozási rendjének összehangolására is, mert eltérőség esetén nehezen megoldható adminisztratív problémák jelenhetnek meg, melyet meg kell oldani az MH vonatkozó szabályozóiban, [8][9] beleértve a meglévő rendszerek szabályozásának változtatásával, a képzéssel és hatósági akkreditálással kapcsolatos feladatokat.

Minősített adatkezelő rendszerek esetében:

- NATO és EU minősített elektronikus adatkezelő rendszereknél a rendszerbiztonsági követelmények, valamint az üzemeltetési biztonsági szabályzat kialakítása az aktuális NATO, EU szabályzók, valamint a jogszabályoknak megfelelően kell, hogy történjen.
- NATO struktúrába tartozó nemzeti szervezet, vagy kirendelt erő esetén a NATO általános szabályozók mellett a NATO szervezetekre specializált követelményeknek is meg kell felelni.
- Nemzeti minősített adatkezelő rendszer esetében a biztonsági dokumentumokat a vonatkozó jogszabályok által meghatározott követelmények szerint kell kialakítani.
- NATO EU követelmények, vagy jogszabályban meghatározott esetekben a minősítési szintnek megfelelő rejtjelzést kell alkalmazni elektronikus adatkezelés esetén.[5] A

[3] A biztonsági osztályok kialakításával kapcsolatos szakmai kihívás, hogy a már idézett Ibtv. alapján elrendelt végrehajtást szabályozó rendelet hogyan fogja a törvény által meghatározott öt biztonsági osztályt definiálni [4], tekintettel arra, hogy a minősítési szintek száma négy.

[4] Az elkülönítetten kezelt adatbázisok egyesítése, illetve a kezelt adatok mennyiségének gyorsuló ütemű növekedése miatt ennek a kérdésnek általános vizsgálata, az egyes szakterületi lehetőségek feltárása és megoldások kidolgozása szükségszerűen előtérbe fog kerülni.

[5] A korábbi nemzeti követelmények alkalmazása során rejtjelzés területén az „adatkezelés” a gyakorlatban a védett terület határán túl történő elektronikus továbbításra egyszerűsödött az adatkezelés, ami az „adattárolás” érdekében végzett rejtjelzés háttérbe szorulását okozta.

rejtjelzést a hatósági követelményeknek megfelelően kell kialakítani és alkalmazása az illetékes hatóság engedélyezésével történhet.
- „Bizalmas!” és magasabb minősítési szint esetén a minősítési szintnek megfelelő, az adatkezelő eszközökre és helyszínekre vonatkozó kompromittáló kisugárzás elleni védelmi rendszabályokat kell kialakítani és fenntartani.
- Minősített adatkezelő rendszer tervezését, fejlesztését, kialakítását, üzemeltetését az akkreditáló hatóság követelményeinek figyelembevételével kell végezni.

Új elektronikus adatkezelő rendszer alkalmazásba vétele, vagy a tervezett változtatás utáni alkalmazásba vétel csak funkcionális és biztonsági ellenőrzés, az üzemeltetési és biztonsági dokumentumok ellenőrzése, és a szükséges képzések dokumentált végrehajtása után történhet.

ENGEDÉLYEZÉS

Az engedélyezési fázis lényege, hogy új vagy módosított elektronikus adatkezelő rendszerek, szolgáltatások csak engedélyezési eljárás által történő feljogosítással kerülhessenek használatba. Az engedélyezés széles körben értelmezve lehet egy hatósági eljárás keretén belül történő akkreditálás vagy műszaki ellenőrzés, helyi körben egy üzemeltetési folyamat változtatásakor a teszt eljárás áttekintése, a dokumentumok pontosításának ellenőrzése és a szükséges képzés befejezésével az új eljárás alkalmazásba vételének jóváhagyása.

Új elektronikus adatkezelő rendszer használatba vétele, vagy a változást követő használatba vétel csak a meghatározott engedélyezési eljárás sikeres lefolytatása után történhet.

A rendszerek kialakításakor a NATO, EU követelményeknek, és a jogszabályoknak megfelelően azonosítani kell az engedélyezési eljárást, az engedélyezésre feljogosított személyt.

Az elektronikus adatkezelő rendszer üzemeltetési és biztonsági dokumentumaiban egyértelműen azonosítani kell az akkreditálási, auditálási és egyéb engedélyezési jogosultságokkal rendelkező hatóságokat és szervezeteket, az alkalmazásba vétel, vagy változás engedélyezési eljárásban hatáskörrel rendelkező szerveket, szervezeteket vagy személyeket illetve a szükséges eljárásokat. A jogszabályban meghatározott információs rendszerek és a minősített elektronikus adatkezelő rendszerek használatba vétele, vagy meglévő rendszeren változások megtétele a hatósági feladatokat ellátó szervezetek, szervek követelményei szerint kialakított eljárás lefolytatása és a szükséges határozat (engedély) kiadása alapján történhet.

Az elektronikus minősített adatokat kezelő rendszert ideiglenesen más biztonsági környezetben üzemeltetni, vagy más szabályok szerint üzemeltetni csak az esetre specializált engedéllyel lehet.

Az elektronikus minősített adatokat kezelő rendszeren tesztelés csak a tesztelésre kiadott engedély birtokában hajtható végre.

Az elektronikus minősített adatokat kezelő rendszer azonos, vagy eltérő minősítésű (vagy biztonsági osztályú) adatokat kezelő rendszerrel, vagy nem minősített adatokat kezelő rendszerrel csak az összekapcsolást engedélyező eljárás után lehetséges. Az összekapcsolást biztosító rendszerre vonatkozó biztonsági szabályozás kialakítása, jóváhagyása az akkreditálási feltételek közé tartozik.

AZ ÜZEMELTETÉS BIZTONSÁGI SZEMPONTJAI ÉS FELADATAI

Az elektronikus adatkezelő rendszerek életciklusában az üzemeltetés fázis feladatai a legismertebbek, a felhasználókat is ez az időtartam szolgálja ki, de ennek ellenére rengeteg gyakorlati példa mutatja, hogy ez a legjobban „kivívásokkal teli" időszak.

Az elektronikus adatkezelő rendszerek üzemeltetése csak *jóváhagyott üzemeltetési és biztonsági dokumentumok alapján, az arra felhatalmazott személyek által történhet*. A „jóváhagyott dokumentum" kifejezésnek tartalmaznia kell azt a meghatározást is, hogy MIT kell üzemeltetni. Ez a követelmény a jóváhagyott hardver és szoftver konfigurációt, az engedélyezett hálózati összekapcsolásokat, illetve a szükséges üzemeltetési folyamatokat tartalmazza.

A felhatalmazott személyek kapcsán ki kell emelni, hogy a nemzetbiztonsági ellenőrzés és a szükséges megismerési felhatalmazások mellett kiemelt fontosságú az adott munkakör elvégzéséhez szükséges *végzettség, tudás és gyakorlati tapasztalat megléte*, mely kérdés fontosságát a napjainkban tapasztalható munkaerő elvándorlás igazol. Ugyanígy fontos a *szerződő partnerek alkalmazottainak felhatalmazása*, és a munkavégzés szabályozása, felügyelete, vagy a *távozó üzemeltető vagy biztonságért felelős személy elszámoltatása, és hozzáférési jogosultságainak azonnali visszavonása*.[6]

Az üzemeltetési és védelmi rendszabályok csak *a jóváhagyó szerv vagy szervezetek engedélyével, a szükséges dokumentálási és képzési eljárások után változtathatók*. Ez a követelmény a sok mérgelődést okozó „így szoktuk" vagy „azt mondták, így csináljam" egyszerűsítések által okozható károk megelőzését célozza.

A rendszerekért vagy szolgáltatásokért felelős vezetőknek *meg kell akadályozni a meghatározott üzemeltetési és védelmi rendszabályok egyszerűsítését, felülírását, és meg kell akadályozni az engedély nélküli változtatásokat*, így egyszerűen elkerülhető, hogy például ellenőrzés során derüljön ki, hogy a pontosnak vélt konfigurációs nyilvántartás a néhány évvel korábbi változásokat nem tartalmazza. A követelmény teljesítéséhez *kulcskérdés a szabályozott munkakör és munkavégzés, az oktatás és időszakos továbbképzés és az ellenőrzés*.

Az üzemeltető, biztonságért felelős és a felhasználói állományt a rájuk vonatkozó kötelezettségekről, feladatokról, az őket érintő *üzemeltetési és biztonsági körülmények változásáról rendszeres időnként tájékoztatni kell*. A tájékoztatással megelőzhetők az ismerethiányra visszavezethető hibák, illetve meghatározhatók a tervezett változásokkal kapcsolatos feladatok, melynek egyik legfontosabb célja a váltásos rendben dolgozó állomány naprakész ismereteinek biztosítása, illetve felhasználói oldalon a zökkenőmentes munkavégzés támogatása.

Az elektronikus adatkezelő rendszer szabályos üzemeltetése és használata, valamint *az üzemeltetési és biztonsági problémák szabályozókban rögzített módon történő jelentése minden érintett személy feladata*.

Az üzemeltetésre és biztonságra vonatkozó adatokat az elektronikus adatkezelő rendszer üzemeltetése során folyamatosan ellenőrizni, elemezni és értékelni kell. Itt nem csak az elsőre gondolt biztonsági események utáni kutatás a legfontosabb szempont.

Az üzemeltetett eszközök meghibásodásainak típusa, gyakorisága, a kiesések összetétele, a forgalmi adatok változásai, a kiszolgáló elemek terhelési mutatóinak figyelemmel kísérése, vagy csak egyszerűen a szerverterem hűtési-fűtési rendszerének vagy a földelésnek az ellenőrzése is meglepetéseket előzhet meg, illetve segítheti a megelőző jellegű karbantartások tervezését, segíti a hálózati vagy eszköz szintű amortizációs cserék vagy kiegészítések tervezését, illetve az ehhez szükséges pénzügyi és egyéb területű erőforrások tervezését.

[6] A hozzáférési jogosultságok visszavonása feladat esetenként rosszul értelmezett, mert elvonja a figyelmet arról a tényről, hogy *a munkakör elhagyásának, és nem a munkahely elhagyásának esetét kell kezelni*.

Az elektronikus adatkezelő rendszert és üzemeltetési környezetét *meghatározott időszakonként, valamint változások előkészítésekor kockázatelemzéssel kell vizsgálni*.

Az elektronikus adatkezelő rendszereket specifikusan, az adott rendszerre vonatkozó rendben *biztonsági ellenőrzéseknek kell alávetni*. A biztonsági ellenőrzéseknek szükségszerűen át kell fogni az információbiztonság összes területét.

A kezelt adatok, a biztonsági környezet, a csatlakozó rendszerek függvényében ez *az ellenőrzés inkább ellenőrzési rendet kell, hogy jelentsen*. Az üzemeltető állomány ellenőrzésén kívül ide kell sorolni a különböző szintű elöljárói ellenőrzéseket és célellenőrzéseket, a hatósági ellenőrzéseket, illetékesség esetén a NATO, EU különböző biztonsági szervezeteinek ellenőrzéseit, ami az adminisztratív ellenőrzés mellett a mérnöki szintű elemzést, auditot, vagy összekapcsolt rendszerek esetén külső sebezhetőség elemzést is tartalmazhat, mely ellenőrzési típusok még tovább specializálhatók.

Változások csak jóváhagyott terv, kockázatelemzés és teszt, valamint tájékoztatás és képzés után végezhetők.

A RENDSZERBŐL TÖRTÉNŐ KIVONÁS BIZTONSÁGI SZEMPONTJAI ÉS FELADATAI

Kevés esetben mondható ki, hogy meghatározott időszakra létrehozott elektronikus adatkezelő rendszer – annak elemeivel együtt – az adott feladat teljesítése után valóban eléri a rendszerből történő kivonást, így biztonsági szempontból kiemelt fontosságú az adatkezelő rendszerekkel és az adatokkal való teendők említése.

Az elektronikus adatkezelő rendszer üzemeltetésből történő kivonása csak *az engedélyező szerv, szervezetek vagy személyek engedélyével történhet*. Az engedély nélküli végzett műveletek eredménye könnyen okozhat hálózati szinten váratlan eseményeket, problémákat főleg a szükséges üzemeltetési információk hiánya, rendszerdokumentumok pontatlansága esetén. Emiatt nyilvánvaló, hogy egy hardver vagy szoftver kivonása a rendszerből, vagy egy rendszer leállítása *csak az egész információs környezet ismeretében a szükséges előkészítési, és összehangolási lépések után végezhető*.

A rendszerből történő kivonást *jóváhagyott eljárással kell végrehajtani*, melynek tartalmaznia kell az *összes dokumentummal és adattal, valamint az elektronikus adatkezelő rendszer hardver és szoftver elemeivel kapcsolatos biztonsági követelményeket* és védelmi rendszabályokat.

A rendszerből történő kivonás tervezésekor *meg kell határozni a kezelt adatok biztonsági osztályának megfelelő eljárást az adatok más rendszerbe történő áttelepítéséhez, tárolásához vagy archiválásához*.

A rendszerből történő kivonás szakfeladatait *csak az arra feljogosított személyek végezhetik*. Az eszközökkel kapcsolatos műszaki feladatok, adatmentések során előfordulhat nagymennyiségű üzemeltetési vagy felhasználói adattal történő művelet, ami lényegesen nagyobb információs katasztrófát okozhat, mint korábban egy felhasználó által elérhető adatokkal történő biztonsági probléma.

A rendszerből történő kivonáskor meg kell határozni a hardver és szoftver elemekre vonatkozó újrahasznosítási, adattörlési, megsemmisítési vagy egyes műveleteket tiltó rendszabályokat. Az elektronikus adatok megbízható törlése külön tárgyalást igénylő témakör. Az információs kockázatok egy bizonyos szintjén már előfordulhat, hogy *a szervezeti érdek csak a fizikai megsemmisítést tartja elfogadhatónak, ami külön technikai megoldásokat fog igényelni*, mely megoldások erőforrás szükséglete nem biztos, hogy minden esetben bekerült a „tervezői látókörbe”.

Tárolás vagy archiválás esetén *meg kell tervezni és ki kell alakítani a szükséges biztonsági környezetet, és adatkezelő infrastruktúrát úgy, hogy bekövetkező technikai és eljárási*

változások esetén is biztosított legyen az adatok hozzáférése és kezelhetősége. A technológia rohamos idejű fejlődése néhány év alatt is képes váratlan helyzeteket produkálni, amelynek egyik jelensége lehet, hogy adott fájlformátum, megjelenítési mód, vagy szoftver a korszerűbb információs környezetben már nem alkalmazható, csatlakozási felületek, átalakítók már kezelhetők. Ilyen esetben meglepetéseket okozhat például az elektronikus hitelesítés szolgáltatás esetében a szolgáltatót terhelő, jogszabály által meghatározott tízéves visszakereshetőségi kötelezettség, vagy rejtjelzett adatok tárolása esetén a kulcsmenedzsment kérdések bonyolultsága. Emiatt külön feladat – és nem csak biztonsági szempontból tekinthető kihívásnak – az adatok és az adatkezelési környezet huzamosabb időn keresztül történő biztosítása.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A cikk a Szabályzatban megfogalmazandó fontosabb elektronikus információ biztonsági kérdések megvilágítását célozta a híradó és informatikai szakterületi feladatok támogatása érdekében.

