HADMÉRNÖK

KATONAI MŰSZAKI TUDOMÁNYOK ONLINE

IX. Évfolyam 3. szám 2014. szeptember

NKE
BUDAPEST

A szerkesztőség elérhetősége:
Nemzeti Közszolgálati Egyetem,
1101. Budapest, Hungária krt. 9-11. A. épület 9. emelet, 901. iroda
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:

Balog Károly - Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Bárdos Zoltán - Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Bartha Tibor
Berecz Antónia - Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Diamant Péter Kamilló - MH Egészségügyi Központ I.sz Általános Sebészeti Osztály
Dr. Fekete Károly - Nemzeti Közszolgálati Egyetem, KÜI egyetemi docens
Dr. Fekete László - MH Egészségügyi Központ I.sz Általános Sebészeti Osztály
Gávay György - Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
GRÉGORY, Lucas - Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Gyarmati József - Nemzeti Közszolgálati Egyetem, KLI egyetemi docens
Gyebrovszki Tamás - NBSZ Kormányzati Eseménykezelő Központ
Dr. Györkös Roland István – Nemzeti Adó-és Vámhivatal
Dr. Halász László - Nemzeti Közszolgálati Egyetem, HHK professzor emeritus
Dr. Kalácska Gábor - Szent István Egyetem, Gépészmérnöki Kar, egyetemi tanár
Károly Krisztián - Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Kassai Károly - Honvédelmi Minisztérium, HIICSF, osztályvezető
Kátai-Urbán Lajos - Nemzeti Közszolgálati Egyetem, KI egyetemi docens
Dr. Kende György - Nemzeti Közszolgálati Egyetem, HHK egyetemi tanár
Kiss Béla Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. Koronváry Péter - Nemzeti Közszolgálati Egyetem, KTK egyetemi docens
Kovács Zoltán - Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Lukács Loránd - Budapesti Műszaki és Gazdaságtudományi Egyetem, VIK doktorandusz
Mészáros Gergely - Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Muhoray Árpád - Nemzeti Közszolgálati Egyetem, KI egyetemi docens
Dr. Nagygyörgy Ádám - MH Egészségügyi Központ I.sz Általános Sebészeti Osztály
Nagyné Dr. Takács Veronika - Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Papp Zoltán - Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
PÖCHER, Harald - Bundesheer
Rácz László - Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Rajki János - MH vitéz Szurmay Sándor Budapest Helyőrség Dandár, MH HIRFK
Sebők István - Nemzeti Közszolgálati Egyetem, HHK gyakorlati oktató
Dr. Szakál Zoltán - Szent István Egyetem, Gépészmérnöki Kar, adjunktus
Szegediné Dr. Lengyel Piroska – Zsigmond Király Főiskola főiskolai docens
Takács Zoltán - Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Tóth Eszter – MH Egészségügyi Központ VEI RAVGYI
Török Szilárd - Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Zentai Ágnes - Harmónia Egészségcentrum

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Takács Zoltán
takacs@samsonterv.hu

ELEKTRONIKUS MEGFIGYELÉS JOGSZABÁLYI HÁTTERE

Absztrakt

Az elektronikus megfigyelőrendszer a biztonságtechnikában a legelterjedtebb elektronikai eszköz. A felvételek készítése, tárolása, felhasználása csak az emberi, valamint a személyiségi jogok figyelembevételével történhet. A szerző a cikkben a 2014 júniusban érvényes jogszabályok és állásfoglalások alapján kívánja bemutatni a munkahelyeken az elektronikus megfigyelés tájékoztatási kötelezettségeit.

The electronic surveillance system for security technology, the most widely used electronic devices. Preparation, storage and use of the images only human, and taking into account the place of privacy. The author wishes to present in the workplace electronic surveillance information obligations according to the valid laws and resolutions in June 2014 article.

Kulcsszavak: *elektronikus megfigyelés, képrögzítés ~ elektronical observation, image recording*

BEVEZETÉS

Általánosságban elmondható, hogy vagyonvédelmi szempontból a kamerák jelenléte egyrészt visszatartó hatású a cselekménytől, másrészt a bekövetkezett esemény után az események könnyebben rekonstruálhatók. Munkaidő alatt a részleges élesítettségű státuszban lévő behatolás jelző rendszer védelmét a videó megfigyelő rendszer egészíti ki információ begyűjtésével, tárolásával. A videó megfigyelő rendszer a munkahelyen lehetségesen előforduló számos esemény esetén hasznos segítséget jelenthet. A videó megfigyelő rendszer természetesen nem sértheti az ott dolgozó személyek alapvető jogait, ügyelni kell, hogy az öltöző, tisztálkodó, szociális helyiségek tereit nem lehet megfigyelni. A térfelügyelet eme hatékony eleme kialakításánál fontos, hogy a rögzített kép az adatvédelmi jogszabályok figyelembevételével kerüljön rögzítésre és az elvárt képminőség, valamint a pontos időhöz történő időszinkronizálás biztosított legyen. [1]

ELEKTRONIKUS MEGFIGYELÉS

A video megfigyelő rendszerek zártláncú televízió rendszerek, amelyeket csak a hálózatba kapcsolt csoport tagja láthatják. A megfigyelő eszközök lehetnek fixen telepített, vagy vezérelhető eszközök. A vezérelhető eszközöket a vezérlőből, vagy számítógépre telepített szoftver segítségével lehet irányítani. A vezérlés irányulhat a kamera mozgatására, vagy annak fókuszának állítására. A megfigyelő eszközök lehetnek kültéri vagy beltéri kamerák. [2]. A megfigyelés történhet élőképen, a monitorok figyelésével, valamint az adatok adathordozóra, vagy merevlemezre való rögzítéssel archiválhatók, később azok visszanézhetők.

A monitorok megfigyelése, valamint a rögzített adatok felhasználása aggályokat vethet fel az információs önrendelkezési joggal kapcsolatban, a személyiségi jogokkal kapcsolatban. Ezzel kapcsolatosan a Nemzeti Adatvédelmi és Információs Hatóság 2013-ban ajánlást adott ki, amelyben kifejti a munkáltató tájékoztatási kötelezettségét a munkavállaló felé. A tájékoztatás célja az elektronikus megfigyelőrendszer rövid bemutatása, a képződött adatok kezelésének és tárolásának, a módjának, valamint az adatokhoz való hozzáférhetőségének bemutatása.

JOGSZABÁLYI ELŐZMÉNYEK

1993-ban elfogadásra került a LIX. törvény az országgyűlési biztosokról. Ekkor három országgyűlési biztosi címet neveztek meg:

- állampolgári jogok biztosa
- adatvédelmi biztos
- kisebbségi jogok biztosa

majd 2008-tól a jövő nemzedékek biztosa. Az adatvédelmi biztos fel lett jogosítva e törvény által, hogy a törvényekbe ütköző adatbázisokat megsemmisítse, valamint jogi szakértelmének, tapasztalatának megfelelően a panaszos ügyek kivizsgálását, jogsérelmek esetén a sérelem tárgyának megszüntetését elősegítse. Az ombudsman ellenőrzési tevékenységet is jogosult volt végrehajtani. [3] A Munka Törvénykönyve megfogalmaz olyan kritériumokat, amelyek iránymutatásul szolgálhatnak a munkahelyi elektronikus megfigyelőrendszerekre (Mt. 9. valamint a 11. §-ai). [4]

Az elektronikus munkahelyi megfigyelést a Munka Törvénykönyve [4], a személy-és vagyonvédelmi törvény [5], valamint az információs önrendelkezési jogról szóló törvény, [6] szabályozza.

Hatósági állásfoglalás [7]

A Munka Törvénykönyve általánosan fogalmaz, ezért egyes munkahelyeken a szabályozások az információs önrendelkezési jognak különböző mértékű teljesülését eredményezheti. Az egységes mértékű érvényesülés érdekében a Nemzeti Adatvédelmi és Információszabadság Hatóság 2013. január 23-n egy ajánlást adott ki. Az ajánlás alapján a munkahelyen jogszerűen lehet elektronikus megfigyelést végezni az alábbi feltételek alapján:

- a munkavállaló köteles a munkáltató iránymutatása alapján munkát végezni, tehát a tőle elvárható gondossággal, szaktudással és a munkavégzési szabályok megtartásával eljárni [7]
- a munkáltató a Munka Törvénykönyve feljogosítása alapján lehetőséget kapott arra, hogy a munkavállalót a munkavégzéssel kapcsolatos tevékenységek során ellenőrizze (ez a tevékenység adatkezeléssel jár) [7]
- „… munkáltatói ellenőrzéshez kapcsolódó adatkezelés… a munkaviszony természetéből fakadó, a munkavállalói hozzájárulástól adott esetben független adatkezelés.” [7]

Ennek megfelelően az adatkezelést korlátozzák a következő rendelkezések:

- „A munkáltatói ellenőrzés és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével; illetőleg a munkavállaló magánélete nem ellenőrizhető.” [4] [7]
- „A munkavállalót előzetesen tájékoztatni kell az adatkezelés lényeges követelményeiről” [4] [6] [7]
- „Az adatkezelés akkor jogszerű, ha a munkáltató az adatkezeléssel kapcsolatban betartja az Infotv. alapvető rendelkezéseit: a célhoz kötött és a tisztességes adatkezelés elvét. A munkáltatói ellenőrzés akkor tekinthető jogszerűek, amennyiben az a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges.” [4] [7]
- „A munkáltatói ellenőrzés akkor tartható jogszerűnek, amennyiben az a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges.” [4] [7]

A MUNKAHELYI ELEKTRONIKUS MEGFIGYELÉS GARANCIÁLIS KÖVETELMÉNYEI

Az ajánlás kitér arra, hogy a munkáltató köteles a az alkalmazott eszközökkel kapcsolatban egy belső szabályozást kiadni, amely mindenki számára egyértelműen, közérthető nyelvezetben megfogalmazva részletesen szabályozza az adatkezelést. Ez a belső szabályozás a garancia arra, hogy a munkáltató az alkalmazottat a Munka Törvénykönyvében, valamint az Információs önrendelkezési jogról és információszabadságról szóló törvény keretein belül ellenőrizze.

- Az adatok felhasználhatóságának a határait a 2005. évi CXXXII. törvény a személy- és vagyonvédelmi, valamint magánnyomozói tevékenység szabályairól szóló törvény (továbbiakban SzvTv.) 31.§ 1. – 7. pontja szabályozza. Általánosságban elmondható, hogy a fel nem használt felvételeket a felvétel készítését követő harmadik munkanapon azt törölni kell.
- Elektronikus megfigyelőrendszert biztonságtechnikai szerelő, vagy elektronikus vagyonvédelmi rendszerszerelő telepíthet, annak kezelését biztonságtechnikai kezelő, biztonságtechnika-kezelő, személy- és vagyonőr, biztonsági őr, vagy fegyveres biztonsági őr végezheti. [5]

- A munkáltató köteles igazolni azt, hogy a kiépített elektronikus megfigyelő rendszer megfelel a célhoz kötöttség elvének [6]. Az elektronikus megfigyelőrendszert elsősorban emberi élet, testi épség, személyi szabadság védelme, a veszélyes anyagok őrzése, az üzleti, fizetési, bank- és értékpapírtitok védelme, vagyonvédelem céljából lehet alkalmazni. Így például a kamerás megfigyelés esetkörébe tartozhat a veszélyforrást hordozó létesítmények, munkahelyiségek (nagyteljesítményű gépeket tartalmazó szerelőcsarnokok, egyes gyártási folyamatok). [5]
- A garanciáknak ki kell terjednie az emberi méltóság tiszteletben tartására. [4]
- Az elektronikus megfigyelés által készült felvételek alkalmasak arra, hogy a megfigyelt területen dolgozó személyek szokásait, behatoljanak a magánszférába, valamint intim élethelyzeteket rögzítsen. Ezek miatt korlátozni kell a felvételekbe való betekintés lehetőségét, amelyre a munkahelyi szabályozásban, és a szabályozás végrehajtásában garantálni kell.
- Nem megengedett olyan kamera kihelyezése, amely célzottan egy munkavállalót, és/vagy az ő tevékenységét figyeli meg, vagy olyan kamerarendszer alkalmazása, amelynek célja a dolgozók munkahelyi viselkedésének befolyásolása.
- Olyan élethelyzeteket megfigyelni/rögzíteni szintén nem megengedett, amely az emberi méltóságot sérti, így különös tekintettel öltözőkben, mosdókban, orvosi szobában, vagy az ahhoz tartozó váróteremben, vagy ahol a dolgozók a munkaközi szüneteiket töltik. Ez azonban nem jelenti azt, hogy ezeket a helyiségeket nem lehet megfigyelni akkor sem, ha jogszerűen ott nem tartózkodhat senki (pl. munkaszüneti napon).
- A kamerák látószögét úgy kell meghatározni/beállítani, hogy a látószöge teljesítse a célhozkötöttség elvét, az csak a céljával összhangban lévő területre irányulhat, a megfigyelőrendszer csak saját tulajdonban/használatban lévő terület megfigyelésére alkalmazható.

A munkavállalót, valamint a területre érkező minden látogatót tájékoztatni kell megfigyelés tényéről. A munkavállalóval szemben nincs szükség a munkavállaló hozzájárulására a megfigyelésnek, azonban őt egy – a munkaszerződéstől független dokumentumban – tájékoztatni kell a megfigyelés tényéről, és az adatkezelésről. A tájékoztatónak legalább az alábbi információkat kell tartalmazni:

- A jogszabályi háttérre
- Tájékoztatni kell a megfigyelés céljáról, a területről vagy a megfigyelés tárgyáról
- Tájékoztatni kell a megfigyelés módjáról (közvetlen megfigyelés, vagy rögzített mód)
- Az elektronikus megfigyelőrendszert üzemeltető személy meghatározásáról
- Hol-, és mennyi ideig kerülnek megőrzésre a felvételek
- Milyen adatbiztonsági intézkedéseket (garanciákat) hozott a munkáltató
- Kik, és milyen célból jogosultak a felvételek megtekintésére,
- Fel kell hívni a jogaikra, és a jogaik alkalmazásának módjaira a figyelmet
- Továbbá tartalmaznia kell azt, hogy az információs önrendelkezési jogokban bekövetkezett vélt vagy valós sérelmeik esetén milyen jogorvoslatokkal élhetnek

A munkáltató köteles továbbá figyelemfelhívó jelzést kihelyezni az elektronikus megfigyelés tényéről. Olyan területen, ahol munkavállaló és látogató egyaránt tartózkodhatnak, akkor a munkáltatónak gondoskodnia kell ismertető elhelyezéséről is. [5]

A megfigyelést kezdeményező munkáltató bejelentési kötelezettséggel tartozik a Nemzeti Adatvédelmi és Információs Hivatal felé, és ebben a bejelentésben nyilatkozni kell arról, hogy az Infotv. [6] 65.§ (3.) bekezdés a) pontja hatálya alá tartozik-e. [7]

BEFEJEZÉS

A munkahelyeken, úgymint az egészségügyi intézményekben, benne a rendelőintézetekben, kórházakban kialakított munkafolyamatok, gyógyászati segédeszközök és gyógyszerek védelme kiemelt fontosságú, beleértve az ott dolgozó, kezelt, vagy oda látogató személyek személy- és vagyonvédelmét. A megfigyelőrendszerek önmagukban nem alkalmasak a védelemre, azonban a jól látható és táblákkal való figyelemfelhívás a megfigyelésre, visszatartó erejű. A megfigyelőrendszerek csak részei a komplex biztonsági rendszereknek.

A védelmi terv kialakításakor figyelembe kell venni, hogy sem az ott dolgozókat, sem pedig az oda látogatókat ne feszélyezze a védelmi rendszer megléte. A kamerarendszerek kialakítása különös körültekintést igényel az egészségügyi intézményekben, ahol különösen nehéz az intézmény jellege miatt a rendszer kialakítása, ahol a kezeltek a kezelés, valamint a vizsgálatok jellege miatt sokszor kerülnek intim helyzetekbe. A védelmi terv kialakításánál javasolt kikérni az ellátást biztosító egészségügyi személyzet véleményét a kezeltek emberi méltóságának megőrzése érdekében. Egészségügyi intézményekben kiemelt figyelmet kell fordítani a fertőző-, vagy méreganyagok védelmére, úgymint a kábító hatású szerek védelmére.

AJÁNLÁS A MUNKAHELYI TÁJÉKOZTATÓ TARTALMÁRA

A fenti ajánlások betartásával a következő tájékoztatás szerkeszthető, amely a jogszabályi követelményeknek is maradéktalanul eleget tesz:

Tájékoztatás célja

Ez a tájékoztatás leírja az elektronikus vagyonvédelmi rendszer használatának törvényi feltételeit, a képződött adatok felhasználásának és tárolásának módját, az adatok kezelésére valamint felhasználására jogosult személyek / szervezetek nevét, és az a adatkezelés szabályozását.

Jogszabályi háttér

Elektronikai vagyonvédelmi rendszer alkalmazása esetén a Munkáltató köteles tájékoztatást nyújtani munkavállalói részére. A munkáltatói ellenőrzéshez kapcsolódó adatkezelés a Munka Törvénykönyve alapján a munkaviszony természetéből fakadó, a munkavállalói hozzájárulástól független adatkezelés.

Tájékoztatási kötelezettség

Ez a tájékoztató anyag tartalmazza a munkáltató által alkalmazott az elektronikus vagyonvédelmi rendszerre tekintettel az alábbiakat:

- az adatkezelés jogalapját;
- az egyes kamerák elhelyezésére és a vonatkozásukban fennálló célra, az általuk megfigyelt területre, tárgyra, illetőleg arra, hogy az adott kamerával, közvetlen vagy közvetett megfigyelést végez-e a munkáltató;
- az elektronikus rendszert üzemeltető személy meghatározását;
- a felvételek tárolási helyét és időtartamát;
- az adatok megismerésére jogosult személyek körét, illetőleg arra, hogy a felvételeket a munkáltató mely személyek, szervek felé milyen esetben továbbíthatja;
- a felvételek visszanézésére vonatkozó szabályokat, illetve, azt, hogy a felvételeket milyen célból használhatja fel a munkáltató;
- a munkavállalókat milyen jogok illetik meg az elektronikus megfigyelőrendszerrel kapcsolatban és milyen módon tudják gyakorolni a jogaikat;

- a munkavállalók az információs önrendelkezési joguk megsértése esetén milyen jogérvényesítési eszközöket vehetnek igénybe.
- A munkavállalók tájékoztatása megfigyelőrendszer működéséről és annak szabályozásáról jelen dokumentum tudomásul vételével megtörténik. Új munkavállalók esetén a tájékoztatás a munkába állás előtt, jelen dokumentum megismertetésével történik.
- A munkáltató kötelezettségének megfelelve figyelemfelhívó jelzést helyezett el arról, hogy az adott területen elektronikus megfigyelőrendszert alkalmaznak. [5]

Adatkezelés jogalapja

Az elektronikus vagyonvédelmi rendszer alkalmazására elsősorban személy- vagyonvédelmi okok miatt kerül sor.

Kamerával történő megfigyelés

Az egyes telephelyeken a személy- és vagyonvédelmi kamerák elhelyezkedését jelen tájékoztatás mellékletei tartalmazzák. Általánosságban kijelenthető, hogy a munkáltató által elhelyezett minden kamera vagyonvédelmi célt szolgál. A kamerák által megfigyelt terület a telephelyek bejárata, illetve a telephelyeken lévő épületek kijáratai, rakodórámpái.

Az elektronikus vagyonvédelmi rendszer üzemeltetési szabályai

- A munkáltató a munkavállalók személyhez fűződő jogát tiszteletben tartja, annak korlátozásának módjáról, feltételeiről és várható tartalmáról előzetesen tájékoztatta. /Mt. 9. § (1)-(2)/
- A munkáltató a munkavállalót csak a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló magánélete nem ellenőrizhető. /Mt. 11. § (1)/
- A munkáltató előzetesen tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak. /Mt. 11. § (2)/
- Az adatkezelés során jogszerűen járunk el, mivel betartjuk az Infotv. 4. § (1)-(2) alapvető rendelkezéseit, ami a célhoz kötött és tisztességes adatkezelés elve.
- A rögzített felvételeket főszabályként 21 napig tároljuk. A tárolás helye a DVR valamint beléptető rendszer vezérlő számítógépének a merevlemeze. A 3 napnál hosszabb ideig történő felvétel megőrzés azért indokolt, mert a termelés során keletkezett hibás gyártmány felfedezése gyakran a vevőnél történik meg, ezért a hiba felfedezése után a minőségügyi, gyártástechnológiai elemzések folytán a felvételekre szükség lehet.
- A rögzített felvételeket a munkáltató harmadik fél részére csak törvényben meghatározott esetben (pl. rendőrség, munkavédelmi hatóság részére) adja át. A rögzített anyagokat kizárólag szabálysértés vagy bűncselekmény gyanúja, munkahelyi baleset esetén lehet visszanézni.
- A munkáltató igazolni tudja, hogy az általuk alkalmazott elektronikus megfigyelőrendszer és beléptető rendszer egymástól független, és összeegyeztethető az Infotv. 4. § (1)-(2) bekezdésében szereplő célhoz kötöttség elvével és érdekmérlegelés teszttel. Ezek szerint a személyes adatok kizárólag meghatározott célból, jogi gyakorlás és kötelezettség teljesítése érdekében kezelhető.