Az életciklushoz kötve bemutatott fontosabb biztonsági követelmények és szempontok jól mutatják a védelmi rendszabályok sokszínűségét, bonyolultságát. Nyilvánvaló, hogy *a biztonsági kockázatok kizárásához ilyen szintű elektronikus információvédelmi rendszabályok nem lehetnek elégségesek*, illetve az adatkezelés sajátosságai sem teszik lehetővé, hogy a harcászati rádiók szintjétől a szövetségesi együttműködést biztosító stratégiai szintű szolgáltatásokat együttesen ilyen röviden lehessen bemutatni.

Összefoglalásként elmondható, hogy az elektronikus adatkezelő rendszerek kialakítása üzemeltetése és rendszerből történő kivonása *lényegesen bonyolultabb feladat, mint az a köztudatban ismert*. Az összetett üzemeltetés támogató feladatok előrelátó erőforrás tervezés hiányában csak ideig-óráig lehetnek sikeresek, illetve az is látható, hogy *mekkora jelentősége van a pontosan megfogalmazott követelményeknek*, ami a híradó és informatikai szakfeladatok hadműveleti területről történő támogatásának fontosságát húzza alá.

A kockázatelemezés és kezelés, az ellenőrzés, a szabályozás, a felelősségek azonosítása, a változások követése és rögzítése, valamint a képzés *az életciklus állomásokon egységesen megjelenő feladat kell, hogy legyen*. A napi életben előállhat olyan helyzet, amikor *a felső szintű szabályozó keretjellege miatt pontosan nem alkalmazható a katonai képességek híradó és informatikai rendszereinek védelmére*. Ilyen esetekben fontos szerepe van a szakképzett biztonsági menedzsmentnek, annak érdekében, hogy *kidolgozzák a szükséges helyettesítő megoldásokat, azokat ellenőrizzék, és a megoldás engedélyezése érdekében végezzék az illetékes hatóságok felé a szükséges adminisztratív feladatokat*. Ez a megoldás lényegesen hatékonyabb, mint az adott probléma megküldése a hatóság felé, mert *az esetek nagy részében a katonai specialitások, működési jellemzők vagy a környezet pontos ismerete nélkül a legnagyobb jóindulattal sem könnyű jó szakmai tanácsokat adni*.

A feladatok összetettsége felvet egy újabb szempontot: *a szervezeten belüli és a szervezetek közötti együttműködés kérdését* és fontosságát. Korábban a kevesebb feldolgozott adat, kevesebb hálózati szolgáltatás miatt viszonylag egyszerűbb volt a honvédelmi szerv vezetőjének helyzete. Az üzemeltető informatikai állomány, a híradó eszközök és komplexumok kezelő állomány, valamint a számítástechnikai titokvédelmi felelős kijelölésével a feladatok nagy része „kipipálható” volt. Napjainkban ez a helyzet lényegesen bonyolultabbá vált. Gyakori az a helyzet, hogy a híradó és informatikai üzemeltetők, a biztonságért felelős személyek más szervnél vagy szervezetnél találhatók, illetve *a hálózatok szolgáltatásai és üzemeltetés szervezeti határokon átnyúló feladatokat jelent*. Ezen összetettség miatt a szervezeti vezetők feladata is megváltozott: az eddig elégséges sorszámos rendelkezés kiadása helyett a szervezeti együttműködés kérdéseit is kezelni kell, ráadásul nem csak vezetői szinten történő

kapcsolattartásra szűkítve, mert a hálózatokba történő gondolkodás megköveteli az üzemeltető és biztonsági állomány közvetlen kapcsolattartását is!

A szakfeladatok bemutatása rámutat arra is, hogy szükség van a terminológiai kérdések fontosságának említésére. A hadtudomány egyik soros feladata a szakkifejezések megnyugtató rendezése, beleértve a híradó és informatikai szakterületet is.

Jelen cikk megjelenésekor a szakkifejezések kérdése még nyitott, így szükség van annak jelzésére, hogy az alkalmazott „elektronikus adatkezelő rendszer" kifejezés a tervezett Szabályzatban alkalmazott, egyeztetett terminológiai gyakorlatnak megfelelő kifejezéssel helyettesítendő, tartalmi szempontból lefedve az elektronikus adatkezelés területeit.

Felhasznált irodalom

[1] A Magyar Honvédség Informatikai Szabályzata, Ált/210, 1993

[2] 218/2013 HVKF paranccsal módosított 209/2013 HVKF parancs a Magyar Honvédség Híradó - Informatikai Szabályzatának kidolgozásáról

[3] 346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról, 6. §, 28-31. §.

[4] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)

[5] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

[6] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

[7] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról, 15. §.

[8] A Honvéd Vezérkar híradó, informatikai és információvédelmi csoportfőnökének 9/2012. (HK 14.) HVK HIICSF szakutasítása a Minősített Elektronikus Adatkezelő Rendszer Üzemeltetés Biztonsági Szabályzatára vonatkozó általános követelményekről

[9] A Honvéd Vezérkar híradó, informatikai és információvédelmi csoportfőnökének 10/2012. (HK 14.) HVK HIICSF szakutasítása a Minősített Elektronikus Adatkezelő Rendszer ellenőrzésére vonatkozó általános követelményekről, 5, 7, és 10. p.

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Kende György
kende.gyorgy@uni-nke.hu

GONDOLATOK MTA DOKTORI, EGYETEMI TANÁRI ÉS BOLYAI ÖSZTÖNDÍJ PÁLYÁZATOKRÓL

Absztrakt

Jelen publikációban a szerző bírálóként, előterjesztőként, és bíráló bizottsági tagként gyűjtött tapasztalatait adja közre az egyetemi tanári, MTA doktori és a Bolyai ösztöndíj pályázatok vonatkozásában. Áttekinti a különböző szabályzókban foglalt követelményeket, és rámutat azok teljesítésének nehézségeire. Mindhárom pályázatnál az egyik fontos elvárás a nemzetközi ismertség és elismertség bemutatása. Ezért a szerző azt javasolja, hogy teremtsük meg a kereteket a pályázók segítésére, például kutatói szabadsággal, külföldi publikációs lehetőségekkel, nemzetközi konferenciákon való részvétel lehetőségével, megfelelő nemzetközi (NATO) munkacsoportokba való delegálással, vagy más eszközökkel. A szerző arra a következtetésre jut, hogy a Bolyai ösztöndíjnak, az egyetemi tanári kinevezésnek, és az MTA doktora cím elérésének egy egymásra épülő, egységes egészet képező folyamatot kell képeznie, mely alulról felfelé építkezik, világos ívű, átlátható, és logikus láncot alkot.

In this paper the author sums up his experience as an evaluator, proposer, reviewer and committee member regarding professorship, doctoral (Doctor of the Hungarian Academy of Science, DSc) and the Bolyai scholarship applications. An overview of the requirements clearly shows the difficulty of performance. All three sets of requirements contain the major demands of an international reputation. The author recommends to create a framework for supporting applicants by different means, such as sabbaticals, international publishing opportunities, opportunities to participate at international conferences, to attend relevant international (NATO) working group, or other means. The author concludes that processes of application for Bolyai scholarship, professorship and DSc title should be built on one another. The processes must form a coherent whole, from the bottom-up, be transparent and show a clear and logical chain.

Kulcsszavak: *MTA doktora, egyetemi tanár, Bolyai ösztöndíj, publikálás, konferenciák ~ Doctor of The Hungarian Academy of Science (DSc), professorship, Bolyai scholarship, publication, conferences*

BEVEZETÉS

A magasan kvalifikált tudományos és oktatói utánpótlás kibontakozásának segítése mindig is egyik legnemesebb feladata volt az idősebb kollegáknak. A kettős juttatás tilalma miatt – ha nem is a Nemzeti Közszolgálati Egyetemen egészében, de a Hadtudományi és Honvédtisztképző Karon mindenképpen – jelentősen csökkent a vezető oktatók száma. Az elmúlt években (2007 óta) több MTA doktori cím megszerzésére irányuló cselekménynek voltam részese előterjesztőként és bírálóbizottsági tagként; továbbá bírálok Bolyai ösztöndíj pályázatokat, és értékelem az éves beszámolókat (2010 óta). Nem ritkán megesik, hogy egyetemi tanári pályázatok írásakor is fordulnak hozzám oktató kollegák konzultáció céljából (2005 óta). Ezért úgy gondoltam, hogy megosztom a három témakörben készült pályázatokkal kapcsolatos ismereteimet. Jelen publikációval az a célom, hogy összegezzem a fenti kérdéskörökben összegyűlt tapasztalataimat, és kisebb-nagyobb javaslatokat tegyek a folyamatok jobbítására. Szeretném azt is, ha az alábbi dolgozat segítené a fiatalabb kollegák pályázati munkáját.

NÉHÁNY OKTATÓI ÉS TUDOMÁNYOS PÁLYÁZATRÓL

Egyetemi tanári pályázatok[1]

Az egyetemi tanári pályázatok általános követelményei között – többek között – az szerepel, hogy a pályázatra összességében maximum 200 pont adható, míg az elérendő minimum 150 pont. A 150 pont a Magyar Felsőoktatási Akkreditációs Bizottság (MFAB) támogatása elnyerésének szükséges, de nem feltétlenül elégséges feltétele.

A hadtudományt illető pontozási szempontok (követelmények)[2] közül kiemelem – teljesítésük nehézsége okán - a külföldi (nemzetközi) vonatkozásúakat. Ilyenek:

Minimum 5 idegen nyelvű, tudományos folyóiratban megjelent publikáció, ezek közül legalább 2 egyszerzős; rangos külföldi – nemzetközi konferencia szervezése; nemzetközi K+F programokban részvétel; pályázati eredményesség, (pl. nemzetközi kutatási projektvezetés).

Továbbá: felkérések nemzetközi konferencia tisztségekre, plenáris előadásokra; választott rangos tisztségek; nemzetközi tudományos folyóiratnál szerkesztő-bizottsági tagság, megjelenés, elismerések, díjak nemzetközi szakmai fórumon.

Az oktatást illetően: legalább féléves előadás, szeminárium tartása idegen nyelven, külföldi vendégtanári meghívás.

A fenti külföldi vonatkozású értékelési szempontok jelentős részének teljesítése nem kizárólag, és talán nem is elsősorban a pályázótól függ, hanem attól, hogy a pályázónak milyen jellegű a kutatási területe, milyen beosztásban dolgozik, és hogy egyáltalán hozzájut-e ilyen lehetőségekhez.

Úgy gondolom, hogy a nemzetközi ismertség és elismertség követelményeinek teljesítése tekintetében, mindenekelőtt a lehetőségekhez való hozzáférést illetően a potenciális pályázóknak jelentős segítséget kell kapniuk.

A Bolyai ösztöndíjnak, az egyetemi tanári kinevezésnek, az MTA doktora cím elérésének egy egymásra épülő, egységes egészet képező folyamatot kell képeznie. A követelmények megfogalmazásában a hadtudományi szakembereknek jelentős szerepük van. E követelményeknek alulról felfelé építkező, világos ívű, átlátható, logikus láncot kell alkotniuk, és azt kell meggyőzően mutatniuk, hogy az út teljes egészében bejárható.

---

[1] A Magyar Felsőoktatási Akkreditációs Bizottság (MFAB) honlapja. Egyetemi tanári pályázat. http://www.mab.hu/web/index.php?option=com_content&view=article&id=431:egyetemi-tanari-palyazat&catid=82:beadvanyok&Itemid=634&lang=hu Letöltve 2013.augusztus 5.

[2] Egyetemi tanári pályázat véleményezés. A Magyar Felsőoktatási Akkreditációs Bizottság honlapja, 15. oldal. http://www.mab.hu/web/doc/beadvanyok/EtSzbsz_130507.doc Letöltve 2013. augusztus 5.

Néhány esetben előfordult, hogy kollegák hozzám fordultak egyetemi tanári pályázatuk megírása kapcsán – vagy azért, hogy megnézzék az én 2004-ben benyújtott pályázatomat (ami azért mostanra már elég régi), vagy azért, hogy nézzem át a pályázatukat benyújtás előtt. Itt egy kicsit szeretnék megállni azon a kérdésen, hogy helyes-e, célszerű-e egy idősebb (tapasztaltabb, már egyetemi tanár) kollegát megkérni pályázatunk átnézésére, etikus-e ez.

A helyességet illetően: a pályázók egy része, nem akarván zavarni vagy másnak feladatot generálni, érthető és tapintatos módon ódzkodik attól, hogy egy idősebb kollegától tanácsot kérjen – pedig ebből csak előnye származhat, és biztos vagyok benne, hogy az ilyen kérések az esetek döntő többségében kedvező fogadtatásra lelnek. Egy külső és tapasztaltabb szemlélő minden bizonnyal hasznos észrevételeket tud tenni, bizonyos értelemben a leendő bíráló szemével képes nézni a pályázatot. És ami még igen lényeges: egy ilyen konzultáció teljesen informális, következmények nélküli, és a pályázatot író kollegának teljesen szabad keze van abban, hogy milyen javaslatokat fogad el, és milyeneket nem. Úgy gondolom, hogy ilyen segítségét kérni nemcsak helyes, hanem hasznos is. Itt is igaz az, hogy több szem többet lát.

A konzultáció (pályázat átnézés) etikus voltát illetően: induljunk ki abból, hogy véleményt kérni általában is és az esetek döntő többségében is etikus. Olyan pályázatoknál, ahol többen versengenek (pl. a Bolyai ösztöndíj esetében általában négy pályázatra jut egy elnyerhető ösztöndíj) a pályázó nem tudhatja, hogy a többiek kérnek-e ilyesféle konzultációt. Az a tapasztalatom, hogy nem kevesen kérnek, és aki nem kér, az kisebb hátrányba kerülhet. Mi ennek a hátránynak a tartalma? Nemegyszer tapasztalom, hogy a pályázat a lényeget tekintve jó vagy igen jó, valós eredményeket, megalapozott elképzeléseket tartalmaz – de az összeállítás, a hangsúlyok nem jó helyen vannak, a szerkezet is laza, és a pályázat akár a kiváló tartalom ellenére sem igazán meggyőző. Természetesen a bírálónak a lényegre kell figyelnie és az értékeket kell észrevennie, de nem hiszem, hogy a bírálók teljes mértékben függetleníteni tudják magukat az apróságoktól, és ha ilyeneket, esetleg pontatlanságokat észlelnek, akkor az összbenyomásra feltehetően és többé-kevésbé érthetően kevesebb pontot adnak. Összességében tehát az ilyesféle konzultációban semmilyen etikai problémát nem látok.

Pályázat az MTA doktora tudományos címre

Az MTA doktora tudományos címre (Doctor Academiae Scientiarum Hungaricae, rövidítve: DSc, a továbbiakban: az MTA doktora) történő pályázat benyújtására vonatkozó tájékoztató az MTA honlapján olvasható.[3] Erről a webhelyről az MTA IX. Gazdaság és Jogtudományok Osztályra kattintva elérhető az osztály doktori követelményrendszere, továbbá az osztály által elfogadott folyóiratlisták, beleértve a Hadtudományi Bizottság folyóiratlistáját is. Látható, hogy a követelmények teljesítése és azok elvárt módon való bemutatása (beleértve a minimumkövetelményeket) a pályázótól komoly erőfeszítést igényel. Az elmúlt néhány évben az MTA Hadtudományi Bizottsága három pályázó teljesítményét nem ítélte megfelelőnek (kevés pontot adott). Ennek következményeként az MTA IX. osztálya sem támogatta ezeket a pályázatokat. A szóban forgó három pályázat közül kettőnek előterjesztője voltam, és bátran mondhatom, hogy ezek egyáltalán nem voltak esélytelenek, de mindkettőnél gond volt a minimumkövetelmények teljesítésével vagy azok értelmezésével. Ezért azt javaslom, hogy a jövőben minden pályázó keressen a beadás előtt egy vagy akár több (lehetőleg MTA doktora címmel, és lehetőleg Hadtudományi Bizottsági tagsággal rendelkező) kollegát, akivel kellő mélységben konzultálhat a benyújtandó pályázatáról. Célszerű lenne, ha ezt a gondolatot a Hadtudományi Bizottság is támogatná, ezzel mintegy bátorítást adva a pályázni készülő kollegáknak, nevezetesen, hogy a potenciálisan szóba jöhető kollegák a kérésüket korántsem fogják tehernek tekinteni.

[3] Tájékoztató Az MTA doktora tudományos címre történő pályázat benyújtásához. http://www.mta.hu/cikkek/tajekoztato_az_mta_doktora-12563 1 Letöltve: 2013. augusztus 5.

A Hadtudományi Bizottság által kijelölt előterjesztők elektronikus felületen tölthetik le a benyújtott anyagokat, és véleményüket (előterjesztésüket) is ugyanerre a felületre kell feltölteniük. A letöltött anyagok közül a legfontosabbak kiválasztása, azok kinyomtatása, rendezése, továbbá maga a lényegi munka, egy-egy pályázat előterjesztésének elkészítése igen sok munkaórát vesz igénybe. Ehhez képest a pályázóval való, beadás előtti konzultáció néhány órája nem is lenne olyan jelentős időráfordítás, és úgy gondolom, hogy hatékonyan segítené a pályázót az anyagok összekészítésében.

Nemritkán hallani azt a véleményt, hogy az Nemzeti Közszolgálati Egyetemen (de a Hadtudományi és Honvédtisztképző Karon mindenképpen) kevés az MTA doktori címmel rendelkező oktató, és kevés az egyetemi tanár is. Az egyetemi tanári ambíciók teljesülésének egy lehetséges útja az, hogy a kollega először az MTA doktora címet szerzi meg, minthogy az jelentősen megkönnyíti az egyetemi tanári pályázat elkészítését (az MTA doktora cím bizonyítja a tudományos kiválóságot).

Úgy gondolom, helyes lenne valamilyen kereteket létrehozni és a megfelelő formákat meglelni ahhoz, hogy támogassuk az MTA doktora címre pályázókat, például kutatói szabadsággal, külföldi publikációs lehetőségekkel, és külföldi konferenciákon való részvétel lehetőségével, vagy megfelelő nemzetközi (NATO) munkacsoportokba való delegálással. A pályázó kollégákat célszerű lenne „helyzetbe hozni", mindenekelőtt a külföldi ismertség és elismertség tekintetében. Úgy gondolom ugyanis, hogy ezt magától a pályázótól elvárni nem feltétlenül helyes, a pályázónak nem az ügyességével, a nyitott szemmel járással, a jó kommunikációval, azaz a saját menedzselésével kell kitűnnie (ilyen követelmény egyébként sincs), hanem a tudományos teljesítményével. Helyesnek tartanám, ha az arra érdemes kollegák segítése valamilyen szabályozott formában történne, mert ez kiszámíthatóságot és biztonságot adna a pályázóknak, és bizonyos fokú tervezhetőséget az Egyetemnek (karoknak).

Az MTA doktori pályázat bonyolultságát bemutatandó felsorolom, hogy a pályázónak (vagy kérelmezőnek, ez az MTA Doktori Szabályzat 3.§ (2) bekezdésének szóhasználata) milyen anyagokat kell összeállítania:

(1) szakmai önéletrajz,
(2) MTA doktori értekezés,
(3) a doktori értekezés összefoglalója,
(4) a tudományos munkásság összefoglalása,
(5) a tudományos publikációkra való hivatkozások jegyzéke,
(6) a jelentős publikációk listája,
(7) a tudományos publikácik jegyzéke az MTMT[4] nyilvános adatbázis alapján,
(8) publikációs adatlap,
(9) a tudományos közlemények áttekintő adatai,
(10) tudományos közéleti adatlap.

A fenti anyagokat az előterjesztőnek az alábbi előírások alapján kell bírálnia:

(1) a doktori eljárásokban 2013. szeptember elsejétől alkalmazandó szabályzatok (41 oldal), benne a 3. oldaltól az MTA Doktori Szabályzata[5];
(2) ügyrend az MTA Gazdaság- és Jogtudományok Osztályának az MTA Doktora tudományos cím megszerzéséért indított eljárásban való közreműködéséről (101 oldal)[6],
(3) ügyrend az MTA IX. Osztály Hadtudományi Bizottsága közreműködéséről az MTA doktora tudományos cím megszerzéséért indított eljárásban (8 oldal, hatályos 2013. szeptember 1-től)[7];

[4] Magyar Tudományos Művek Tára. https://www.mtmt.hu Letöltve: 2013. augusztus 5.
[5] http://mta.hu/data/cikk/12/28/61/cikk_122861/doktori.pdf Letöltve: 2013. augusztus 5.
[6] http://mta.hu/data/cikk/12/14/51/cikk_121451/IX.pdf Letöltve: 2013. augusztus 5.
[7] http://www.mtahtb.zmne.hu/PDF/HB_doktori_ugyrend.pdf Letöltve: 2013. augusztus 5.

(4) a Hadtudományi Bizottság speciális MTA doktori követelményei (16 oldal)[8], továbbá;
(5) az MTA IX. Gazdaság- és Jogtudományok Osztálya követelményei a doktori műre és a tézisekre vonatkozóan (12 oldal)[9].

A fenti öt szabályzó összesen 178 oldalt tesz ki, amelynek egyes részeit az előterjesztőnek igen alaposan, szinte betűről-betűre el kell olvasnia, megértenie, és alkalmaznia. Más részeket elegendő csupán elolvasni az általános kép megértéséhez. Szeretném hozzátenni, hogy a fenti szabályzók szinte folyamatosan (1-2-3 évente) frissülnek, jellemzően és általában a magasabb követelménytámasztás irányába. Hozzáteszem még azt is, hogy az előterjesztőnek egyáltalán nem könnyű kiigazodnia a különböző, a szándékok szerint egybevágó előírásokban, a pontozási szempontokban és az egyes táblázatokban.

A fenti öt szabályzó kigyűjtésével két célom volt:

- Az egyik, hogy az MTA doktora cím megszerzésére törekvő kollegák lássák ezeket a szabályzókat, és azt ajánlanám nekik, hogy ezeket igen alaposan tanulmányozzák, és ítéljék meg saját maguk, hogy várhatóan milyen eséllyel pályázhatnak a cím megszerzésére. Különösen felhívnám szíves figyelmüket a minimumkövetelmények teljesítésére.
- A másik célom az volt, hogy javaslatot tegyek: az MTA doktori követelményrendszert érdemes lenne összehasonlítani a Magyar Felsőoktatási Akkreditációs Bizottság egyetemi tanári követelményrendszerével. Úgy gondolom, hogy ez a korántsem kis munka viszonylag egzakt módon, számokkal, táblázatok szerkesztésével elvégezhető, és az eredmény várhatóan több mindent megmutatna. Igazolhatná (vagy cáfolhatná) azt a becslésemet, hogy ez a két követelményrendszer minőségileg és tartalmában nagyon is hasonlít egymásra, és az eltérések jelentős része mennyiségi. Egy ilyen elemzés jól áttekinthető képet adna az egyetemi tanári kinevezésre és az MTA doktori címre pályázó oktatóknak, segítené az önértékelést, és felvázolná a fenti törekvések eléréséhez vezető lehetséges útvonalakat.

Bolyai ösztöndíj[10]

A Bolyai ösztöndíj fontosságának bemutatásához idézem Glatz Ferencnek, az MTA volt elnökének egy nyilatkozatát[11] 2000-ből: *„A Bolyai-ösztöndíj az akadémiai doktori réteg* (jelenleg mintegy 2300 fő) *utánpótlását jelenti* és összeköti a *lokális autonómiák* által adott PhD-végzettséggel rendelkező fiatal kutatókat az *országos (nemzeti) autonómiával,* az Akadémiával.

Megállapítható, hogy a Bolyai ösztöndíj jól illeszkedik a hazai ösztöndíjak láncolatába (Békésy, Magyary, Bolyai, Széchenyi) és betölti szerepét a tudományos utánpótlás képzésében (PhD, MTA doktora cím, MTA levelező ill. rendes tagja).

A Bolyai-ösztöndíj *hidat képez* az országos autonómiában döntő szerepet játszó akadémiai doktorok, akadémikusok és a fiatal kutatói generáció között. Biztosítani kívánja a tudományban a különböző generációk együttdolgozását és együttgondolkodását."[12]

A Bolyai ösztöndíj pályázatoknak két bírálója van, egy bíráló maximum 50 ponttal értékelheti a pályázatot. Ez az alábbi módon tevődik össze: (1) A pályázó tudományos eredményeinek értékelése publikációk, szabadalom, ill. alkotás alapján, adható pontszám 0-10 pont. (2) A pályázó tudományos eredményeinek hatása, adható pontszám 0-10 pont. (3) A

[8] http://www.mtahtb.zmne.hu/PDF/2_sz_mell_HB_spec_doktori%20_elfogadott_12_10_08.pdf Letöltve: 2013. augusztus 5.
[9] http://www.mtahtb.zmne.hu/PDF/1_sz_mell_IX_O_Dokt_kov_DT.pdf Letöltve: 2013. augusztus 5.
[10] http://mta.hu/cikkek/?node_id=22421 Letöltve: 2013. augusztus 5.
[11] http://mta.hu/cikkek/bolyai-osztondij-126361 Letöltve: 2013. augusztus 5.
[12] A dőlt betűs kiemelések a 10. sz. lábjegyzetben szereplő MTA honlapról vannak.

tervezett kutatómunkát illetően: a pályázó előzetes kutatási eredményei a kutatási témakörben, adható pontszám: 0-5 pont; időszerűsége, adható pontszám: 0-5 pont; kidolgozottsága, adható pontszám: 0-5 pont; kivitelezhetősége az ösztöndíj időtartama alatt, adható pontszám: 0-5 pont; összesen 20 pont. (4) A pályázó személyének értékelése összbenyomás alapján, adható pontszám: 0-10 pont. Látható, hogy az összbenyomás alapján adható pontszám az összes adható pontszám 20%-át teszi ki – ez bizony nem kevés, az egyetemi tanári és az MTA doktori pályázatoknál ilyen szempont nincsen.

A pontozással kapcsolatban megemlítem még, hogy az MTA IX. osztály Bolyai János Kutatási Ösztöndíj Szakértői Kollégiumának bírálói számára kiadott pontozási segédlet is komoly hangsúlyt helyez a külföldi vonatkozásokra. Ilyenek: minősített nemzetközi publikáció és nemzetközi konferencia megmérettetés, nemzetközi hivatkozások, nemzetközileg is újdonságnak számító, nemzetközi kutatásokkal szinkronban lévő, nemzetközileg is jelentős eredmény esélye.

A Bolyai ösztöndíj pályázat – a várható sikeresség, azaz a pályázat elnyerése szempontjából is – jelentősen különbözik az egyetemi tanári és az MTA doktori pályázatoktól. Az utóbbiaknak ugyanis „csak” a bírálók szűrőjén kell átmenniük, továbbá, ezen pályázatok eredményessége az esetek döntő többségében nem függ más pályázatoktól. A Bolyai pályázatoknál – minthogy ezek versengenek - általában az adott évben benyújtott egy, esetleg két legjobb, azaz legmagasabban pontozott pályázat nyer. Így elképzelhető, hogy valamelyik évben több igen színvonalas pályázatból is kiesik néhány, míg egy másik évben kevesebb jó pályázat érkezik be, és alacsonyabb pontszámmal is el lehet nyerni az ösztöndíjat. Ennélfogva logikus, helyes, és javasolható, ha egy valamelyik évben sikertelen pályázó a következő évben, években is pályázik, hiszen az adott évben az adott mezőnyben kell a legjobbnak vagy második legjobbnak lenni.

ÖSSZEGZÉS

Összegeztem tapasztalataimat, és igyekeztem javaslatokat tenni az eredményesebb pályázatírás céljából. Javaslataim lényege, hogy helyes lenne olyan kereteket és feltételeket teremteni, amelyek hatékonyan segítik a pályázati munkát. Ennek egyik fő eleme, hogy mind a három pályázatnál igen lényeges a külföldi ismertség és elismertség, a kutatások nemzetközi hatása, ezért a pályázó kollegák publikációinak külföldi megjelenését, külföldi konferenciákon való részvételét segíteni kell. További támpontokat adhat a pályázóknak, hogy áttekintettem az egyes pályázatok fontosabb bírálati szempontjait. A fiatalabb kollegáknak egészében és részleteiben is ismerniük kell ezeket a szempontokat, az eredményes pályázatokhoz vezető utakat, és bíztatást kell kapniuk, hogy ezek az utak nyitottak, átláthatóak, járhatóak, és ezeket érdemes is bejárniuk. Mert hajózni kell. Navigare necesse est.

Felhasznált irodalom

[1] Tájékoztató az MTA doktora tudományos címre történő pályázat benyújtásához. Az MTA honlapja. http://mta.hu/cikkek/tajekoztato_az_mta_doktora-125631 Letöltve: 2013. augusztus 5.

[2] Egyetemi tanári pályázat. A Magyar Felsőoktatási Akkreditációs Bizottság honlapja. http://www.mab.hu/web/index.php?option=com_content&view=article&id=431:egyetemi-tanari-palyazat&catid=82:beadvanyok&Itemid=634&lang=hu Letöltve: 2013. augusztus 5.

[3] A Magyar Tudományos Akadémia Doktori Szabályzata http://mta.hu/data/cikk/12/28/61/cikk_122861/doktori_szabalyzat_modosiitasokkal_egyseges_szerkben_20111206_(2).pdf Letöltve: 2013. augusztus 5.

[4] A Bolyai ösztöndíj. http://mta.hu/cikkek/?node_id=22421 Letöltve: 2013.augusztus 5.

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Kolonics Gábor
kolonicsg@yahoo.com

UV PROTECTING CAPABILITY TESTING OF THE SUNSCREEN PRODUCTS MADE FROM NATURAL SUBSTANCES WITH SELF TESTING

Abstract

Both in Hungary and in missions there is an increased risk of high ultraviolet radiation. It is a complex task to prevent UV radiation and primary prevention with an important element of using sunscreen products constitute an important part of it. The advanced sunscreen products, as part of primary and secondary prevention planned by the author, play an important role in military health protection. These substances are characterised by being effective, of natural origin, easily producible in large quantities, cheap, having non-toxic and antioxidant properties. Three types of natural sun protection creams were produced by the author, and it was proven by self-experimentation that the products are able to reduce the impact of the artificial UV source causing erythema.

Mind itthon , mind a missziókban fokozott kockázatot jelent a magas ultraibolya sugárzás. Megelőzése komplex feladat, melynek fontos része a primer prevenció, melynek fontos eleme a napvédő anyagok használata. A katonai egészségvédelemben a szerző által tervezett primer és szekunder prevenciós rendszer részeként fontos szerepet játszanak a korszerű napvédő anyagok. Ezeknek az anyagokra jellemző, hogy hatékonyak, természetes eredetűek, nagy mennyiségben könnyen előállíthatóak, olcsók, nem toxikus, antioxidáns tulajdonságúak. A szerző 3 féle természetes alapú napvédő krémet állított elő és önkísérlettel igazolta, hogy a készítmények képesek csökkenteni a mesterséges UV forrás erythema képző hatását.