- A célhoz kötöttség elve, illetve az érdekmérlegelés tesztje is megköveteli, hogy a kamerák látószöge a célterületre irányulhatnak csak. Így kizárólag saját tulajdont vagy használatban lévő területet figyelünk meg.
- A munkavállalóknak kiadott a megfigyelőrendszerről szóló tájékoztatóban pontosan megjelölésre kerültek, hogy az adott kamerák milyen célból lettek elhelyezve, milyen területre irányul a látószögük.
- A munkáltató elsősorban emberi élet, testi épség, személyi szabadság védelme, veszélyes anyagok, veszélyes gépek megfigyelése, illetve vagyonvédelem céljából alkalmazza az elektronikus vagyonvédelmi rendszert.
- A munkáltató olyan kamerával nem rendelkezik, amely kizárólag egy munkavállalót és az általa végzett tevékenységet figyeli meg, vagy aminek célja a munkavállaló viselkedésének befolyásolása.
- A munkáltató nem végez megfigyelést olyan helyiségekben, és nem telepít beléptető rendszert, ahol ez az emberi méltóságot sértheti. Különösen vonatkozik ez öltözőkre, zuhanyzókra, illemhelyekre, öltözőkre, de olyan helyiségben sem, ahol a munkavállaló a munkaközi szünetét tölti.
- Vannak azonban olyan időszakok, amikor a munkahely teljes területe megfigyelhető, beleértve a tiltott területek is. Ezek az időszakok pl. munkaszüneti napok, munkaidőn kívüli napok, amikor senki nem tartózkodik jogszerűen a területen.
- Az Infotv. alapelveit alkalmazzuk a felvételek visszanézésekor is. Csak szűk személyi csoport rendelkezik jogosultsággal, akik döntéshozatali jogkörrel rendelkeznek.

Adatok kezelésére, felhasználására jogosult személyek / szervezetek

Az elektronikus megfigyelőrendszert vagyonvédelmi szolgáltató vállalkozás üzemelteti, az élőképet a Szolgáltató vagyonőr munkatársai figyelik. A rögzített felvételek legfeljebb 3 munkanapig tárolhatók, a felvételeket gyanú esetén a biztonsági szakember ismételten megnézi. A felvételeket jogerős határozat/végzés ellenében, vagy a hatóságok felszólítására a hatóságok részére át kell adni. Az adatok a rögzítő merevlemezén kerülnek tárolásra. A merevlemez tárkapacitása úgy lett meghatározva, hogy három naponként újra írja önmagát.

Mellékletek

- Melléklet: kamerával megfigyelt terület, jelölve a kamera látószöge

Panaszkezelés

Az a személy vagy szervezet, aki vélelmezi, hogy jogaiban korlátozás történt, vagy jogsérelem érte, írásban kérelmezheti a cégvezetőtől, vagy a NAIH ügyfélszolgálatán (1530 Budapest, Pf.: 5. címen, vagy személyesen a 1125 Budapest, Szilágyi Erzsébet fasor 22/c címen illetve a +36 (1) 391-1400 telefonszámon, illetve az ugyfelszolgalat@naih.hu e-mail címen.) az eset kivizsgálását.

Elosztás

- Minden munkavállaló oktatásban részesül:
    a) új belépők bevezető oktatásán
    b) éves ismétlő oktatás keretein belül
- Ha a munkavállalókon kívül egyéb személyek is a megfigyelt területre lépnek, akkor ők az Szvtv. szerint külön tájékoztatást kapnak. Az ügyfelek, vendégek a munkáltató területére való belépéssel elismerik és tudomásul veszik a kamerás megfigyelés tényét

és egyben hozzájárulnak ahhoz, hogy róluk felvétel készüljön. A megfigyelő rendszer létéről és működéséről a munkáltató kötelezettségének megfelelve figyelemfelhívó jelzést helyezett el arról, hogy az adott területen elektronikus megfigyelőrendszert alkalmaznak.

Felhasznált irodalom

[1] Berek Tamás: Vagyonvédelmi koncepció kialakításának sajátosságai veszélyes anyagok vizsgálatát biztosító létesítmények esetében 2011. Hadmérnök http://hadmernok.hu/2011_4_berek.php

[2] Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései (doktori értekezés, 2009. Budapest

[3] Az állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. Törvény

[4] 2012. évi I. törvény a munka törvénykönyvéről

[5] 2005. évi CXXXII. törvény a személy-és vagyonvédelmi, valamint magánnyomozói tevékenység szabályairól

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

[7] Nemzeti Adatvédelmi és Információs Hatóság NAIH-4011-6/2012/V (2013.01.23 Dr. Péterfalvi Attila) ajánlása

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Bartha Tibor
bartha.tibor@uni-nke.hu

LTLX 7000 – EGY ÚJSZERŰ NEM HALÁLOS FEGYVER AGÓNIÁJA?

Absztrakt

A nem halálos fegyverek egyik jól ismert csoportját azon eszközök képezik, amelyek a célba becsapódó lövedékek okozta traumahatást használják fel a szemben álló fél megállítására, harc- vagy cselekvésképtelenné tételére. A lövedékek lehetnek gumigolyós, gumisörétes, babzsák, vagy a nagyobb kaliberű habszivacs gránátok. Ezen fegyverek alapvető problémája, hogy kisebb lőtávolságon képesek akár halálos kimenetelű sérülés okozására is, nagyobb lőtávolság esetén pedig hatásuk jelentéktelen. Ezen alapvető probléma megoldására körvonalazódott az olasz Védelmi Minisztérium és a Beretta cég közös programja 2001-ben. A fejlesztés eredménye az LTLX 7000 típusjelű nem halálos fegyver, képes volt közel állandó becsapódási energiát biztosítani 70 méterig. A fegyvert elsősorban a béketámogató műveletekben résztvevőknek szánták. Az ígéretes fejlesztésből a lendület az évtized végére lassan kifogyott és napjainkban úgy néz ki, hogy lassan el is felejtődik. A szerző a fejlesztés folyamatába ad bepillantást.

As a group of the non-lethal weapons represents those kinetic energy weapons, that are able to deliver non penetrating projectiles to the targets. Among others these weapons are eg. 12 gauge rubber bullest, ammunition and bean bag rounds as well as in larger caliber 40 mm sponge grenades. In general these ammunition are able to temporarily incapacitate the target. The main problem of these weapons that they are often powerfull enough to kill at close range and to weak at long range to stop the target. As a the solution of this problem a new development project was launched by Fabbrica d'Armi Pietro Beretta S.p.A. in cooperation with Italian Ministry of Defence in 2001. The result of this development was Beretta LTLX 7000 Constant Kinetic Energy Weapon. The LTLX 7000 delivers the same kinetic energy on the target up to 70 meters, regardless of the range. The weapon was intended to use for Italian peace support military units. At the beginning the project was very promising, however by the end of the last decade the impulse of the development slowed down and nowadays it seems slowly but surely died. In this article the author gives an insight into the details of the project.

Kulcsszavak: ***n****em halálos fegyverek, állandó kinetikai energiájú fegyver, nem áthatoló lövedék, kutatás-fejlesztés ~ non-lethal weapons, constant kinectic energy weapon, non-penetrating bullets, research and development.*

BEVEZETÉS

A nem halálos fegyverek egyik jól ismert csoportját azon eszközök képezik, amelyek a célba becsapódó lövedékek okozta traumahatást használják fel a szemben álló fél megállítására, ideiglenes harc- vagy cselekvésképtelenné tételére. Ebbe csoportba tartoznak többek között a gumi vagy egyéb plasztikus anyagból készült lövedékek, sörétek, repeszek, habszivacs gránátok, illetve babzsák lövedékek (1. ábra).

1. ábra. 40 mm habszivacsgránát, üstökös és négyzet alakú babzsák lövedékek [2]

Ezeket a lövedékeket, gránátokat szokás nem áthatoló lövedékeknek, gránátoknak is nevezni. A lövedékek célba juttatására sima vagy huzagolt csövű fegyvert egyaránt alkalmaznak. Huzagolt cső esetén a gránátok szórása, azaz a fegyver pontossága nagyban megnő. Jellemző űrméretük simacsövű fegyverek esetén a 12-es, gránátok esetén pedig a 37 mm vagy 40 mm. A gránátvető lehet önálló fegyver vagy szerelhetik a katona egyéni lőfegyverének csöve alá.

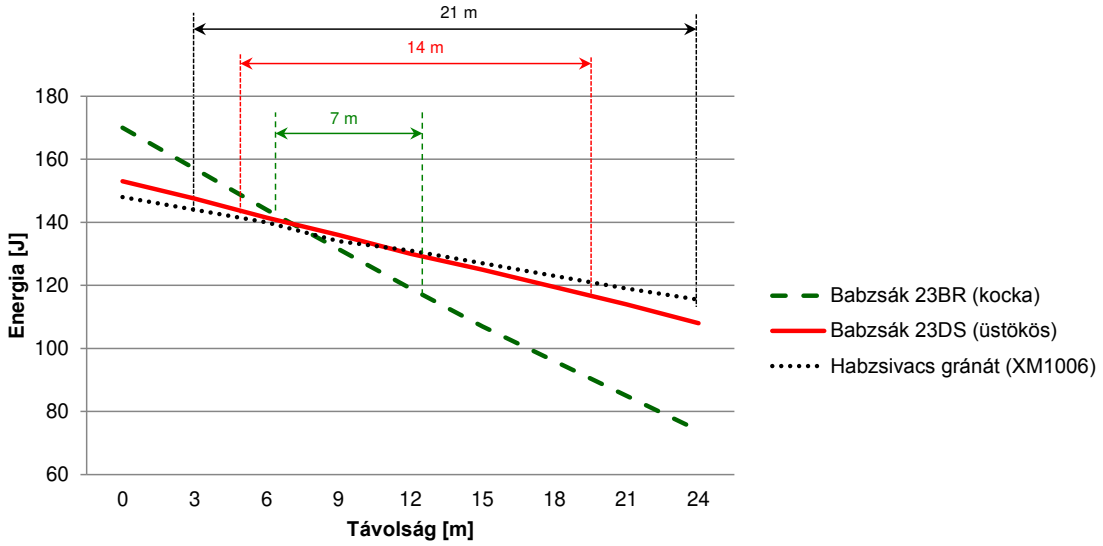
A nem halálos fegyverek ezen csoportjába sorolják az FN 303 típusjelzésű sűrített levegővel működő, törékeny lövedéket alkalmazó félautomata fegyvert is, amelyet a belgiumi Fabrique Nationale de Herstal fejlesztett ki 2003-ban. Az FN 303 a polgári életben oly népszerű paintball fegyverek rendfenntartó célra is alkalmazott nagyobb testvérének tekinthető.

A nem áthatoló lövedékek a célba való becsapódásuk alkalmával mozgási energiájuk száz százalékát a célnak „adják át” ezáltal jelentős, de a célszemély által – az esetek többségében – még elviselhető traumahatást idéznek elő. A lövedékek által okozott traumahatás általában elegendő ahhoz, hogy a célszemélynek komoly fájdalmat, zúzódást okozzon. Hatásukkal biztosítani tudják, hogy a rendfenntartó erők hagyományos (értsd: halálos) fegyvereik alkalmazása nélkül legyenek képesek céljukat elérni.

A fegyverekből kilőtt lövedék sebessége (ezáltal mozgási energiája) a röppályán nem állandó. A csőtorkolat előtt közvetlenül mérhető sebesség a távolság növekedésével a légellenállásnak köszönhetően fokozatosan csökken. A röppályán a sebességcsökkenés nagyban függ a lövedék geometriai kialakításától is.

Ezeknek a fegyvereknek számos előnyük mellett, van egy alapvető problémájuk. Nem igazán az a probléma velük, hogy adott távolságon túl a lövedékek célban kifejtett hatása már jelentéktelen, azaz a célra szinte semmilyen hatással és főleg megállító hatással nem rendelkeznek. Sokkal nagyobb gondot jelent e fegyverek tekintetében, hogy a csőtorkolat

közelében a lövedék mozgási energiája még túlságosan is nagy lehet ahhoz, hogy a célszemélynek komoly, esetleg halálos sérülést is okozzon. Ez a „halálos hatás” pedig összeegyeztethetetlen a nem halálos fegyverek jellegével. Ezeket a fegyvereket ugyanis pontosan azzal a céllal hozták létre, hogy a lehetőleg ne, vagy a lehető legkisebb valószínűséggel okozzanak halálos kimenetelű sérüléseket.



2. ábra. Különféle nem áthatoló lövedékek mozgási energiájának alakulása a távolság függvényében [3].

A 2. ábra három nem áthatoló lövedék röppályán mérhető mozgási energiaváltozását mutatja a lőtávolság függvényében. Az ábrából megállapítható, hogy a mozgási energiája a négyzet (kocka) alakú babzsák lövedéknek csökken a legdrasztikusabban a röppályán. Ez azért rossz, mert a lövedék viszonylag hamar – azaz rövid távolságon – eléri azt az energia értéket, amelynél a becsapódó babzsák lövedék, már szinte semmilyen hatással nincs a célszemélyre. Ebből a szempontból sokkal kedvezőbb a helyzet a pontozott vonallal jelzett habszivacs gránát esetében. Ennél a lövedék típusnál a mozgási energia esése a röppályán nem olyan meredek, mint az előző esetben. Az amerikai Defence Technology Federal Laboratories, Inc. által kiadott anyag [3] szerint hatásosnak1 tekinthető az a lövedék, amelynek mozgási energiája a célba való becsapódáskor 115-145 J között van. Ezen érték fölött a lövedék, akár halálos kimenetelű sérülést is okozhat, ezen érték alatt pedig hatásossága meglehetősen csekély, főleg ha a célszemély vastag ruházatot visel.

A 2. ábra alapján a kocka alakú babzsák lövedék hatásos mozgási energia tartománya 6-13 m, az üstökös alakúé 5-19 m, míg a habszivacs gránáté 3-24 m közzé esik.

Nem nehéz belátni, hogy a választható lövedékek közül azt kell előnybe részesíteni, amelynek egyrészt a hatásos lőtávolsága2 másrészt, a hatásos mozgási energia tartománya a legnagyobb. Ezen nem halálos fegyvereknél tehát elvárás, hogy a hatásos lőtávolsága és a hatásos energia tartománya a lehető legnagyobb legyen.

Nos, kétségtelen tény, hogy az előzőek egy igen komoly problémát is felvetnek e fegyverekkel kapcsolatban. Ha belegondoljunk abba, hogy egy bevetés során a rendfenntartó erő nem ritkán kerül olyan stresszes helyzetbe, amikor a másodperc tört része alatt kell értékelnie a kialakult helyzetet, és ezt követően a lehető leggyorsabban, szabály- és előírásszerűen kell reagálnia. A megfelelő reagálásba természetesen az is beletartozik, hogy használnia kell fegyverét – legyen az akár a halálos vagy éppen a nem halálos.

[1] A lövedék képes a szemben álló fél megállítására, harc- vagy cselekvésképtelenné tételére.
[2] Az a távolság, amelyen még képes a szemben álló fél megállítására, harc- vagy cselekvésképtelenné tételére.

Nem nehéz belátni, hogy egy ilyen – nem egy esetben több szempontból is túlfűtött – helyzetben arra is figyelemmel lenni, hogy a célszemély történetesen 6 méteren belül van-e vagy sem, vagy már 13 méteren kívül helyezkedik el, igen komoly kihívást jelenthet az alkalmazóra nézve. Mert ugye első esetben még ne használjuk a fegyvert, mert akár halálos sérülést is okozhatunk, második esetben pedig már nem érdemes használni, mert hatástalan. Ha ehhez hozzá vesszük a kialakult helyzet esetleges dinamikáját – pl. ha célszemély fut felénk vagy gyorsan távolodik tőlünk – akkor szinte lehetetlen, hogy ezeket a távolságokat helyesen felmérjük és a fegyvert a hatásos energia tartományon belül tudjuk alkalmazni.

A FEJLESZTÉS KEZDETE, MEGFOGALMAZOTT KÖVETELMÉNYEK

Mint arra már rámutattam, ezen fegyvereknél tehát az alapproblémát az jelenti, hogy a fegyverhez közel kerülő célszemély akár halálos kimenetelű sérülést is szenvedhet, míg nagyobb távolságon alkalmazásuk akár teljesen hatástalan is lehet. A felhasználó számára az lenne az optimális megoldás, ha a lövedék mozgási energiája a röppálya minden egyes pontján állandó, vagy közel állandó lenne, és ennek az energia értéknek olyan mértékűnek kellene lennie, hogy a célszemélyt ideiglenesen harc-, vagy cselekvésképtelenné tudja tenni, vagy legalábbis legyen képes megállítani, esetleg eredeti szándékától eltéríteni úgy, hogy ne okozzon halálos kimenetelű sérülést.

A fenti probléma megoldására az olasz Védelmi Minisztérium 2001-ben a Jövő Katonája fejlesztési program, Nem Halálos Képességek alprogramja keretében közös kutatás-fejlesztési együttműködést kötött a Fabbrica d'Armi Pietro Beretta S.p.A céggel. A közel ötszáz éves tervezési és gyártási tapasztalattal rendelkező Beretta cég mérnökei egy újszerűnek tűnő megoldást találtak a fent leírt probléma kiküszöbölésére és kifejlesztették az egylövetű BERETTA LTLX 7000 fegyvert.

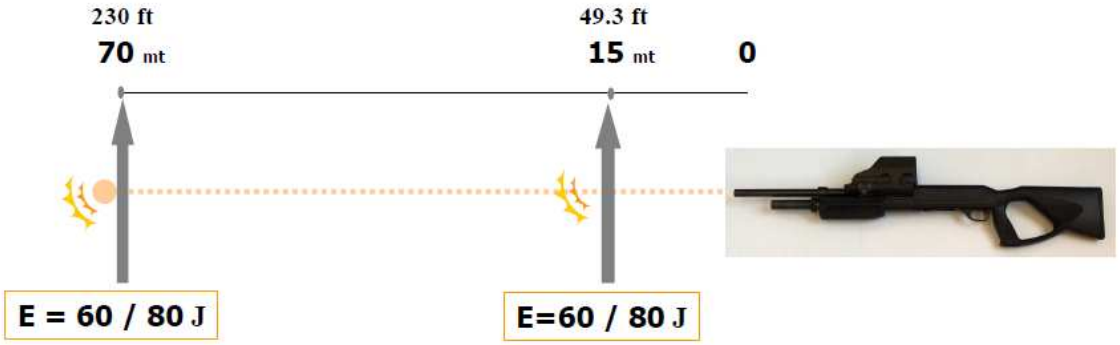
A megalkotott konstrukció természetesen nem tudja azt biztosítani, hogy a lövedék a röppálya minden egyes pontján ugyan olyan mozgási energiával rendelkezzen, hiszen ez fizikailag lehetetlen. A cég mérnökei nem is ezt célozták meg a fejlesztési koncepciójukban, hanem azt tűzték ki célul, hogy olyan eszközt fejlesszenek ki, amely lövedékének becsapódási energiája – adott távolságtartományon belül – a célba való becsapódáskor közel állandó legyen, függetlenül a cél adott tartományon belüli tényleges távolságától (3. ábra). Tekintettel arra, hogy a fegyver elsősorban a béketámogató műveletekben résztvevő katonák számára fejlesztették ki, ezért ezt a távolságtartományt 15÷70 méter között határozták meg.

A követelmények között szerepelt még továbbá, hogy:

- a könnyebb kiképzés érdekében a fegyver kialakításában és ergonómiailag hasonló legyen, mint a már hasonló feladatokra alkalmazott 12-es sörétes fegyver[3];
- az alkalmazott nem áthatoló lövedék trauma hatása legyen képes a célszemély megállítására, ideiglenes harc-, vagy cselekvésképtelenné tételére, eredeti szándékától való eltérítésre;
- a fegyver hagyományos elemekből felépülő lőszert alkalmazzon;
- rendelkezzen a céltávolság becslésére alkalmas optikai irányzékkal;
- a lövedékek becsapódási energiájának 15 és 70 méter között, a cél távolságától függetlenül 60-80J között kell lennie.
- a magassági (H) és szélességi (SZ) szórás összege maximum 1000 mm lehet 70 méteren[4]

[3] Amely alkalmas volt gumi-, és babzsák lövedékek kilövésére

[4] H+L=1000 mm, amit úgy is lehet értelmezni, hogy a lövedékeknek 70 méteren egy 50x50 cm-es területen belül kell becsapódniuk.