Keywords: *UV radiation, personal UV protection, skin cancer, prevention, sunscreen ~ UV sugárzás, személyes UV védelem, bőrrák, misszió, megelőzés, napvédő*

INTRODUCTION

Skin cancer incidence is increasing worldwide in white populations in the last decades. Melanoma incidence increases faster than for any other cancer. Fortunately enough, the main risk factor which is responsible for these trends is known: solar and artificial UV. These circumstances predestine skin cancer as a target cancer for primary prevention. Primary prevention deals with strategies to avoid risk factors by means of changing people's behaviour and/or modifying environmental or artificial exposure conditions. One main recommendation which is always given in primary prevention of skin cancer is the use of sunscreens as a measure to reduce UV-exposure. However, this "simple" message has to be expanded upon in order to be sure that it does not lead to a wrong use of sunscreens and un-intended prolongation of exposure time. Primary prevention can effectively be combined with secondary prevention (early detection, screening) to reduce the burden of skin cancer and to decrease incidence, morbidity and mortality. [1]

Whilst the pathogenesis of skin cancer is multi-factorial, UV exposure is a major contributing factor. Squamous cell carcinomas (SCC) are directly related to chronic UV exposure over a lifetime and cutaneous melanoma seems to be related more to intermittent exposure. [2]

The ability of sunscreens to reduce sunburn is well established, confirmed by "extensive human experience." [1] It is important, particularly for public education, that although erythema is the end point used in the most standard evaluation of sunscreens, the prevention of sunburn does not equal prevention of all UV radiation–induced effects. It should be remembered that sunscreens are recommended for use as part of a "package" of sun protection strategies, including wearing tightly woven clothing, a hat, seeking shade, and avoiding peak exposure times. Sunscreens should not be used as a means of extending the duration of sun exposure. [3]

Safety of sunscreen compounds: Mutagenicity, photochemistry

There is no study to date showing that sunscreens are carcinogenic. However, chemical sunscreen compounds (also known as organic sunscreens) do absorb UV radiation. They then are in an excited state and must reenter the ground state by dissipating the absorbed energy by one of several processes. This energy is probably mostly dissipated harmlessly, but it is possible that the energy may be be involved in chemical reactions in the skin. The energy may be dissipated by fluorescence, phosphorescence, selfquenching, or heat. [3] The compounds may also undergo photofragmentation and photoisomerization or may transfer the energy to other molecules, including oxygen. Reactive oxygen species and other photoproducts may be formed. These highly reactive species could possibly react with a variety of cellular components, including DNA. [3]

PRODUCTION OF NATURAL SUN PROTECTION CREAMS

A sun protection cream containing three natural substances was produced. non ionic hydrophilic ointment was used as carrier. An nonionic hydrophilic ointment was prepared and used by the authors that contained grape seed oil and not paraffin oil. The composition per 100g: polysorbate 60 10 g, grape seed oil 10 g, cetylstearylalcohol 30 g, vaseline 70 g) The ointment contains no active substance. The product in not expected to cause any adverse effects, data on adverse effect is not known. Bath ointment for sensitive skin. It can also be used for hair and scalp.

Sunscreen product that contains one active component:

Maximum weight: 100 g
Fulvic acid: 5 %

Fulvic acid 5 g, Sterile distilled water 50 g, Unguentum hydrophilicum nonionicum 45 g. Fulvic acid was dissolved in sterile distilled water, added into the ointment base while stirring and the mixture was homogenized. The product was stored in a tightly closed plastic container. The ointment can be washed off with water, and is an O/W emulsion type.

Maximum weight: 100 g
Polyphenol: 10 %

Sunscreen product that contains two active components:

Maximum weight: 100 g
Fulvic acid: 5 %
Polyphenol: 5 %

SELF-EXPERIMENTATION

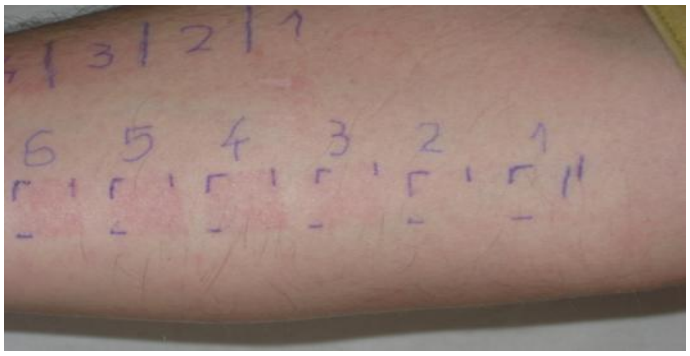
MED classification

For one person, the Minimum Erythema Dose (MED) is the amount of UV radiation that can cause observable erythema 8-24 hours after the irradiation of the skin. [4] In this case, the minimum irradiation time of the given source was examined that can cause mutation.

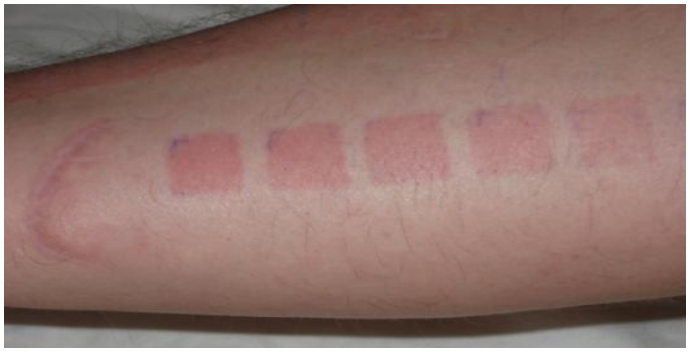
There was a distance of 35 cm kept between the source and the irradiated area. The irradiated area was the author's palmar surface of the right forearm. The skin surface was covered with a perforated cover plate, in which the perforation was divided into 6 parts. It was marked with numbers 1 to 6 in the following figure. The area marked with the number 1 was irradiated for 30 seconds, then each subsequent was irradiated half a minute longer, so the area marked with number 6 was exposed to UV radiation for 3 minutes.

Experience:

After 1.5 minutes immediately after the irradiation, erythema was formed (Figure 1). After the completion of the irradiation, 4 hours later, however, the mutation was formed in the total irradiated area. (Figure 2).



1. Figure Untreated surface immediately after the irradiation
Source: author



2. Figure Untreated surface 4 hours later
Source: author

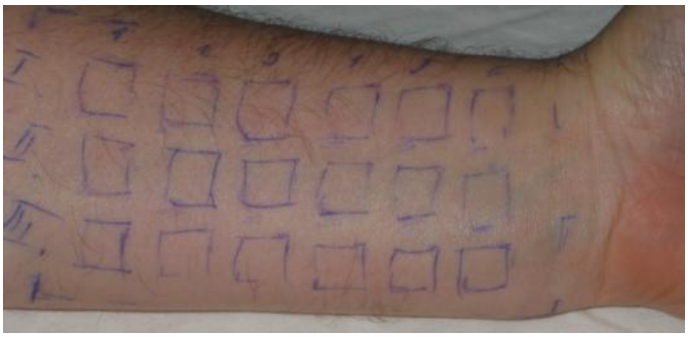
In the erythematous areas, burning sensation and pain occurred. 24 hours later, erythematous mutation was still visible and pain was felt but it slightly eased (Figure 3).

3. Figure Untreated surface the following day
Source: author

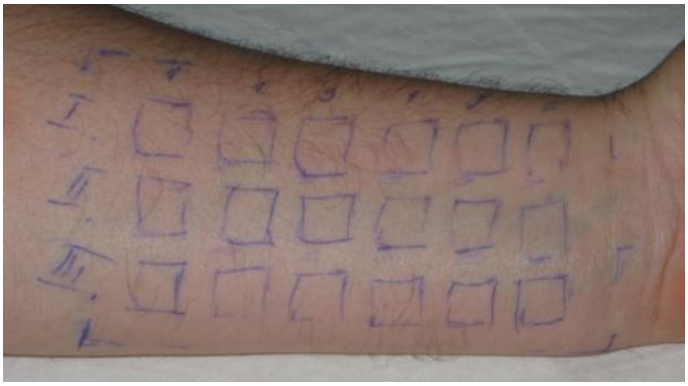
In the case of MED it may be stated that for the given UV source and distance it was less than 30 s.

Skin irradiation treated with one and two component sunscreen product.

The distance between the UV source and the irradiated area is equal to the previous ones. The irradiated area was the author's palmar surface of the left forearm. The skin surface was covered with a perforated cover plate, in which the perforation was divided into 3 x 6 parts. It was marked with numbers 1 to 6 in the following figure in 3 lines (I-II-III).



4. Figure Treated surfaces immediately after the irradiation
Source: author



5. Figure Treated surfaces 3.5 hours later
Source: author

The area marked with the number 1 was irradiated for 30 seconds, then each subsequent was irradiated half a minute longer, so the area marked with number 6 was exposed to UV radiation for 3 minutes.

However, this time the skin was treated with a natural substance product made by the authors before the irradiation. Line I was treated with a one component sunscreen product containing fulvic acid. Line II was treated with a one component sunscreen product containing polyphenol. Line III was treated with a two component sunscreen product containing fulvic acid and polyphenol.

6. Figure Treated surfaces the following day
Source: author

Experience:

Erythema did not occur (Figure 4.) immediately after the irradiation. There was no changes on skin 3.5 hours later (Figure 5.). Erythema still did not occur 24 hours later and the skin surface was undamaged (Figure 6). No pain occurred in any cases.

CONCLUSIONS

The experiments carried out showed that mutations on the untreated surface of the body induced by artificial ultraviolet radiation were prevented by the natural products on the treated surface. This basic experience therefore forms the basis for a series of experiment with the long-term goal of creating a product that can be produced on an industrial scale, which is cheap, natural, harmless to health, has no adverse effects and because of the content of natural active substances, it has positive physiological or possibly precancerous effects.

References

[1] Rüdiger Greinerta,, Mathieu Boniolb Skin cancer Primary and secondary prevention Progress in Biophysics and Molecular Biology 107 (2011) 473-476

[2] Magdum , Leonforte, McNaughton , Kim ,Patel , Haywood - Sun protection - Do we know enough? Journal of Plastic, Reconstructive & Aesthetic Surgery (2012) 65, 1384-1389

[3] Lim et al The health impact of solar radiation and prevention strategies Journal of The American Academy of Dermatology Vol. 41. , Iss. 1., 81-99, ISSN 0190-9622

[4] Protecting Workers from Ultraviolet Radiation-Paolo Vecchia, Maila Hietanen, Bruce E. StuckEmilie van Deventer, Shengli Niu ICNIRP 14/2007 ISBN 978-3-934994-07-2

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Kolonics Gábor – Kóródi Gyula
kolonicsg@yahoo.com - korodigy@freemail.hu

MELANOMA RISK ASSESMENT IS PART OF THE EXAMINATION OF MEDICAL SUITABILITY FOR MILITARY

Abstract

In this study, authors present a proposal for melanoma risk assessment that has been submitted by them, which will form an integral part of the examination of suitability of soldiers in Annex 16 to the Ministerial Decree 7/2006. (III. 21.). This legislation is under revision these days. The risk assessment is a very important pillar of the complex UV protection authors have supposed. By using it, we will be able to identify and closely monitor the high-risk individuals, and if necessary, we may direct them to special medical care in time.

Cikkükben a szerzők ismertetik az általuk benyújtott melanoma kockázatfelmérés javaslatot, amely a napjainkban módosítás, átdolgozás alatt álló 7/2006. (III. 21.) HM rendelet 16. mellékletében iránymutatásként a jövőben a katonák alkalmasság-vizsgálatának szerves részeként szerepel. Ez a kockázatfelmérés egyik nagyon fontos pillére az általuk elképzelt komplex UV védelemnek, segítségével kiemelhetjük, szorosan követhetjük a magas kockázatú egyéneket, szükség esetén időben szakellátásra irányíthatjuk őket.

Keywords: *health protection, UV radiation, examination of suitability, screening test, skin cancer, melanoma, risks, mission, prevention ~ egészségvédelem, UV sugárzás, alkalmasság vizsgálat, szűrővizsgálat, bőrrák, melanoma, kockázat, misszió, megelőzés*

INTRODUCTION

UV radiation is one of the most calculable harmful agents among the extreme external factors for our soldiers serving in missions (e.g. Afghanistan, Cyprus etc.) far from Hungary.[1] The harmful ultraviolet (UV) radiation is an almost constant risk factor with common occurrence and potential damaging effect.[2] Especially the occurrence of melanoma malignum is becoming more common and can cause death. (This tumour may spread rapidly, causing death within months of its recognition. [3]). It influences the serviceability of our soldiers both short- and long-term. The screening examinations of the high-risk individuals and to direct them to special medical care contribute significantly to the prevention of this risk impact.

MELANOMA

Solar radiation induces acute and chronic reactions in human skin. Epidemiological studies suggest that solar UV radiation is responsible for skin tumor development via gene mutations and immunsuppression, and possibly for photoaging. DNA damage caused by direct UV radiation and by indirect stress via reactive oxygen species (ROS) UV induces immunsuppression which may play a crucial role in skin cancer development [4] Ultraviolet B and A radiations (respective wavelength ranges 280-315 and 315-400 nm) are present in sunlight at ground level. The ultraviolet radiation does not penetrate any deeper than the skin and has been associated with various types of human skin cancers. [5] Three types of skin cancers comprise this group:basal cell carcinoma (BCC), squamous cell carcinoma (SCC), and cutaneous melanoma (CM). The first two are often collectively referred to as non-melanoma skin cancer (NMSC). BCC and SCC both result from the malignant transformation of keratinocytes, the major structural cell of the skin. CM, on the other hand, results from the malignant transformation of melanocytes, which are the skin's pigment producing cells. [6]

PREVENTION

The International Agency for the Research on Cancer (IARC) has grouped solar UV (UVB = 280-315 nm and UVA = 315-400 nm) as well as UV-radiation used in sunbeds in Group 1 ("carcinogenic to humans"). This has been reasoned by the overwhelming evidence coming from epidemiological data and invitro and in-vivo experiments which prove a causal connection between UV and skin cancer . Because the main risk factor for induction and development of skin cancer (-natural and artificial UV-) is known so well, and early forms of skin cancer (also malignant melanoma) can be treated very successfully, skin cancer can be prevented by means of primary and secondary prevention.

Primary prevention needs a long time and ongoing activities to achieve changes in behaviour of the soldiers which reduce risks of UV-induced skin cancer. Set against a background of dramatically increasing skin cancer incidences and being aware of the known difficulties in changing the behaviour of people, primary prevention, alone, might not be enough to fight the skin cancer problem. Therefore a combination with methods of secondary prevention seems appropriate. Secondary prevention deals with the early detection of malignancies which are curable in an early stage of their development. Because it is known that skin cancers (and especially MM, the deadliest skin cancer) can be cured with high efficiency in their early stages, skin cancers are also a target for secondary prevention, i.e., early detection and screening [7]

UV PROTECTION

The complex UV protection is divided into three parts

- education
- prevention - regulation, personal protection
- screening tests (pre- and post-test)

All the three pillars of the protection against UV radiation is substantial, particular emphasis will therefore be placed on finding solutions to the challenges in all three issues. In our previous article, [1] we have proposes an education and regulation system for the UV prevention. The detailed description of our developed new sunscreen products to be used as part of the personal protection will be the subject to later publications.