3. ábra. Az alkalmazott alapelv [4]

A becsapódási energia megegyezik a lövedék célba való becsapódásakor mérhető (vagy inkább csak számítható) mozgási energiával.

Ennek megfelelően az $E_{becsap} = \frac{1}{2}mv^2$ összefüggésből kiindulva (ahol az *m,* a lövedék tömege, a *v* pedig a lövedék becsapódáskor mérhető/számítható sebessége) az alábbiak állapíthatóak meg. Miután a lövedék tömege a röppályán állandó, ezért a kitűzött cél csak úgy valósítható meg, ha azt lehet biztosítani, hogy bármely távolságon történő becsapódás esetén a becsapódási sebesség olyan mértékű, hogy a becsapódási energia a fent leírtaknak megfelelően alakuljon. Azaz a megoldás kulcsát a lövedék kezdősebességének megfelelő mértékű megválasztásában kell keresni.

LTLX 7000 SZERKEZETI KIALAKÍTÁSA

Az LTLX 7000 fegyver, mint rendszer három fő részből épül fel. Magából a fegyverből, mint indító szerkezetből, a távolságbecslésre alkalmas holografikus optikai irányzékból, valamint a lőszerből (4. ábra).

4. ábra. LTLX7000 fegyver és lövedéke [4]

A fegyverhez alkalmazott lőszer, az indító tölteten kívül, egy kb. 16-18 gramm tömegű nem áthatoló lövedéket tartalmaz, amelyet a röppályán forgással stabilizálnak. Az alumínium hüvelyben elhelyezkedő lövedék két részből áll. A plasztikus anyagból készült fejrész, amely a becsapódás során deformálódik és biztosítja, hogy a lövedék ne hatoljon be a célba. Plasztikussága révén a lövedék fejrésze a becsapódási pontban az eredeti átmérőjéhez viszonyítva nagyobb felületen adja át a mozgási energiáját. A lövedék fejrésze egy kemény műanyagból készült hengeres részbe integrálódik. A kemény műanyag részen kialakított

nagyobb átmérőjű perem biztosítja a lövedék megforgatását a fegyver huzagolt csövében (4. ábra – 3-4. képei).

A kialakított modellnél megállapítható, hogy a lövést követően, a lövedék sebességének röppályán való módosítására a kezelőnek már nincs lehetősége, illetve, hogy az indítótöltetben levő lőpor mennyisége – azaz a keletkezett lőporgázok mennyisége – pedig állandó. Ezek figyelembevételével a megoldást a tervezők következőkben látták. A megfelelő kezdősebességet az határozza meg, hogy a felszabaduló lőporgázok mennyiségének mekkora hányada kerül felhasználásra a lövedék gyorsítására[5]. A keletkezett lőporgázok fel nem használt részét pedig szabályozott módon a szabadba engedik. Könnyű belátni, hogy adott lövedék 70 m-re való célba juttatására sokkal nagyobb kezdősebesség (lőporgáz nyomás) szükséges, mint ugyanannak a lövedéknek 15 m-re való eljuttatására.

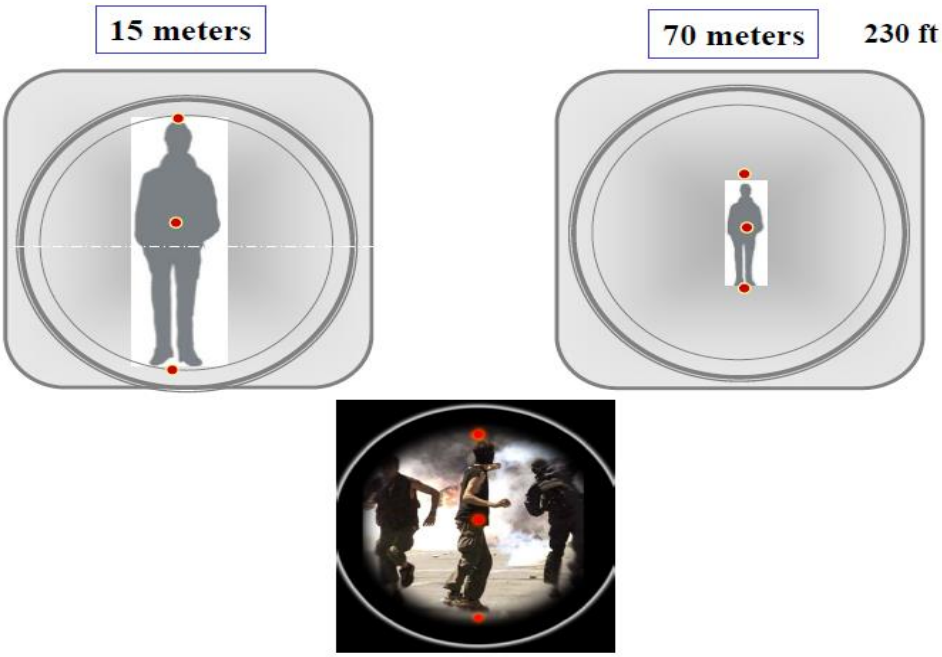
A fenti cél elérése érdekében a fegyver csövén egy kifúvónyílást alakítottak ki, amely lehetővé tette a „felesleges" lőporgázok csőből való szabályozott elvezetését. A kifúvónyílás keresztmetszetét egy másik alkatrész rácsúsztatásával tudták változtatni a két szélső helyzet között[6], Ezzel szabályozva, hogy a keletkezett lőporgázok hány százaléka kerüljön a szabadba.

A lövedék kezdősebessége tehát attól függ, hogy a keletkezett lőporgázok hány százalékát használják fel a lövedék gyorsítására. Minél inkább el van zárva a kifúvónyílás annál több lőporgáz kerül felhasználásra a lövedék gyorsítására és ezáltal nagyobb lesz a lövedék kezdősebessége. És fordítva, minél inkább nyitott a kifúvónyílás keresztmetszete, annál inkább kevesebb lőporgázt használnak fel a lövedéket gyorsítására – hiszen ekkor több lőporgáz távozik a rendszerből felhasználatlanul – ezáltal a lövedék kezdősebessége (és végső soron a mozgási energiája) is kisebb lesz. A követelményként megfogalmazott 60÷80 J becsapódási energia 70 méteres lőtávolságot feltételezve kb. 105 m/s-os, míg 15 méteren pedig 95 m/s-os kezdősebességet jelent.

Ahhoz viszont, hogy számítható legyen a lövedék szükséges kezdősebessége ismerni kell a cél távolságát. A cél távolságának gyors és pontos lemérésére a lézeres távolságmérők adnák a kézenfekvő megoldást. Hogy a tervezők mégis, miért nem ezt a megoldást választottak, annak alkalmazástechnikai és gazdasági okai is vannak. Egyrészt a megkívánt becsapódási energia sem pontos érték, hanem egy 60÷80 J közötti tartomány, ezért nem szükséges centiméter pontosan megmérni a cél távolságát sem. Ráadásul a fegyver tervezett alkalmazása során elsősorban mozgó célokkal kell döntően számolni, mintsem álló céllal. Azaz elegendő a cél távolságának centiméter pontos mérése helyett, csupán adott határon belüli becslést biztosítani. Másik ok volt, hogy egy lézeres távolságmérő beszerzési költsége nagyobb, áramforrás igénye pedig további logisztikai problémákat is felvet.

A fegyverhez kifejlesztett, speciális ballisztikai számításokra is képes holografikus irányzék lehetővé teszi a kezelő számára a viszonylag gyors távolságbecslést. Az irányzék bal oldalán elhelyezett kezelőgombok segítségével a kezelő képes az irányzék látómezejének két vörös pontját magasságban beállítani. A vörös pontok megfelelő beállítása viszont igen komoly kiképzettséget és főleg gyorsaságot igényel, hiszen lehet, hogy a távolságbecslés végrehajtásával egy időben szinte azonnal ki is kell váltani a lövést. Ellenkező esetben – mozgó célt feltételezve –, a cél közelíthet a lövő felé vagy távolodhat tőle, ami ugye egy ismételt távolságbecslést vonhat maga után.

[5] A felhasznált hányad pedig természetesen a céltávolság függvénye.
[6] Teljesen zárt vagy teljesen nyitott állapot.



5. ábra. Az irányzék látómezeje, a távolságbecslésre alkalmazott vörös pontokkal [4]

A kezelőnek, nem kell mást tennie, minthogy az alsó pontot a célszemély talpához, míg a felső pontot a cél fejének felső részére illeszteni. Könnyű belátni, minél közelebb van a cél annál nagyobb a két pont közötti távolság, a céltávolság növekedésével pedig a két pont közötti távolság fokozatosan csökken. Miután a két vörös pont közötti távolság értéke arányos a cél távolságával, ezért a vörös pontok állításával egy időben a távolságbecslés is megvalósul. A távolságbecsléssel egy időben – a becsült távolság értéknek megfelelően – a csövön lévő kifúvónyílása is automatikusan, a kívánt mértéknek megfelelően lezárásra vagy kinyitásra kerül.

A fejlesztés során egy másik problémát is meg kellett oldaniuk a fejlesztőknek. Nevezetesen a célszemély magasságának a problémáját. Jogosan tehető fel ugyanis a kérdés, hogy milyen magas célra van az irányzék távolságbecslő része beprogramozva. Miután az emberek magassága földrészenként, vagy régiónként is eltérő lehet, ezért ez koránt sem elhanyagolható részletkérdés[7]. Ezen probléma kiküszöbölésére a holografikus irányzék ballisztikai számításokért felelős egységét programozhatóvá tették. Ezáltal viszonylag rövid időn belül lehetségessé vált az egyes régiókban élő emberek magasságának megfelelően az eszközt beprogramozni.

A FEJLESZTÉS UTÓÉLETE, AVAGY A LASSÚ AGÓNIA KEZDETE?

A lassan 15 éve kezdődött fejlesztésnél alapvető cél volt, hogy bővítsék a béketámogató műveletekben résztvevő olasz katonai erő által alkalmazható nem halálos fegyverek körét, ezáltal is árnyaltabb válaszadást biztosítva számukra egy esetleges konfrontáció esetén. A prototípus kifejlesztésére a szerződést 2002-ben írta alá az olasz Védelmi Minisztérium a Fabbrica d'Armi Pietro Beretta S.p.A céggel. A fejlesztés eredményeként az első három prototípus példány 2006-ban készült el, amelyeket a Védelmi Minisztérium a sikeres vizsgálatokat követően elfogadott. A fegyverrel a csapatgyakorlatot 2007-ben hajtották végre, majd ezt követően 2008-ban – korlátozott darabszámban – a műveleti területen résztvevő csapatok is tesztelhették. Már a fejlesztés szakaszában a cég számos nemzetközi rendezvényen bemutatta az eszközt, mint egy igen perspektivikusnak ítélt nem halálos fegyvert. Tény és való,

[7] Európában az 1,7 m magas céllal lehet számolni.

hogy ezek a bemutatók döntően csak Powerpointos-prezentáció szintjén valósultak meg. Ezt követően viszont nem nagyon lehetet hallani a fegyverről.

Nem igen mondható sikeresnek az a fejlesztés, amelynél a kifejlesztett eszközzel való ellátása a csapatoknak, még a fejlesztés kezdetét követő tízedik évet követőn sem kezdődik meg.

Lehetne keresni az okokat vagy találgatásokba bocsátkozni, hogy miért állt le megint egy ígéretesnek induló fejlesztés a nem halálos fegyverek területén. Erről nem igen találunk sehol sem hiteles és valós magyarázatot. Sikertelen fejlesztésekről – érthetően – senki sem beszél szívesen, és főleg nem a nagy nyilvánosság előtt. A nem halálos fegyverek területén sajnos több olyan sikeresnek tűnő fejlesztést is lehetne példaként említeni, amely valamilyen okból kifolyólag lassan a felejtés mocsarában süllyedt. A lehetséges okokra vonatkozóan már 2012-ben tettem kísérletet a Hadmérnök oldalain [6]. A megjelent cikkben foglaltakon túlmenően jelen esetben a fegyver iránti nem kellő mértékű érdeklődésben közrejátszhat az is, hogy azok a béketámogató műveletek ahol ezen fegyvernek szerepet szántak, nem nélkülözik a dinamikát. Azaz igen kicsi annak a valószínűsége, hogy a csapatok álló céllal találkozzanak, hacsak valamilyen barikádharcot nem tételezünk fel. Sokkal inkább elképzelhető a futó, vagy a viszonylag gyors helyzetváltoztatásra képes célok megjelenése, aminél ugye a távolságbecslés megvalósítása és a lövés azonnali kiváltása szinte lehetetlen. A gyors egymást követő lövést pedig a fegyver egylövetű jellege nem teszi lehetővé. Arról nem is beszélve, hogy a fegyver használata fokozottabb elővigyázatosságot igényel, ha a célszemélyek és a polgári lakosság vegyesen van jelen.

Nehéz elfogadni, de nagyon úgy tűnik, hogy itt megint egy ígéretesnek induló fejlesztés lassú, de biztos agóniájának vagyunk szemtanúi.

Felhasznált irodalom

[1] P. Raffaelli: A Concept proposal from Beretta - 3nd European Symposium on Non-Lethal Weapons May 10-12, 2005 – Ettlingen

[2] Bartha Tibor: Nem halálos fegyverek (Egyetemi E-jegyzet) – Zrínyi Miklós Nemzetvédelmi Egyetem – Budapest, 2009

[3] 40 mm Exact Impact és az életre kevésbé veszélyes speciális lőszerek (SIM) - A Magyar Rendőrség és a Fegyveres Szervek részére tartott szakmai bemutató anyaga – Budapest, 2006

[4] Less Than Lethal Concept – http://www.dtic.mil/ndia/2008Intl/BerettaandDeftech.pdf (letöltés: 2012. december 10.)

[5] Beretta LTLX7000 shotgun http://www.thefirearmblog.com/blog/2009/04/06/beretta-ltlx7000-shotgun/- (letöltés: 2009. május 5.)

[6] Bartha Tibor: Nem halálos fegyverek integrációjának helyzete a NATO-ban – Hadmérnök, 2012. december (VII. évfolyam 4. szám.)

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Gávay György - Gyarmati József - Kalácska Gábor-
Sebők István - Szakál Zoltán
gavay.gyorgy@uni-nke.hu

LÖVEDÉK PÁNCÉLLEMEZEN TÖRTÉNŐ ÁTHALADÁS METALLOGRÁFIAI VIZSGÁLATA

Absztrakt

A cikk lövedékkel roncsolt páncéllemezek metallográfiai vizsgálatát mutatja be. A kutatás során különböző típusú és különböző sebességű lövedékkel roncsolt szintén különböző anyagösszetételű acél és páncéllemezek kristályszerkezetében történő változások lettek vizsgálva. Az egyes lemezek védelmi képességéről, hiteles méréseken alapuló eredmények születtek.

This paper shows a metallographic test of different plates which were hit by bullets. During the research the changes of crystal structure of different kind of steel was examined using different types of bullets. The other important aim of the research was to define the defense capabilities of the different plates and armors based on authentic measurement.

***Kulcszavak**: védelmi képesség, páncél, anyagvizsgálat ~ defense capabilities, armor, material testing*

1. BEVEZETÉS

A Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Katonai Logisztikai Intézet, Haditechnikai Tanszék és a Szent István Egyetem Gépészmérnöki Kar, Gépipari Technológiai Intézete közös kutatást indított, amely a lövedékkel roncsolt páncéllemezek vizsgálatát tűzte ki fő célul [1]. A témával a kutatóműhely sikeresen pályázott a Nemzeti Közszolgálati Egyetem rektora által kiírt „Egyetemi Kutatóműhely támogatása" című pályázatra, amely így a kutatás anyagi fedezetét biztosította.

A kutatás kiindulópontja volt, hogy a lövedék által roncsolt lemez metallográfiai vizsgálatával hazai és a nyilvános külföldi irodalom nem foglalkozik. Rendelkezésre állnak szabványok, de ezek csak a lövedékálló védőmellények védelmi képességének az ellenőrzésével foglalkoznak. [2] [3] Ezen szabványok lényegében csak a vizsgálati körülmények leírását valamint a mérési eredmények értékelését írják elő. Nincs viszont semmi olyan hazai kutatás vagy kifejlesztett eljárás, amely a lövedékkel roncsolt anyagokban történő változások leírásával és ezáltal a védőképességük változásának meghatározásával foglalkozna. Ennek megfelelően nincs semmi olyan hazai és MH által elérhető eljárás, amely a fémes és nemfémes páncélzat védőképességének az időbeni változásával foglalkozik.

Az elmúlt évtized háborúi, amelyekben a Magyar Honvédség is rész vett, a védelmi képességek fokozására vonatkozó igény megfigyelhető volt mind hazai mind pedig a szövetséges haderők részéről. A felhasználói igény valamint annak szinte folyamatos növekedése indokolta számunkra a hazai felhasználó és kutató számára nem kellőképpen ismert illetve el nem érthető terület tudományos igényű kutatását.

2. KUTATÁSI CÉLOK

A kutatás során az alapvető célkitűzésünk fémes anyag lövedékkel történő átütési folyamatának leírása volt. Ezen belül meghatározó volt a roncsolt lemezek kristályszerkezetében történő változások azonosítása. A munkamegosztás a két intézmény között a rendelkezésre álló anyagi és humán erőforrás alapján történt. A NKE HHK a metallográfiai vizsgáló laboratóriumában vizsgálatok elvégzéséhez szükséges csiszolatok legyártását, valamint kísérleti lövészetek megszervezését végezte. A minták elemzését és az ide vonatkozó következtetések levonását a Szent István Egyetem kutatói végezték.

A kutatási célok részletesen a következők voltak:

- a fémkristályokban bekövetkező változások leírása;
- a hatászóna megállapítása;
- horpasztás esetén a deformáció és az szerkezeti változás alapján a védőképesség csökkenésének megállapítása;
- egyes a Magyar Honvédség által használt páncélok védelmi képességének megállapítása;
- egyes a Magyar Honvédségben használt töltények hatásadatainak megállapítása.

A fenti lista utolsó két kutatási célja mintegy kiegészítő célként és ennek megfelelően kiegészítő eredményként jelent meg. A kísérletekre két különböző típusú páncéllemez állt rendelkezésre. Az első a Magyar Honvédság által is használt páncél, ez a továbbiakban „A" páncélként kerül megnevezésre. A második pedig egy korszerű páncél, amely „B" lemezként kerül megnevezésre. Az „A" páncél 8 mm vastagságú, a „B" páncél pedig 6,5 mm vastagságú volt.

Referenciaanyagként egy kereskedelmi forgalomban kapható és minőségi tanúsítvánnyal rendelkező 8 mm vastagságú melegen hengerelt acéllemez lett kiválasztva.

A vizsgáló töltényeknek a Magyar Honvédségben rendszeresített puska és karabélytöltény lágyacél magvas és páncéltörő változata lett kiválasztva.

A vizsgálatba bevont lőszerek:

- 7,62×54R mm LPSZ;
- 7,62×54R mm B32;
- 7,62×39 mm BZ.

A páncéllemezek különböző sebességgel lettek meglőve. A becsapódási sebességek megtervezésekor a következő elveket lettek figyelembe véve:

1. Legyen átütés és legyen horpasztás.
2. A roncsolt lemezek legyenek összevethetők, vagyis a lehetőségek függvényében azonos eredménnyel legyenek a különböző lemezek azonos típusú és sebességű lövedékkel meglőve.
3. Részeredményként álljon rendelkezésre az a sebességtartomány, amely alatt nincs átütés, vagyis a lemez védelmet nyújt.

A rendelkezésre álló keret nyolc óra lőtérbérletet tett lehetővé, ezen felül korlátozott volt a rendelkezésre álló minta, ezért a kétfajta űrmérethez tartózó fegyverek, vagyis a géppuska illetve a gépkarabély lőtáblázata szerinti torkolati sebességével lett kezdve a lövészet és innen lett csökkentve mindaddig amíg, az átütés helyett már csak horpasztás történt.

A mérés hitelessége céljából minden lövés azonos lőszerrel és töltettel azonos lemezre három alkalommal lett elvégezve.

3. A KUTATÁS MENETE

A kutatás az alábbi pontokban leírtak szerint sorrendben és tartalommal történt.

Lövészet

A kísérleti lövészet végrehajtására a Polgári Kézilőfegyver és Lőszervizsgáló Kft. lőtere lett kibérelve. A kft. a lövészethez biztosította a lőszert az általunk előírt torkolati sebességnek megfelelő tömegű lőportöltettel szerelve. A lövészet ballisztikai mérőcsőből lett végrehajtva. A mérési helyszínét a 1. ábra mutatja.

a b c

1. ábra. A Kísérleti lövészet helyszíne[1]
a: befogott céltárgy; b: fénykapu; c: ballisztikai mérőcső irányzékkal

Mechanikai vizsgálatok

A referencialemez a kereskedelmi forgalomban kapható melegen hengerelt 8 mm vastagságú acéllemez volt, ehhez a szállító minőségi tanúsítványt adott, ezért itt a mechanikai vizsgálatok elvégzése nem volt szükséges.