Furthermore, the risk assessment of melanoma being the third pillar of the UV protection will be described. This was considered feasible for Psychological Examination Institute to build it in its protocol, which was confirmed by the above mentioned regulation.

Melanoma risk assessment

During our research, we submitted a proposal arising from the summary of many relevant documents to the Institute of Psychological Suitability, aimed at reinforcing the usage of our risk assessment during the examination of suitability, as part of the medical examination.

Risk assessments have the great advantage that they are short and do not require expertise in oncology, and can significantly reduce the risks of melanoma malignum.

The assessment has three parts:

1. Filling the following table on the basis of information obtained by inspection and anamnesis:

Skin type	hair colour	skin colour	trends in sunburns	tanning
I	red	white, summer-freckled	+++	never
II	blond	white	++	mildly, temporary
III	light brown	white	+	brown
IV	brown	brown	seldom	brown
V	dark brown	dark brown	rare	deep brown
VI	black	black	never	black

On the basis of this, a patient in type I-II is identified as high risk for melanoma. [8]

2. The number of birthmarks needs to be determined: [9]
   - If someone has only a few birthmarks that are easily recognisable, it is not a risk factor.
   - If someone has many birthmarks, it must be determined if the number is above 50.

Number of birthmarks	
<50	>50

3. Family anamnesis:

A family history of melanoma	
No	Yes

On the basis of this risk assessment, for patients in type I-II and/or having more than 50 birthmarks and/or melanoma in family history, skin examination (dermatoscopy) is necessary.

When a soldier with melanoma risk applies to other missions, an opinion of a skin examination expert has to be submitted.

Place of risk assessment in the examination of suitability

When this study is written, the legislation on military suitability (Ministerial Decree 7/2006. (III. 21.) on considering the mental and physical health competence related to professional and contract military service and studies in military establishment, and on the rules for the authorization of sick leave, compensatory time off and reduced daily service) is under modification. Our submitted proposal is used as part of the medical examination in the draft of the law. The risk assessment is part of the examination of soldiers in the draft of Annex 16 to the Ministerial Decree 7/2006. (III. 21.).

SUMMARY

The complexity, simplicity and efficiency of the melanoma risk assessment we have developed, enabled it to be the part of the examination of suitability in the draft legislation. Thereby, we may reduce the risk of environmental impacts on soldiers. The classification of individuals to risk groups enables the selection, closer monitoring and specialised care of the high risk individuals in time. Time is very important in this case, as melanoma malignum is very invasive and progresses rapidly.

References

[1] Kolonics Gábor: The modern UV protection necessity in The Hungarian Defense Forces (A korszerű UV sugárvédelem szükségessége a Magyar Honvédségben)- Hadmérnök IV. évf. 3. szám 2009. szeptember

[2] Occupational diseases A Guide to Their Recognition June, 1977 DHHS (NIOSH) Publication No. 77-181,.

[3] The Merck Manual, Melania 2009

[4] M. Ichihashi, M. Ueda, A. Budiyanto, T. Bito, M. Oka, M. Fukunaga, K. Tsuru, T. Horikawa UV-induced skin damage Toxicology, Volume 189, Issues 1–2, 15 July 2003, Pages 21-39

[5] Frank R. de Gruijl Photocarcinogenesis: UVA vs UVB Methods in Enzymology, Volume 319, 2000, Pages 359-366

[6] J. Longstreth, F.R. de Gruijl, M.L. Kripke, S. Abseck, F. Arnold, H.I. Slaper, G. Velders, Y. Takizawa, J.C. van der Leun Health risks Journal of Photochemistry and Photobiology B: Biology, Volume 46, Issues 1–3, October 1998, Pages 20-39

[7] Rüdiger Greinerta,c,d,*, Mathieu Boniol Skin cancer - Primary and secondary prevention (information campaignsand screening) - With a focus on children & sunbeds Progress in Biophysics and Molecular Biology 107 (2011) 473-476

[8] Paolo Vecchia, Maila Hietanen, Bruce E. Stuck Emilie van Deventer, Shengli Niu: Protecting Workers from Ultraviolet Radiation ICNIRP 14/2007 ISBN 978-3-934994-07-2, Global Solar UV Index, WHO Prctical Guide ISBN 92 4 159007 6

[9] Somos Zsuzsanna: Basics of Modern Dermatology (A korszerű bőrgyógyászat alapjai,) Springer 1995

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Kolonics Gábor
kolonicsg@yahoo.com

THE EXAMINATION OF UV ABSORPTION OF POLYPHENOLS (NATURAL SUBSTANCES IN UV PROTECTION)

Abstract

Thereinafter, as a continuation of the earlier published article about fulvic acids (The examination of the role of natural substances in the protection against UV radiation - Hadmérnök VIII. Évfolyam 1. szám - 2013. március) the author introduced a subsequent natural substance, the solution red grape skin extract ie. polyphenol extract. 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 his series of experiments, the author was looking for substances complying with these principles. [1] As earlier fulvic acids and last polyphenols were taken into account, and the author 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.

A következőkben a szerző egy korábban megjelent, a fulvósavakkal foglalkozó cikk (The examination of the role of natural substances in the protection against UV radiation - Hadmérnök VIII. Évfolyam 1. szám - 2013. március) folytatásaként újabb természetes anyagot - a vörös szőlő héj kivonatát, azaz polifenol kivonatot - mutat be. A katonai egészségvédelemben a szerző által 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 sorozatban ezen elveknek megfelelő anyagokat keresett a szerző, így első lépésként a fulvósavak kerültek látóterébe és azt vizsgálta, hogy ezek az anyagok UV abszorbciója alapján alkalmas lehet-e az általa elképzelt napvédő krém komponenseként alkalmazni.

Keywords: *fulvic-acid, polyphnol, UV absorption ~ fulvósav, polifenol, UV abszorpció*

INTRODUCTION

In the following, the author will present that for personal UV protection, as being part of the complex UV protection planned in the Hungarian Army, the author plans 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 hours 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. [3]

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 following parts

- primer prevention e.g.: education regulation, personal protection
- secunder prevention 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 author has 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 author 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. [1] [4] and continues work with polyphenols recovered from grapes.

HARMFUL UV SPECTRUM

7% of the sunlight is in the ultraviolet range (Nicholson et al., 2005) [5], 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. [6]

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.

1. Figure Biological effects of UV radiation[7]

Thus, the sunscreen substances sought must absorb in UVA and UVB range.

HISTORY OF SUNSCREEN

In 1938, a Swiss chemistry student named Franz Greiter suffers sunburn while climbing Mount Piz Buin on the Swiss-Austrian border and sets out to invent an effective sunscreen. In 1944 Benjamin Green, an airman and pharmacist, uses a greasy substance called "red vet pet" (red veterinary petrolatum) to protect himself and other soldiers from ultraviolet rays during World War II. Heavy and unpleasant, it works primarily as a physical barrier between the skin and the sun. After the war, Mr. Green mixes red vet pet, cocoa butter and coconut oil into a product that would eventually become Coppertone suntan cream. In 1946 Mr. Greiter's product, called Gletscher Crème (Glacier Cream), comes to market under the brand Piz Buin, which is still sold today. The familiar Coppertone Girl was drawn by an illustrator named Joyce Ballantyne. She used her 3-year-old daughter, Cheri, as the modelin 1956. In 1970's Piz Buin introduces sunscreens with ultraviolet A and ultraviolet B filters. In 1978 The Food and Drug Administration proposes to regulate sunscreens, recommending standards for safety and effectiveness. These guidelines — some parts of which never took full effect — mostly dealt with establishing SPF testing and labeling. However, the official document did state, "In the long run, suntanning is not good for the skin." In 1988 The F.D.A. approves a sunscreen product containing avobenzone, a UVA-only filter. The other approved filters until then were UVB ones that had incidental UVA protection. In 1997 The F.D.A. allows sunscreen makers to market the fact that their products contain avobenzone for UVA protection. In 2006 The F.D.A. misses a deadline set by Congress to approve proposed guidelines for sunscreens. In 2007 The F.D.A. finalizes its proposed rules on UVA testing and labeling and starts accepting comments on the proposals. In 2010 The F.D.A. is expected to approve the 2007 guidelines, but the target date is pushed back yet again, most recently to October from May [8]

The author has 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 author examined if, on the basis of the UV absorption of these substances, it may be used as the component of the sun protection cream.

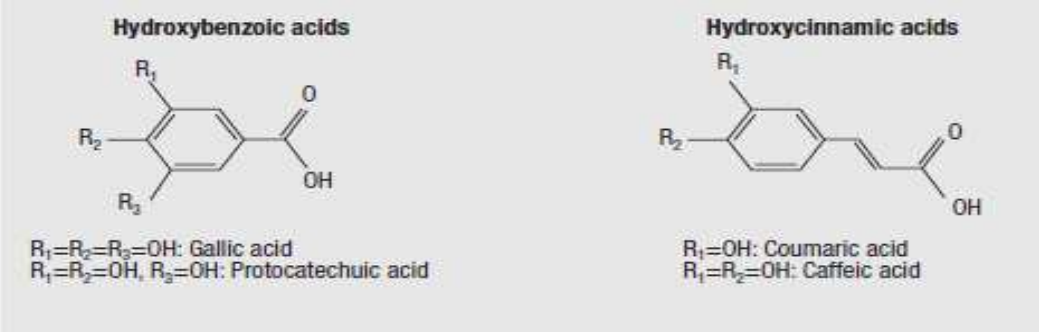
POLYPHENOLS

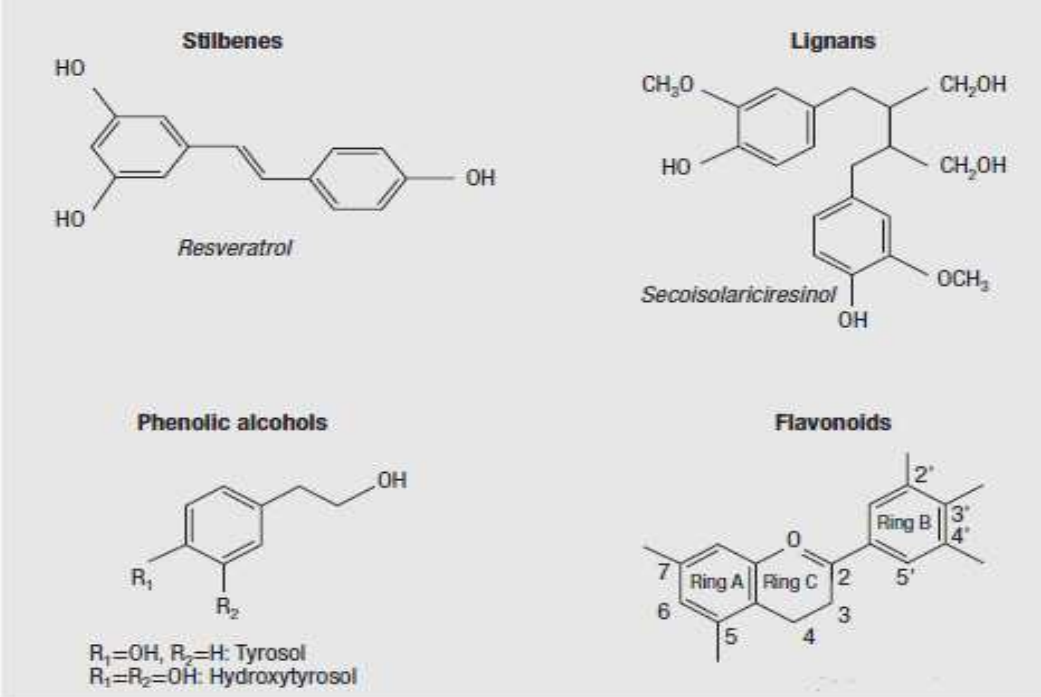
Fruit (grape) and beverages such as tea and red wine represent the main sources of polyphenols. Despite their wide distribution, the healthy effects of dietary polyphenols have come to the attention of nutritionists only in the last years. The main factor responsible for the delayed research on polyphenols is the variety and the complexity of their chemical structure. Emerging findings suggest a large number of potential mechanisms of action of polyphenols in preventing disease, which may be independent of their conventional antioxidant activities. [9] Grapes contain a large amount of polyphenols. Grapes are cultivated largely for the wine

industry, which generates huge amounts of grape pomace as an industrial waste. Some research work has been carried out to seek industrial uses for this waste, including use as animal feed, as nutritive ingredients, in the production of citric acid and the use of anthocyanins from grape skins as colorants. [10] These were why the authors found the red grape skin is a proper source of polyphenols.

Polyphenols comprise a wide variety of moleculesthat have a polyphenol structure (*i.e.* several hydroxylgroups on aromatic rings), but also moleculeswith one phenol ring, such as phenolic acids andphenolic alcohols. Polyphenols are divided into severalclasses according to the number of phenol ringsthat they contain and to the structural elements that bind these rings to one another. The main groups of polyphenols are: flavonoids, phenolic acids, phenolic alcohols, stilbenes and lignans [9]

Research in recent years strongly supports a role for polyphenols in the prevention of degenerative diseases, particularly cancers, cardiovascular diseases and neurodegenerative diseases . Polyphenols are strong antioxidants that complement and add to the functions of antioxidant vitamins and enzymes as a defense against oxidative stress caused by excess reactive oxygen species (ROS). Although most of the evidence of the antioxidant activity of polyphenols is based on *in vitro* studies, increasing evidence indicates they may act in ways beyond the antioxidant functions *in vivo*. In the meantime, chemically, polyphenols are a group of natural compounds with phenolic structural features. It is a collective term for several sub-groups of phenolic compounds, however, use of the term ―polyphenols‖ has been somewhat confusing and its implied chemical structures are often vague even to researchers. Studies have also shown that different polyphenol subgroups may differ significantly in stability, bioavailability and physiological functions related to human health. More than 8000 phenolic structures are currently known, and among them over 4000 flavonoids have been identified. Although polyphenols are chemically characterized as compounds with phenolic structural features, this group of natural products is highly diverse and contains several sub-groups of phenolic compounds. Fruits, vegetables, whole grains and other types of foods and beverages such as tea, chocolate and wine are rich sources of polyphenols. The diversity and wide distribution of polyphenols in plants have led to different ways of categorizing these naturally occurring compounds. Polyphenols have been classified by their source of origin, biological function, and chemical structure. Also, the majority of polyphenols in plants exist as glycosides with different sugar units and acylated sugars at different positions of the polyphenol skeletons. [11]

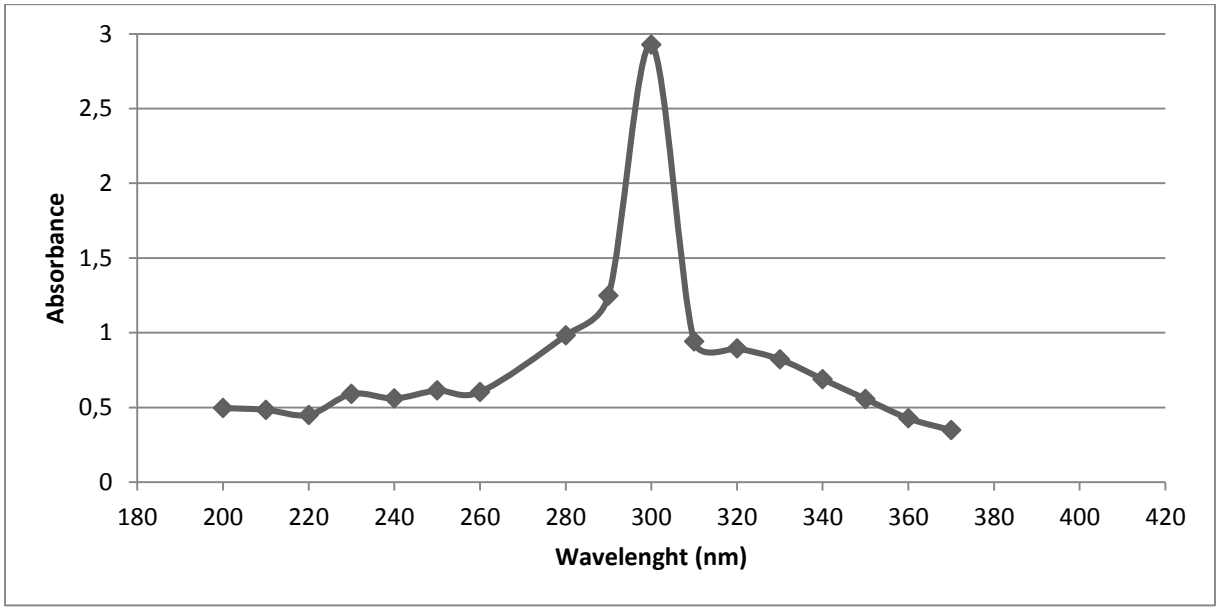




2. Figure. Chemical structures of polyphenols.[9]

UV ABSORPTION OF POLYPHENOLS (RED GRAPE SKIN EXTRACT)

In order to use polyphenols as sunscreen substances, need to examine if it absorbs in the adequate ultraviolet spectrum. During the study, the author found that the solution red grape skin extract absorbs in both UVA and UVB spectrum. This is illustrated in the following graph:



3. Figure Rate of absorbance of polyphenols
(source: author)

SUMMARY:

In this article, polyphenols were 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 author made the similar analysis of fulvic acid and they are planning to examine the UV protective effect of the different composition of these substances.