[1] Helyszín Polgári Kézilőfegyver és Lőszervizsgáló Kft. Saját felvétel.

Az „A” lemez esetében az anyag tulajdonságainak a megállapításához a Szent István Egyetem Gépészmérnöki Kar Tudástranszfer központjában mechanikai vizsgálatok lettek elvégezve. A vizsgálatok során mért értékeket az 1. táblázat mutatja.

1. táblázat. Az „A” páncél mechanikai tulajdonságai [4]

	Rp0,2 [N/mm2]	Rm [N/mm2]	E [GPa]	HV30 [-]
Max	1361	1645	187	456
Min	1325	1564	176	401
Átlag	1335	1603	181	425

A további elemzésekhez szükséges volt a lövedék magjának keménysége, ezért a már kilőtt lövedékek magjain keménység lett mérve, az értékeket mutatja a 2. táblázat.

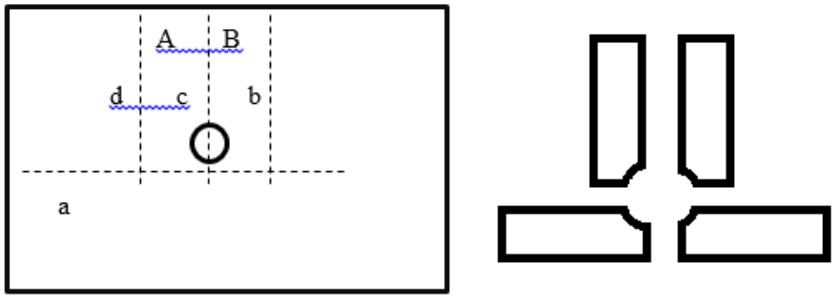
2. táblázat. A kísérletbe bevont lövedékmagok kilövés utáni keménysége HV30 (az LPSZ esetén a felkeményedett mellső rész adatai)

	7,62×54Rmm LPSZ	**7,62×54Rmm B32**	**7,62×39 mm BZ**
Max	225	938	976
Min	193	831	759
Átlag	203	905	885

A „B” lemez esetében az anyag olyan keménységgel rendelkezett, hogy sem az NKE HHK sem pedig a SZIE műhelyeiben a megmunkálása és a próbatest gyártása a megfelelő szerszám illetve technológia hiányában nem volt lehetséges, ezért a mechanikai vizsgálatok itt elmaradtak.

Lemezek előkészítése a mintagyártáshoz

A csiszolatok gyártásához a már meglőtt lemezeket elő kellett vágni olyan mértékben, hogy a további feldolgozáshoz alkalmas legyen. A vágási mintát mutatja az 2. ábra. A vágást, mivel a vágási felület közel esett a csiszolt és vizsgált felülethez, a kristályszerkezetben esetlegesen lezajló és a mintát befolyásoló szerkezeti változások elkerülése végett olyan feltétellel kellet elvégezni, hogy a hőmérséklet ne emelkedjen 200 °C fölé. Ennek megfelelően csak a gépi illetve kézi fűrészelés és az abrazív vízsugaras vágás jöhetett szóba. A referencialemez és az „A” páncél vágása az NKE HHK-n fűrészeléssel megoldható volt. A „B” páncél elővágása annak rendkívül magas keménysége miatt megrendelésre, vízsugaras vágással lett elvégezve.



2. ábra. A lemezek elővágása [4]

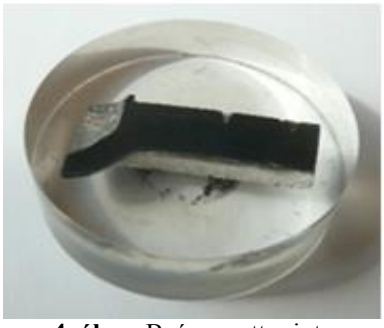
A vágás a 2. ábra „a”, „d” és „b” éle mellett történt, hogy a 2. ábra jobb oldalán levő mindarabok kialakítása lehetővé váljon. A kialakítás lehetővé tette, hogy a „c” él mentén és az arra merőleges „a” éllel párhuzamos felülettel a lemez hengerelési irányára és arra merőlegesen is elvégezhető legyen a vizsgálat.

Beágyazott minták gyártása

A minták a NKE HHK metallográfiai laboratóriumában lettek legyártva. A kutatás során 100 db beágyazott minta készült. A mintagyártás precíziós vágásból, beágyazásból és csiszolásból állt. A felhasznált berendezéseket mutatja a 3. ábra. A végterméket a már vizsgálható beágyazott mintát a 4. ábra mutatja.

a b c

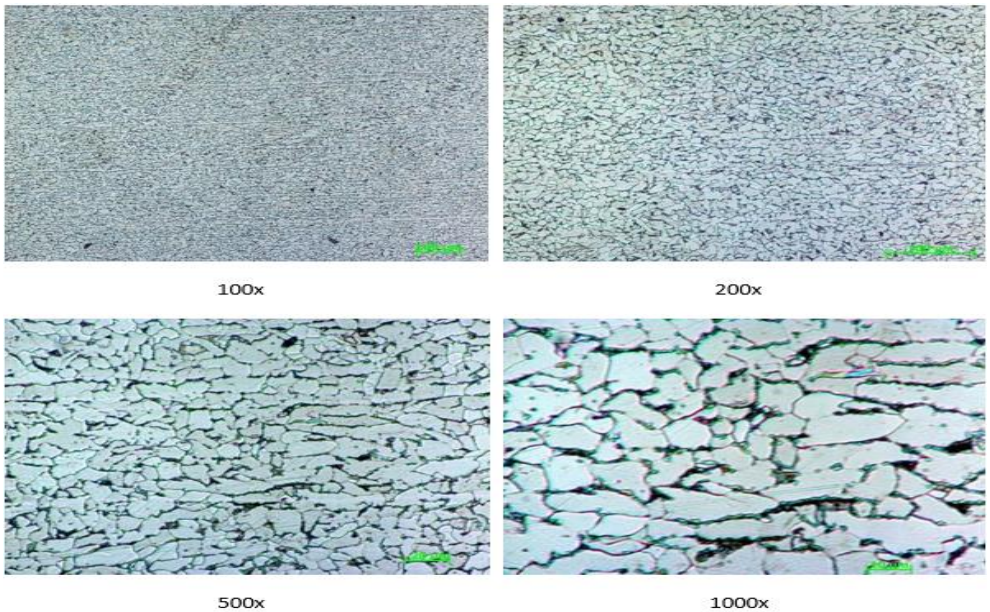
3. ábra. A mintagyártás
a: precíziós vágás; b: beágyazás; c: csiszolás



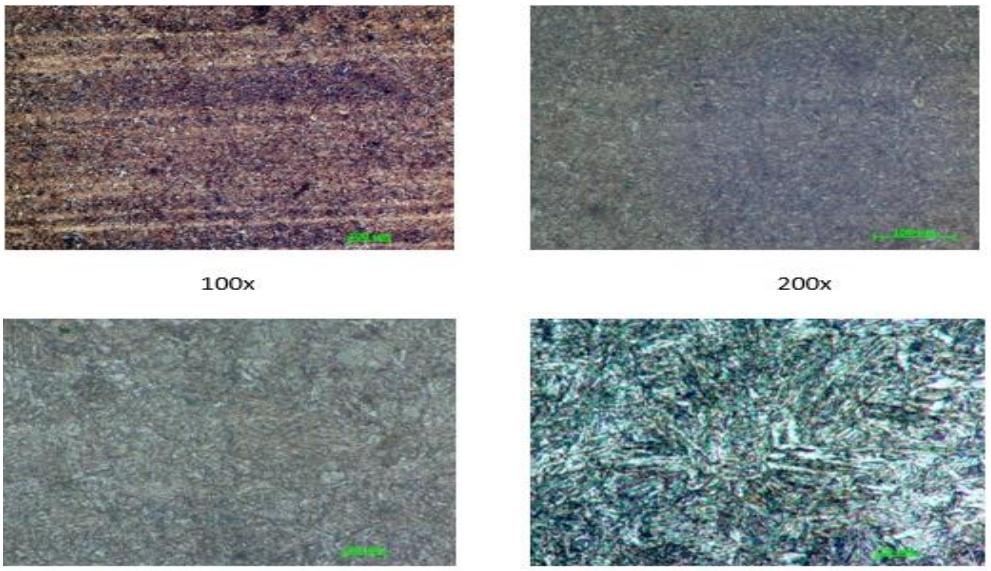
4. ábra. Beágyazott minta

A minták elemzése

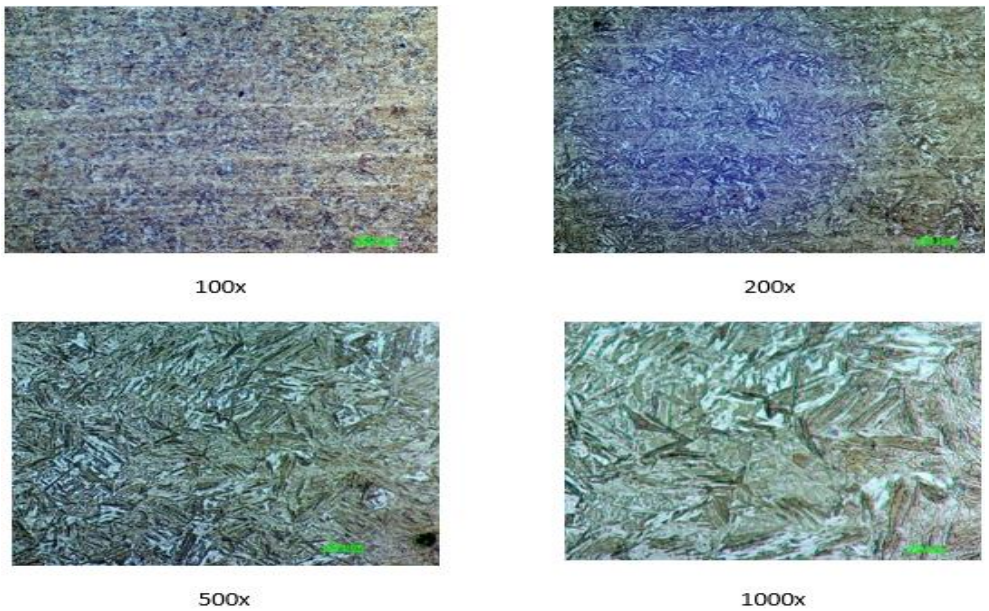
A minták elemzése a SZIE Gépészmérnöki karán lettek elemezve. A beágyazott mintákat maratás követően fémmikroszkóppal lettek vizsgálva. Az 5., a 6. és a 7. ábra a vizsgált anyagok nem roncsolt felületeinek különböző nagyítású képeit mutatják.