References

[1] Kolonics, Kóródi: The examination of the role of natural substances in the protection against UV radiation - Hadmérnök VIII. Évfolyam 1. szám - 2013. március

[2] Kóródi GyulaA térinformatika új lehetőségei a háborús sérült-ellátásban KARD ÉS TOLL 2002:(1) pp. 139-141. (2002)

[3] Kolonics: A korszerű UV sugárvédelem szükségessége a Magyar Honvédségben- Hadmérnök IV. évf. 3. szám (2009. szeptember)

[4] Kóródi Gyula Huminsav előállítása, a tőzeg feltárása ZMNE Vegyi- és Katasztrófavédelmi Intézet, Egyetemi Közlemény (2010)

[5] 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.

[6] 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

[7] Dobozy Attila dr. -Tabularium dermatologiae 2002 Melania Kiadói Kft.

[8] http://www.nytimes.com/2010/06/24/fashion/24skinside.html?_r=0 2013.07.15

[9] D'Archivio, Filesi, Di Benedetto, Gargiulo, Giovannini, Masella : Polyphenols, dietary sources and bioavailability Ann Ist Super Sanità 2007 | Vol. 43, No. 4: 348-361

[10] Yinrong Lu, L. Yeap Foo: The polyphenol constituents of grape pomace - Food Chemistry 65 (1999) 1±8 ISSN: 0308-8146

[11] Rong Tsao: Chemistry and Biochemistry of Dietary Polyphenols - *Nutrients* 2010, *2*, 1231-1246 ISSN 2072-6643

HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Tuba Zoltán – Bottyán Zsolt – Wantuch Ferenc – Vidnyánszky Zoltán – Hadobács Katalin
tubazoltan.met@gmail.com – bottyan.zsolt@uni-nke.hu – wantuch.f@gmail.com – vidnyanszkyz@gmail.com – katalin.hadobacs@gmail.com

JAVASLAT KATONAI MŰVELETEK TERVEZÉSÉNEK METEOROLÓGIAI TÁMOGATÁSI MODELLJÉRE

Absztrakt

Jelen cikkünk célja egy olyan meteorológiai támogatási modell bemutatása, amely a katonai műveletek tervezésének hadműveleti és stratégiai szintjén nyújthat hatékony meteorológiai, klimatológiai támogatást a döntéshozók számára. A javasolt modell az Analytic Hierarchy Process (AHP) és a fuzzy logika eszközrendszerének felhasználásával segít a felhasználóknak kiválasztani a műveletek végrehajtásához optimális időszakot. A bemeneti paraméterek alapján a kívánt végrehajtási helyre vonatkozó, származtatott klimatikus adatokat tartalmazó adatbázis felhasználásával a modell meghatározza az év megfelelő időszakát. A klíma adatbázis a modelltől függetlenül kezelhető, így annak cseréjével a modell tetszőleges műveleti területre alkalmazható, amennyiben az alap klíma adatok rendelkezésre állnak. Cikkünkben egy rövid esettanulmányt is bemutatunk, amely jól szemlélteti a támogató modell képességeit.

This article aims to present a meteorological support model, which is able to provide effective meteorological, climatological support to decision makers in military mission planning on the operational and strategic level. The recommended model uses the tools of Analytic Hierarchy Process (AHP) and fuzzy logic to help users choosing the optimal period of year for mission execution. Based on the input parameters the model marks the appropriate time of the year out for the desired place of execution by using a database with derived climatic parameters. This climatic database is independent from the model. So the model can be applied for any operational area if the necessary climatic data are available. We present a case study in this article to demonstrate the detailed capabilities of the model.

Kulcsszavak: *meteorológiai támogatás, műveleti tervezés, fuzzy logika, AHP ~ meteorological support, mission planning, fuzzy logic, AHP*

BEVEZETÉS

A katonai műveletek, gyakorlatok végrehajtása során a meteorológiai támogatásnak gyakran fontos szerep jut. Kiemelten igaz ez a repülések meteorológiai biztosításában, ahol a felhasználók jelentősen érzékenyebbek az időjárási paraméterek egyes értékeire illetve azok megváltozására. Kijelenthetjük, hogy az egyes feladatok végrehajtási fázisában a meteorológiai támogatás felhasználói oldalról is a folyamat szerves részét képezi. Az időjárási adatok felhasználása azonban jellemzően az operatív előrejelzői produktumokra, mérési, megfigyelési valamint távérzékelési adatokra (műhold, radar, stb.) korlátozódik, statisztikai megközelítéseket nem alkalmaz [1]. A tervezési fázisban a meteorológiai támogatás kizárólag az olyan operatív vagy eseti előrejelzési produktumokkal van jelen, amelyek a műveletek végrehajtás előtti közvetlen előkészítését segítik. A stratégiai vagy hadműveleti tervezés eszközrendszeréből teljes mértékben hiányzik a származtatott klimatológiai adatokra támaszkodó döntéstámogató biztosítás, amely a tervezett feladatok eredményesebb végrehajthatóságát jelezheti előre.

Jelen cikk egy olyan tesztüzemben már működőképes modellt mutat be, amelynek segítségével a katonai műveletek hosszabb távú tervezési fázisában is hatékony meteorológiai támogatás nyújtható a döntéshozó számára. A felhasználói igények pontos megfogalmazása valamint a kiválasztott változókkal szemben támasztott preferenciák meghatározása esetén a modell képes az AHP (Analytic Hierarchy Process) módszer és a fuzzy logika eszközrendszerének segítségével a kitűzött feltételeknek megfelelő optimális időszak kijelölésére, ha a létrehozott adatbázisban a feladat szempontjából releváns információk rendelkezésre állnak. Az alkalmazott módszerek alkalmazásának részletei az alábbiakban egy esettanulmánnyal szemléltetve kerülnek bemutatásra.

A MODELL

A modern repülésmeteorológiai támogatásban a statisztikai alapú megközelítések egyre szélesebb körben kerülnek alkalmazásra. A hagyományos dinamikus megközelítésekkel ellentétben, amelyek az egyes időjárási jelenségek fizikai alapú leírására épülnek, ezek az eljárások egy adekvát klimatológiai adatbázis adatainak feldolgozásával közelítik az időjárás várható alakulását. A módszer lényege, hogy az aktuális időjárási helyzethez meghatározott logika alapján, az arra alkalmas adatbázisban hasonló helyzeteket keresnek, majd ezek feldolgozásával állítanak elő egy többnyire ultrarövid távra szóló előrejelzést. A nemzetközi tapasztalatok azt mutatják, hogy ezek az előrejelzések megfelelő pontosságúak a repülésmeteorológiai biztosítás számára is [2]. Az említett módszerek hazai adaptálása megkezdődött [3] és ez adta az ötletet a bemutatásra kerülő modell kialakításához is.

A modell kitűzött célja, hogy a műveletek tervezése során olyan származtatott klimatológiai adatokon alapuló támogatást nyújtson, amelynek segítségével az adott művelet végrehajtási időszaka pontosan kijelölhető. A módszer kiinduló pontját a felhasználói igények pontos megfogalmazása jelenti. Ennek keretében a felhasználóknak meg kell határozniuk, hogy melyek azok a műveletek, amelyekre az alkalmazott eszközökön vagy akár az élőerőn keresztül az időjárás meghatározó hatást gyakorolhat. Ezután ki kell választaniuk azokat a meteorológiai paramétereket, amelyek a feladatok végrehajtását befolyásoló tényezőket megfelelően jellemzik, azaz rajtuk keresztül meghatározható a műveletek végrehajtásának hatékonysága. Minden egyes kiválasztott paraméter esetében meg kell határozni a működést részben befolyásoló vagy teljes mértékben korlátozó határértékeket, esetleg a felhasználó által megszabott művelet végrehajtási határokat. Ezek alapján a változók értelmezési tartománya három részre osztható:

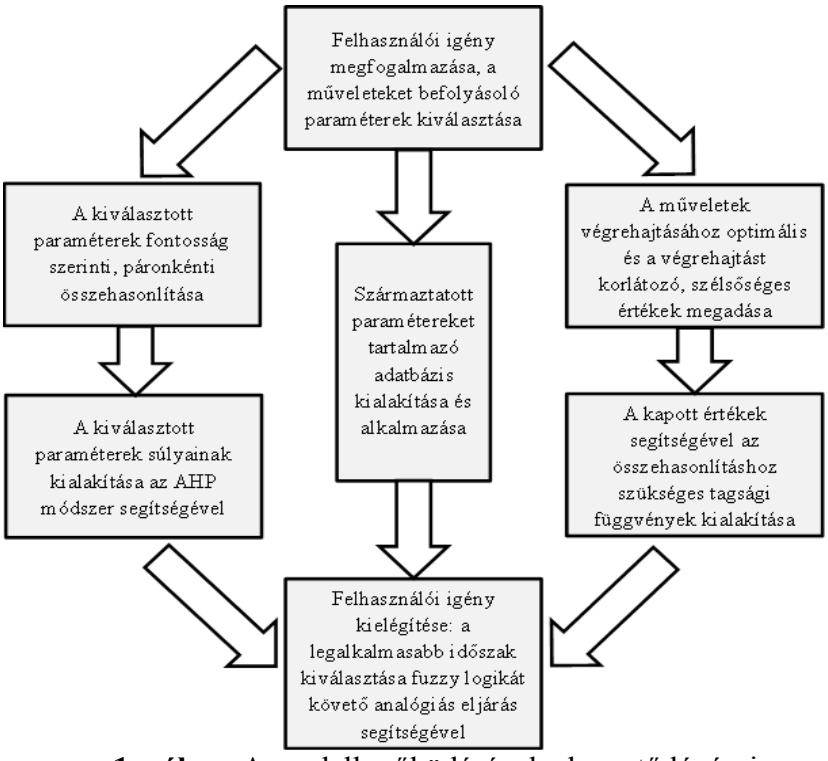
- alkalmas: az alkalmazott eszköz vagy élőerő korlátozás nélkül, hatékonyan vethető be, az időjárási kockázat nem számottevő;
- elfogadható: az alkalmazott eszköz vagy élőerő csak korlátozásokkal és/vagy kisegítő eszközökkel és/vagy csökkenő hatékonysággal vethető be, az időjárási kockázat növekszik;
- alkalmatlan: az alkalmazott eszköz vagy élőerő korlátozásokkal és/vagy kisegítő eszközökkel sem vethető be, az időjárási kockázat nagy.

A megszabott határértékek segítségével kialakíthatók az ún. tagsági függvények, amelyek a fuzzy logikán alapuló analógia kereső eljárás alapját képezik. Ezeknek a segítségével kerül meghatározásra az egyes naptári napok jellemzőinek és a felhasználó által felállított határértékeknek a hasonlósága. A gyakorlati alkalmazásban ez azt jelenti, hogy a felhasználó által kijelölt optimális körülményekhez tartozó paraméter értékek és a vizsgált naptári nap jellemzői milyen mértékben hasonlítanak vagy fordítva megfogalmazva: azoktól milyen mértékben térnek el. Ez a módszer a későbbiekben kerül részletesebb bemutatásra.

A felhasználónak lehetősége van az általa meghatározott szempontok fontosság szerinti páronkénti összehasonlítására, amely alapján a későbbiekben részletesebben bemutatásra kerülő AHP módszer eszközrendszerével meghatározhatók az egyes paraméterek súlyai. A gyakorlatban ez azt jelenti, hogy a kevésbé fontos, azaz kisebb súllyal rendelkező paraméterek esetében a modell megengedőbb lesz az elfogadható kategóriát képviselő értékekkel.

A származtatott paramétereket tartalmazó adatbázist is a felhasználói igényekhez kell igazítani és akár ad hoc jelleggel új változókkal kell kiegészíteni, amelyek a speciális, feladatra szabott elvárásoknak is megfelelnek.

A modell alapvető lépéseinek áttekintését az 1. ábra foglalja össze.



1. ábra. A modell működésének alapvető lépései

Az alábbiakban a modell működéséhez alkalmazott eljárások, módszerek részletes bemutatása következik.

FUZZY LOGIKÁN ALAPULÓ ANALÓGIA KERESŐ ELJÁRÁS ALKALMAZÁSA

A fuzzy halmazelmélet első elméleti leírását Zadeh adta a hatvanas években [4]. Azóta elméletét rengeteg tudományterületen, például a meteorológiában is [5], de elsősorban irányítási, automatizálási problémák megoldására alkalmazták. Lehetőséget ad ugyanis olyan nem egzakt, többnyire empirikus úton szerzett ismeret matematikai alkalmazására, amelyet korábban tudományos módon nem vagy csak kompromisszumokkal tudtak modellekbe illeszteni. A fuzzy logika alkalmazása során akár olyan kifejezések is pontos matematikai jelentéssel láthatók el, mint például a „többnyire hasonló", „kevésbé hasonló", stb. Ezt a lehetőséget használtuk fel jelen cikkünkben mi is. A kialakított adatbázisunkban a felhasználó által meghatározott optimális körülményekhez keresünk hasonló szituációkat. Ehhez a hasonlóság kereséshez pedig a felhasználó tapasztalatai alapján megadott vagy előírásokban megkövetelt határértékek segítségével meghatározott tagsági függvények szükségesek. Ezek a tagsági függvények adják meg a gyakorlati tapasztalatok matematikai leírását. A tagsági függvények értelmezési tartománya bármi lehet, az értékkészletük viszont 0 és 1 közé esik. A modellben felhasznált tagsági függvény általános alakja azokban az esetekben, amikor a vizsgált paraméter optimális értékétől vett eltérés a vizsgálat tárgya:

$$f(x) = \begin{cases} 1, & ha \quad |x| < k_1 \\ \dfrac{k_2 - |x|}{k_2 - k_1}, & ha \quad k_1 \le |x| \le k_2 \\ 0, & ha \quad |x| > k_2 \end{cases}$$

ahol k_1 és k_2 ($> k_1$) a felhasználó által megadott optimális értéktől való eltérés határértékeit jelenti. A tagsági függvény általános alakja azokban az esetekben, amikor a vizsgált paraméter származtatott relatív gyakorisági értékei képezik a vizsgálat tárgyát:

$$f(x) = \begin{cases} 1, & ha \quad x < h_1 \\ \dfrac{x - h_1}{h_2 - h_1}, & ha \quad h_1 \le x \le h_2 \\ 0, & ha \quad x > h_2 \end{cases}$$

ahol h_1 és h_2 ($> h_1$) a felhasználó által megadott alkalmassági kategóriák határértékeit jelentik. A megadott határértékek a felhasználói oldalról azokat az értékeket jelölik, amelyeket a felhasználó a „teljes mértékben alkalmas" és „teljes mértékben alkalmatlan" ún. fuzzy szavakkal limitként jellemez. A bemutatott tagsági függvények segítségével ezután paraméterenként meghatározható a hasonlóság mértéke egy 0 és 1 közé eső számmal. Esetünkben tehát a 0 érték jelentése minden egyes paraméterre az, hogy a paraméter értékei az alkalmatlan kategóriába sorolhatók. Az 1 érték pedig ennek ellenkezőjét jelenti: a paraméter értékei az alkalmas kategóriába tartoznak. A két érték között pedig egy lineáris függvény adja meg az alkalmas/alkalmatlan kategóriától való távolságot. Amennyiben több paraméter együttes vizsgálatáról van szó, akkor az egyedi hasonlósági értékek minimuma adja az összesített hasonlóság értékét. Ez biztosítja azt, hogy bármely paraméter alkalmatlansága esetén az eredmény alkalmatlan lesz illetve csak abban az esetben lesz a végeredmény alkalmas, ha mindegyik paraméter értéke az alkalmas kategóriába esik.

Amennyiben a felhasználó a vizsgált paramétereket fontosságuk szerint súlyozza, akkor az egyes paraméterek hasonlósági értékeihez hozzáadjuk a később bemutatásra kerülő módon meghatározott súlyok 1-ből kivont értékét. Ezzel tulajdonképpen a nagyobb súllyal rendelkező változók hasonlósági értékét csökkentjük virtuálisan, azaz a minimumfüggvény alkalmazása nagyobb eséllyel érinti a fontosabb paramétereket. Könnyen belátható, hogy a hasonlósági értékek minimumának meghatározása után a hasonlóság maximális értéke a maximális súly 1-ből kivont értékével haladja meg az 1-et. Annak érdekében, hogy a paraméterek alkalmatlan kategóriába eső értékei a hasonlóság során 0 értékként jelenjenek meg az előbbiek során kapott új hasonlósági értéket egységesen csökkentettük a minimális súly 1-ből kivont értékével. Ezután a negatív értékeket 0-nak vettük. Ahhoz, hogy a hasonlósági érték a későbbiekben összevethető legyen a súlyok alkalmazása nélküli eljárás eredményeivel, a kapott értékeket lehetséges maximumuk szerint normáltuk. A könnyebb áttekinthetőség kedvéért a későbbiekben a hasonlósági értékek százalékos formában kerülnek feltüntetésre.

AZ AHP MÓDSZER ALKALMAZÁSA

Az Analytic Hierarchy Process (AHP) módszerének első leírását Thomas L. Saaty adta 1977-ben [6]. Az eljárás a többszempontú döntési problémák egy lehetséges megoldását adja, melyet hazai szerzők is részletesen kifejtenek [7][8]. A többszempontú döntési probléma lényege, hogy valamely cél elérése érdekében adott alternatívák közül kell választanunk, véges számú szempont figyelembe vételével. A módszer minden olyan esetben jól alkalmazható, amelyben egyértelműen meghatározható a döntés célja és beazonosíthatók a választható alternatívák illetve a kiválasztás során felhasznált szempontok. Nyilvánvalóan ez sok döntési probléma esetében a katonai szakterületen is applikálhatóvá teszi a módszert. Ahogyan például Gyarmati [9] és Gyarmati és társai [10] is megmutatták, az AHP metodikája hatékonyan alkalmazható haditechnikai eszközök összehasonlító elemzése, kiválasztása során. Munkáikban rámutatnak, hogy a haditechnikai terület többszempontú döntési problémáira milyen korlátokkal és konkrétan hogyan alkalmazható a szóban forgó eljárás.

Esetünkben a többszempontú döntési probléma meghatározása során a kitűzött célt a műveletek végrehajtásához megfelelő időszak kiválasztása jelenti. A kiválasztandó alternatívákat az időszak jellemzésére alkalmas legkisebb egységek, azaz a naptári napok adják. A kiválasztás során figyelembe vett szempontokat pedig a felhasználó által megadott, az adatbázis részét képező származtatott jellemzők képezik. Az alternatívák nagy száma miatt, az AHP módszerből csak a szempontok páronkénti összehasonlításával nyert szempont súlyokat használjuk fel, amelyeket a szempontok páronkénti összehasonlításával nyert mátrix sajátvektor problémájának megoldásaként nyerünk. Ennek meghatározását a következőkben ismertetjük.

Jelentse n azoknak a kiválasztott szempontoknak (esetünkben a származtatott klimatikus jellemzők) a számát, amelyek esetében szeretnénk meghatározni a w_i súlyokat ahol $i = 1, \dots, n$ és a w_i az i-edik szempont fontosságát mutatja. Kiindulásként a felhasználó értékelése alapján minden egyes i, j szempontpárra meghatározott, az i-edik és j-edik szempont fontosságának arányát mutató becslések állnak rendelkezésre. Jelöljük ezeket a_{ij}-vel ahol $i, j = 1, \dots, n$. Természetesen $a_{ij} = \frac{1}{a_{ji}}$.

Meg kell jegyeznünk, hogy például az $a_{ij}a_{jk} = a_{ik}$ egyenlőség nem feltétlenül igaz. Példának okáért tegyük fel, hogy az első szempont kétszer fontosabb, mint a második, és a második szempont kétszer fontosabb, mint a harmadik. Ennek ellenére az első szempont csak háromszor fontosabb, mint a harmadik. Ilyen helyzetekben nem is elvárható, hogy a súlyok

tökéletesen visszaadják az eredetileg megadott fontossági arányokat. A cél az, hogy olyan w_i súlyokat találjunk, amelyek minimalizálják az a_{ij} és $\frac{w_i}{w_j}$ arányok különbségét.

Jelölje A a fontossági arányok $n \times n$ mátrixát. Ha ez a pozitív reciprok mátrix konzisztens, azaz az $a_{ij}a_{jk} = a_{ik}$ egyenlőség teljesül, akkor a keresett $w = (w_1, \ldots, w_n)$ súlyvektor az A mátrix az n sajátértékhez tartozó sajátvektora. Más szavakkal: $Aw = nw$ és ebben az esetben n a maximális sajátérték. Saaty bebizonyította, hogy egy A pozitív reciprok mátrix akkor és csak akkor, konzisztens, ha $\lambda_{max} = n$ ahol λ_{max} a mátrix maximális sajátértékét jelöli. Továbbá azt is bizonyította, hogy a páronkénti összehasonlítás mátrix inkonzisztenciája esetén a λ_{max} maximális sajátértékhez tartozó sajátvektor adja a súlyvektor legjobb becslését, mivel ez minimalizálja az a_{ij} és $\frac{w_i}{w_j}$ arányok különbségét [6].

A fentieket felhasználva az alábbi eljárást követtük:

- a felhasználó által meghatározott a_{ij} ahol $i, j = 1, \ldots, n$ fontossági arányokból létrehoztuk az A mátrixot;
- iterációs módszerrel meghatároztuk a λ_{max} maximális sajátértékhez tartozó w_{max} sajátvektort;
- w_{max} normálásával megkaptuk a keresett $w = (w_1, \ldots, w_n)$ súlyvektort, ahol w_i az i-edik szempont súlyát adta meg.

A való életben a felhasználó szubjektív ítéletén alapuló fontossági arányok a legtöbb esetben inkonzisztenciára vezetnek. Amennyiben ennek mértéke az elfogadott mértéket meghaladná, akkor a felhasználó a páros összehasonlítás korrekciójára kérhető.

Az egyes szempontokhoz kapott súlyokat a korábban ismertetett módon alkalmaztuk modellünkben.

AZ ADATBÁZIS

Az adatbázis létrehozásához egy repülésmeteorológiai jelentő táviratokra (METAR) épülő, korábban létrehozott adatbázist használtunk fel. Az anyaadatbázist a jelentő táviratokból kinyert nyers adatok és származtatott paraméterek kombinációja alkotja [11]. Mivel az abban fellelhető adatok elemi bontásban is megjelennek, ezért az új adatbázis származtatott jellemzőinek előállítása összetettebb előkészítést nem tett szükségessé. Az új paraméterek előállításánál az volt a célunk, hogy egy adott naptári napot minél jobban jellemző, egyszerűen értelmezhető és a katonai műveletekre esetlegesen hatást gyakorló változókat hozzunk létre. Az előállított tizenegy paraméter képezi az adatbázis kiindulási állapotát, amely tetszőlegesen bővíthető a felhasználói igények szerint, amennyiben az anyaadatbázisban a kiszámításhoz szükséges paraméterek rendelkezésre állnak. Az adatbázis hőmérséklettel kapcsolatos elemei esetében az adott naptári napra vonatkozóan számítottuk ki a kívánt mennyiségeket, majd az így kapott adatsort tizenöt napos mozgóátlaggal simítottuk. A jelenlegi adatbázis viszonylagos rövidsége miatt ugyanis így egy adott időszak jellemzői a hasonlóság keresés során lényegesen kisebb fluktuációt mutatnak, ami a felhasználó számára az eredményeket könnyebben értékelhetővé teszi. A relatív gyakorisági elemek esetében először adott év naptári napjaira számítottuk ki az adott feltételnek megfelelő észlelések relatív gyakoriságát, majd ezek naptári nap szerinti átlagát képeztük. A hőmérsékleti elemekhez hasonlóan a simítást itt is elvégeztük. Annak érdekében, hogy a relatív gyakoriság fogalma a felhasználó számára is könnyebben értelmezhető legyen, klimatológiai előtanulmányok és az adott hely éghajlati jellemzőinek ismerete nélkül, az így kapott értékeket a naptári nap szerinti maximális érték szerint normáltuk. Így a végső jellemző nem egy olyan számot rejt, aminek az értelmezéséhez ismernünk kell annak viszonyítási rendszerét, hanem azt mutatja meg, hogy az év egy adott feltétel előfordulása szempontjából

maximális relatív gyakoriságú napjához mérten egy másik nap hány százalékban teljesíti ugyanazt a feltételt. Az egyszerűség kedvéért a továbbiakban ezeket a paramétereket adott kategória relatív gyakoriságainak nevezzük. A látástávolság és a felhőalap vonatkozásában a relatív gyakoriságok tetszőleges határértékekre kiszámíthatók a felhasználói igényeknek megfelelően.

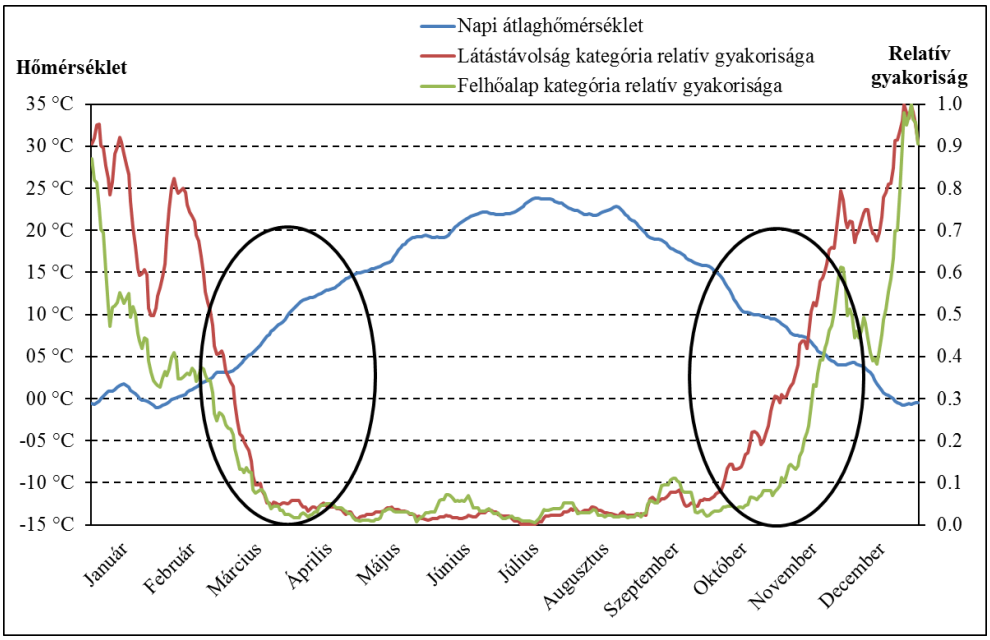
A rendelkezésre álló tizenegy kiszámított paraméter a következő:

1. Naptári nap átlaghőmérséklete
2. Naptári nap átlagos minimumhőmérséklete
3. Naptári nap abszolút minimumhőmérséklete
4. Naptári nap átlagos maximumhőmérséklete
5. Naptári nap abszolút maximumhőmérséklete
6. Adott kategóriának megfelelő látástávolság relatív gyakorisága
7. Adott kategóriának megfelelő felhőalap relatív gyakorisága
8. Zivatar előfordulásának relatív gyakorisága
9. Köd előfordulásának relatív gyakorisága
10. Havazás előfordulásának relatív gyakorisága
11. Ónos csapadék vagy zúzmarás köd előfordulásának relatív gyakorisága

Az adatbázis a modelltől teljesen függetlenítve van, a modell bemeneti paramétereinek kiolvasása történik innen. Nyilvánvaló, hogy az adatbázis cseréjével az adott földrajzi helyre vonatkozó klimatikus viszonyok figyelembe vétele egyszerűen megvalósítható. Ennek segítségével a szükséges adatok birtokában akár missziós műveleti területre vonatkozóan is tervezhető a haditechnikai eszközök és az élőerő alkalmazhatósága. Ez az alkalmazási lehetőség azért lehet kiemelten fontos, mert a döntéshozók ismeretei a vonatkozó területek éghajlati környezetéről esetenként fokozottan korlátozottak.

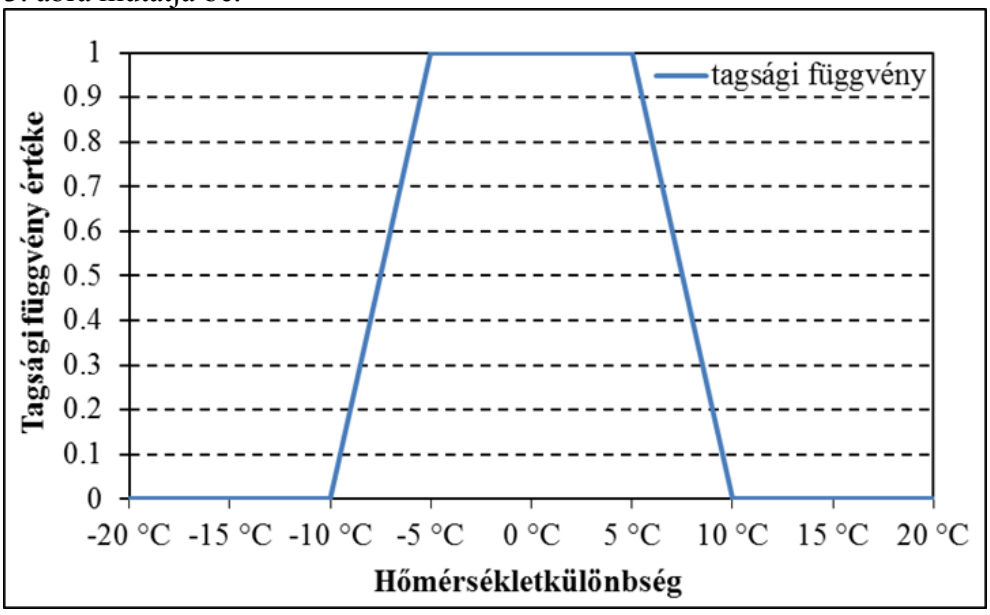
ESETTANULMÁNY

Az esettanulmány kiválasztása irányítottan történt. Ehhez az adatbázisban található, a szolnoki repülőtérre vonatkozó származtatott mennyiségek éves menetét mutató grafikonok kerültek felhasználásra. Az esettanulmány során felhasznált paraméterek esetében ezt a 2. ábra szemlélteti. A kiválasztás alapját az éves menetekben tapasztalható leggyorsabb változások adták, amelyeket a 2. ábrán látható fekete ellipszisek mutatnak. A vizsgált paraméterek kijelölt értékeit ez alapján határoztuk meg. A megadott határértékek fiktívek, nem kötődnek konkrét katonai művelet korlátozó tényezőihez, ugyanakkor a valóságtól nem elrugaszkodottak. Az alkalmazott értékek esetében arra törekedtünk, hogy a modell képességei minél jobban bemutathatóak legyenek.



2. ábra. Az esettanulmány során felhasznált paraméterek éves menete

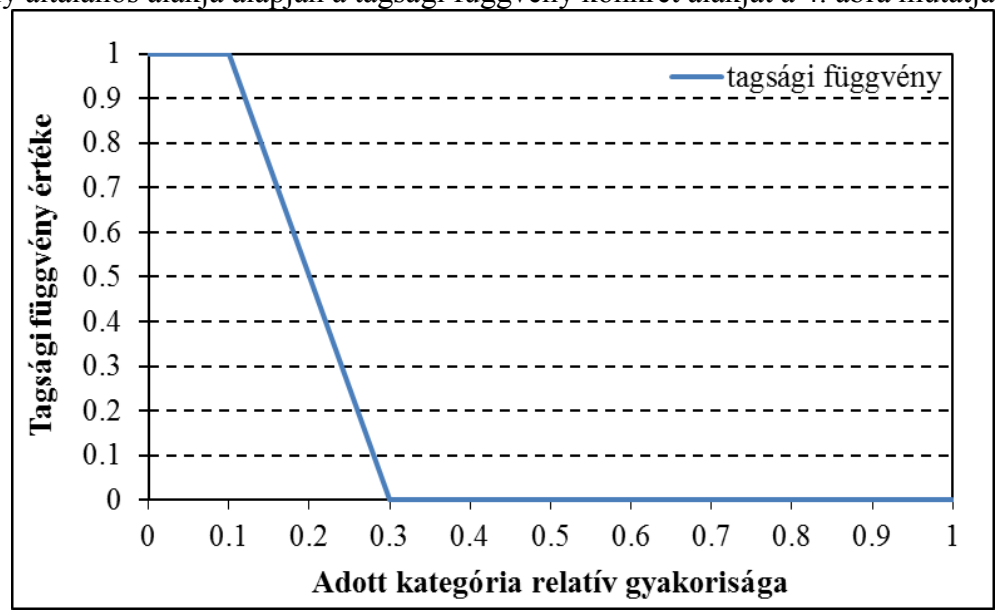
A tervezett műveletek végrehajtását tehát az adatbázisban található három származtatott paraméter befolyásolhatja. A napi átlaghőmérséklet esetében az optimális értéket az 5°C-os hőmérséklet jelenti. Az ettől ±5°C-kal eltérő értéktartomány a műveletek végrehajtására az alkalmazott eszköz vagy élőerő korlátozása nélkül alkalmas. Amennyiben az eltérés 10°C-nál nagyobb, akkor a művelet végrehajtására a körülmények alkalmatlanok. A két érték közötti tartományban a művelet korlátozottan és/vagy csak kisebb hatékonysággal és/vagy kisegítő eszközök alkalmazásával hajtható végre. Az ismertetett értékekkel és a korábbiakban bemutatott vonatkozó tagsági függvény általános alakja alapján a tagsági függvény konkrét alakját a 3. ábra mutatja be.



3. ábra. A tagsági függvény alakja a napi átlaghőmérséklet esetében

A 3000 m-es és az alatti látástávolság valamint a 300 m-es és az alatti felhőalap maximum szerint normált relatív gyakoriságának esetében az optimális értéket az 10% alatti értékek jelentik. Ez az értéktartomány a műveletek végrehajtására az alkalmazott eszköz vagy élőerő korlátozása nélkül alkalmas. Amennyiben ez az érték 30%-nál nagyobb, akkor a művelet

végrehajtására a körülmények nem alkalmasak, pontosabban túl nagy a kockázata annak, hogy a körülmények alkalmatlanok lesznek a vizsgált nap adott részében. A két érték közötti tartományban a művelet korlátozottan és/vagy csak kisebb hatékonysággal és/vagy kisegítő eszközök alkalmazásával hajtható végre az esetlegesen alkalmatlan körülmények elfogadható kockázata mellett. Az ismertetett értékekkel és a korábbiakban bemutatott vonatkozó tagsági függvény általános alakja alapján a tagsági függvény konkrét alakját a 4. ábra mutatja be.



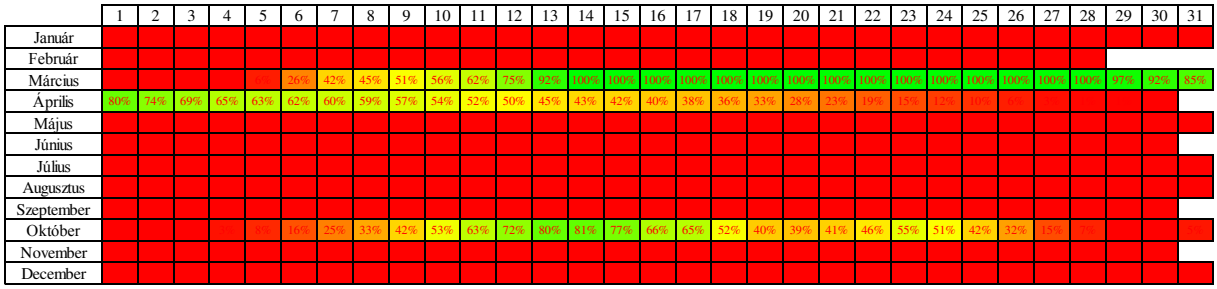
4. ábra. A tagsági függvény alakja adott kategória relatív gyakorisága esetében

A fentiek figyelembe vételével a modell futtatását két különböző módon végeztük el. Az első esetben a kiválasztott paraméterek azonos súllyal szerepelnek, azaz felhasználói szempontból azonos fontosságúak. A második esetben pedig a paraméterek felhasználó általi páronkénti összehasonlítását követően az AHP módszerrel kalkulált súlyok kerültek alkalmazásra (látástávolság: 0,58; felhőalap: 0,31; napi átlaghőmérséklet: 0,11). A páronkénti összehasonlító értékelést az 1. táblázat szemlélteti.

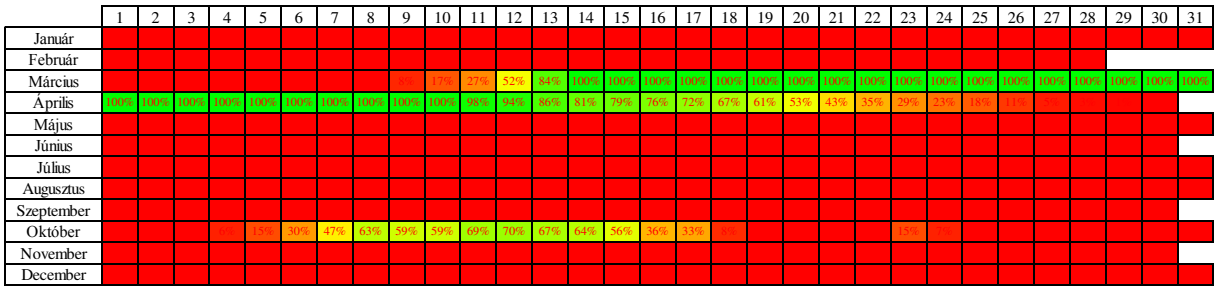
1	3						5					7						9
egyformán fontos	mérsékelten fontosabb						sokkal fontosabb					nagyon sokkal fontosabb						rendkívüli mértékben fontosabb
Látástávolság	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Felhőalap
Látástávolság	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Napi átlaghőmérséklet
Felhőalap	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Napi átlaghőmérséklet

1. táblázat. A páronkénti összehasonlítás eredménye és értékelése

Az 5. és 6. ábra mutatja be a két futtatás eredményét. A legmarkánsabb különbséget a fontossági preferencia esetében az adja, hogy a műveletek végrehajtására tervezett időszak nagy biztonsággal kiterjeszthető április első felére is, illetve az októberi időszak értékei egyértelmű csökkenést mutatnak. Az első esetben a 100%-ot csak azok az esetek jelentik, amikor mindegyik paraméter értékei az alkalmas tartományban találhatók. A súlyok alkalmazása esetében 100%-ot jelentenek azok az esetek is, amikor a legfontosabb paraméter értéke van csak az alkalmas tartományban, de a többi paraméter értéke nem tér el jelentősen az alkalmas értéktartománytól. Jelentős eltérésről akkor beszélünk, ha ebben az esetben a kevésbé fontos paraméter hasonlóságának mértéke az AHP módszerrel meghatározott súlyok különbségének 1-ből kivont értéke alá csökken. Tehát minél nagyobb a fontosságbeli különbség, az eljárás annál megengedőbb lesz a kevésbé fontos paraméter értékeinek esetében az elfogadható tartományon belül.



5. ábra: A modell által a művelet végrehajtására kijelölt időszakok a paraméterek fontosság szerinti értékelése nélkül



6. ábra. A modell által a művelet végrehajtására kijelölt időszakok a paraméterek fontosság szerinti értékelésével

ÖSSZEGZÉS, TOVÁBBI TERVEK, FEJLESZTÉSI LEHETŐSÉGEK

Cikkünkben a katonai műveletek tervezésének meteorológiai támogatási modelljére tettünk javaslatot. A javasolt modell a fuzzy logika és az AHP eljárás eszközrendszerét felhasználva segít a tervezett műveletek végrehajtási időszakának kijelölésében az adatbázisban rendelkezésre álló származtatott klimatológiai paraméterek figyelembe vételével valamint lehetővé teszi a felhasználó számára a kiválasztott paraméterek fontosság szerinti priorizálását. Emellett lehetőséget ad tervezett haditechnikai eszközök bevezetése előtt, azok adott éghajlati környezetben történő alkalmazhatóságának vizsgálatára is.

Fejlesztési terveink között szerepel az adatbázis SYNOP táviratokból származtatott mennyiségekkel való bővítése, amely a jelenleg használt paraméterek minőségének javítását illetve új mennyiségek bevezetését tenné lehetővé. Meg kívánjuk továbbá vizsgálni egyéb, nem meteorológiai paraméterek bevezetésének lehetőségét, hiszen a modell ebből a szempontból nyitott, alkalmazható egyéb jellemzők vizsgálatára is. Végül szeretnénk kidolgozni egy olyan felhasználói felületet, amely felhasználóbarát módon teszi lehetővé a modell használatát.

ÚJ SZÉCHENYI TERV

A PUBLIKÁCIÓ A TÁMOP-4.2.1.B-11/2/KMP-2011-00010 „KRITIKUS INFRASTRUKTÚRA VÉDELMI KUTATÁSOK” PÁLYÁZAT KERETÉBEN KÉSZÜLT. A PROJEKT AZ EURÓPAI UNIÓ TÁMOGATÁSÁVAL, AZ EURÓPAI SZOCIÁLIS ALAP TÁRSFINANSZÍROZÁSÁVAL VALÓSUL MEG.

Felhasznált irodalom

[1] Tuba Zoltán – Wantuch Ferenc – Bottyán Zsolt – Hadobács Katalin – Jámbor Krisztián: Repülésmeteorológiai klíma adatok felhasználásának lehetséges aspektusai pilóta nélküli repülőeszközök (UAV-k) meteorológiai támogatásában. Szolnoki Tudományos Közlemények, XVI., 2012, http://www.szolnok.mtesz.hu/sztk/kulonszamok/2012/cikkek/2012-17-Tuba_Zoltan_es_a_tobbiek.pdf

[2] B. K. Hansen: A Fuzzy Logic–Based Analog Forecasting System for Ceiling and Visibility. Weather and Forecasting, Vol. 22, 1319–1330., 2007

[3] Hadobács Katalin – Tuba Zoltán – Wantuch Ferenc – Bottyán Zsolt – Vidnyánszky Zoltán: A pilóta nélküli légijárművek meteorológiai támogató rendszerének kialakítása és alkalmazhatóságának bemutatása esettanulmányokon keresztül. Repüléstudományi Közlemények, 25, 2, 405-421., 2013, http://www.szrfk.hu/rtk/kulonszamok/2013_cikkek/2013-2-31-Hadobacs_Katalin_es_a_tobbiek.pdf

[4] L. A. Zadeh: Fuzzy sets. Information and Control, 8, 338-353., 1965

[5] B. K. Hansen – D. Riordan: A fuzzy case-based system for weather prediction. Engineering Intelligent Systems, 3, 139–146., 2002

[6] T. Saaty: A scaling method for priorities in hierarchical structures, Journal of mathematical psychology 15(3), 234-281., 1977

[7] Temesi József: A döntéselmélet alapjai. Aula, 2002

[8] Rapcsák Tamás: Többszempontú döntési problémák. MTA Sztaki, 2007

[9] Gyarmati József: Döntési modell kialakítása közbeszerzési eljárás során. Hadmérnök, 3, 36-52., 2007

[10] Gyarmati József – Felházi Sándor – Kende György: Choosing the Optimal Mortar for an Infantry Battalion's Mortar Battery with Analytic Hierarchy Process using Multivariate Statistics. In: Gyarmati József – Felházi Sándor – Kende György: Decision Support Methodologies for Acquisition of Military Equipment, Konferencia helye, ideje: Brüsszel, Belgium, 2009.10.22-2009.10.23. Brüsszel: NATO RTO, 2009. pp. 1-12. (ISBN:978-92-837-0101-9)

[11] Bottyán Zsolt – Wantuch Ferenc – Tuba Zoltán – Hadobács Katalin – Jámbor Krisztián: Repülésmeteorológiai klíma adatbázis kialakítása az UAV-k komplex meteorológiai támogató rendszeréhez. Repüléstudományi Közlemények, 24, (3), 2012, pp. 11-18., http://www.szrfk.hu/rtk/folyoirat/2012_3/2012-3-02-Bottyan_Zs_es_a_tobbiek.pdf