5. ábra. Referencia anyagból készült csiszolat mikroszkópi képe 100-1000x nagyításban [4]



6. ábra. Az „A” páncél csiszolatnak a mikroszkópi képe 100-1000x nagyításban [4]



7. ábra. A „B” páncél csiszolatának mikroszkópi képe 100-1000x nagyításban [4]

3. EREDMÉNYEK

A kutatómunka során sikerült egy, a szabványokat felhasználó, de annál részletesebb áthatolás-vizsgálati módszert kifejleszteni. Ez a módszer továbbfejleszthető, a célanyag repeszhatásának, valamint a szerkezeti torzulásának szimulációs vizsgálatára.

A lövedékek becsapódásának vizsgálatakor megállapítást nyert a két páncél anyag védelmi képessége a gyalogság ellen alkalmazott 7,62 x 54R mm LPSZ lőszer lágyacél-magvas lövedéke ellen, mivel lőtávolságtól függetlenül egyetlen esetben sem történt áthatolás. Tehát mindkét páncéllemez teljes védelmet nyújt a lágyacél-magvas lövedékekkel szemben.

A lövészet során fénykapu segítségével a lövedék sebesség lett mérve. Mivel ezen értékek nehezebben értelmezhetők, ezért a [5] és a [6] irodalmakban található lőtáblázatok alapján a sebességértékekhez a jobb érthetőség érdekében hozzávetőleges lőtávolságok lettek megadva.

A tesztlövészet során sikerült olyan lőtávolságokat szimulálni páncéltörő 7,62 x 39mm BZ gépkarabély lőszerrel, amelyek esetében az adott lövedék a célanyagban megakadt. Ez az „A”

páncél esetében 100 méteres lőtávolságnak megfelelő sebességű lövedék esetében volt. Ekkor lövedék energiája a páncélanyag a folyáshatára és a szakítószilárdsága közötti tartományhoz szükséges erőhatást generált. Tehát ez a páncél 100 méteres lőtávolságon felül nyújt csak védelmet a 7,62 x 39 mm BZ lövedék ellen.

A „B" páncél esetén a vizsgált lőtávolságok és különböző lövedékmagok alkalmazásával sehol sem akadt meg a lőszer. A lágyacél-magvas lövedékek esetében torkolati szinten sem volt átütés, míg a páncéltörő lövedékek torkolati szinten teljes átütést produkáltak minden alkalommal, így nem sikerült egyértelműen feltárni, hogy hol van az adott lőszer esetén az a határ távolság, amely felett már védettség van. A későbbiekben a lőtávolságok kisebb léptékű felosztásával valószínűleg megállapítható lenne ezen anyag esetén is az az energiájú lövés, amely esetén éppen átszakad a lemez, de a lövedék meg nem hatol át. Az BZ lövedék 100 m-es lőtávolságnak megfelelő sebesség esetében teljes átütést produkált, ha ezt összevetjük az „A" páncéllal, ahol hasonló sebességű három lövedékből kettő fennakadt és egy ütötte csak át, akkor úgy tűnhet, hogy az „A" páncél nagyobb védőképességgel rendelkezik. Viszont figyelembe kell venni, hogy a „B" páncél 1,5 mm-el vékonyabb, és a kettő védelmi képességének az egyértelmű összevetéséhez (amennyiben ez szükséges) statisztikailag is értelmezhető lövésszámra van szükség. A „B" páncél tehát az LPSZ lövedék ellen teljes védelmet nyújt, de egyik páncéltörő lövedékek ellen sem nyújt védelmet 100 m-es lőtávolságon belül.

A lemezek védőképességét összegezve a páncélok teljes védelmet nyújtanak a lágyacélmagvas lövedékű és legfeljebb 7,62 mm űrméretű csőhöz tartozó lövedékekkel szemben. Az MH által is használ „A" páncél csak mintegy 100 m lőtávolság felett nyújt védelmet az ugyancsak 7,62mm-es lövészfegyverek páncéltörő lövedékeivel szemben. Itt még egyszer meg kell jegyezni, hogy ez a kutatásnak csak egy részeredménye, a pontos lőtávolságok megállapításához további lövészetre van szükség.

Az „A" páncél anyag a horpasztással járó lövés esetén (7,62 x 54R mm LPSZ lőszer lövedéke torkolati sebességgel) a becsapódáskor roncsolt felülethez közel, maximum 1 mm-es távolságban deformálódik. A horpadás mélysége, illetve a lemez hátoldali felületén kialakult domború felület magassága a legkisebb lőtávolságon a legnagyobb, de ez esetben sem éri el a 0,1 mm-t. A páncéllemez felületén keletkezett zömült rétegen kívül jelentős anyagszerkezeti változás nem következik be. A deformációs zónában a hengerlési szálak torzulnak, azonban a zónán kívül az anyag szerkezete sértetlen. A lemez által nyújtott védelmi képesség egy lövés esetén a lövedék becsapódásának helyén, és annak közvetlen környezetében nem változik. A lemez által lövedék áthatolás nélkül elviselhető lövések száma ugyanazon a helyen, vagy adott távolságon belül további vizsgálatok tárgyát képezi. Az „A" páncéllemezen, a 7,62 x 39 mm BZ lőszerrel végzett kísérletek során, a 100m-es lőtávolságon lehetett olyan eredményt felmutatni, ami alapján valószínűsíthető a védelmi képesség egyik határa. Ennek jelentősége, hogy milyen lőszer ellen, milyen távolságból nyújt védelmet egy harcjármű.

A lőszerek alkalmazásának szempontjából egyértelművé vált, hogy az „A" páncéllemez védelmi képességével szemben az 7,62 x 54R LPSZ lőszer lövedéke még torkolat sebesség esetén is teljesen hatástalan. A lemezen okozott deformáció a védelmi képesség csökkentésének szempontjából nem jelentős. Ennek mértékének pontos meghatározása további vizsgálatokat igényel. A kidolgozott módszer lehetőséget ad a páncéltörő lőszerek hatásos, átütést biztosító lőtávolságának megállapítására. Ez a 7,62 x 39 mm BZ lőszer esetében 100 m-es lőtávolság körüli érték. A lehető legpontosabb hatásos lőtávolság meghatározása szintén további vizsgálatokat igényel.

A „B" páncél anyagnál ugyanezen esetben (ugyanakkora energiájú becsapódás mellett) nem csak a felület közelében deformálódik az anyag, hanem „gumiszalag" módjára megnyúlik az anyag teljes keresztmetszete, így az a lövés hátoldalán is jól látható nyomot hagy. Repedések, amelyek repeszhatás okozhatnak, egyik esetben sem keletkeznek, azonban a „B" páncél anyagon 7,62 x 54R mm LPSZ lőszer, 10 m távolságú lövés esetében a horpasztási zóna szélénél

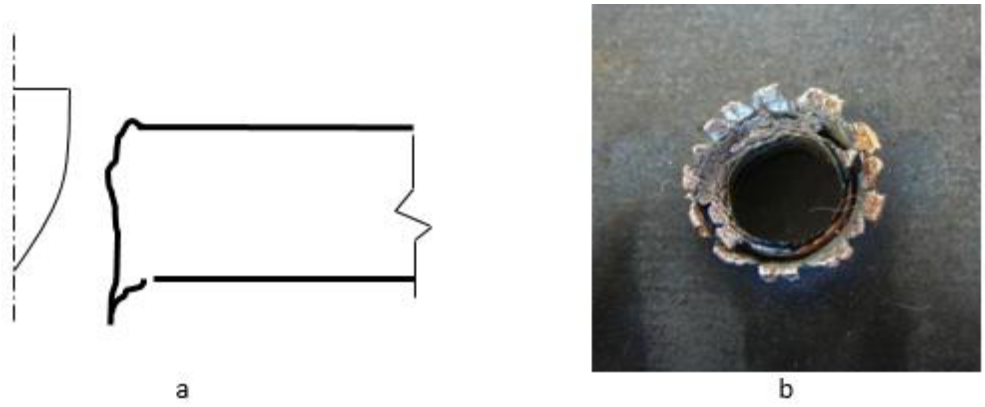
repedések jelennek meg az anyag belseje felé. Ebből új kutatási cél fogalmazható meg miszerint: Milyen mértékben kell növelni az energiasűrűséget, hogy a páncéllemeznél lényegesen kisebb keménységű lövedék megrepessze és átüsse a lemezt?

A tesztlövészetet követően - a korábban leírt módon - a roncsolt célanyagokból mikroszkópos vizsgálatok elvégzésére alkalmas csiszolatok lettek készítetve. Az elkészített csiszolatok elemzése során a roncsolt célanyagokat a deformációk alapján három különböző csoportra lehetett felosztani:

- a vizsgálati körülmény hatására szívósan viselkedik az anyag (van áthatolás);
- a vizsgálati körülmény hatására ridegen viselkedik az anyag (van áthatolás);
- horpasztás (nincs áthatolás).

Az áthatolással járó csoportokba tartozó sérülések más jellegűek, de megállapítható, hogy az anyagszerkezeti változások deformációs zónájának határa egyik esetben sem több mint 2 mm a sérülés peremétől mérve, a páncéltörő lövedék magjának középpontjától (a találat középpontjától) mérve 5 mm. A sérülések minősége azonban a lőtávolságok, az alkalmazott lövedékek, illetve a céltárgyak minőségének függvényében eltért. Azonos lőszer, azonos célanyag, de különböző lőtávolság esetében megfigyelhető az anyagszerkezeti változások mértékének eltérése.

A csiszolatok alapján, megállapítható, hogy lágy referenciának használt anyag áthatolásos lövése esetén az alkalmazott lőszertípusok esetén, abban nem keletkeznek repedések a lövedék okozta lyuk környezetében, így repeszhatással nem, vagy csak csekély mértékben kell számolni. A lövedék okozta deformációs sebesség az áthatolás egyetlen szakaszában sem haladja meg az anyagra jellemző kritikus értéket, amely hatására ridegtörés következne be. A lövedék behatolás pillanatában a lemez és lőszer találkozása során egy kráteres felgyűrődés keletkezik, majd a lövedék behatolása során tolja maga előtt az anyagot, amelyben a megnövekedett terhelés hatására az anyag folyáshatárát meghaladó feszültség keletkezik. A lőszer áthaladása során valószínűleg nem tolt ki maga előtt jelentős anyagot, hanem azt a környezetébe deformálta. Az áthatolást a 8. ábra mutatja.

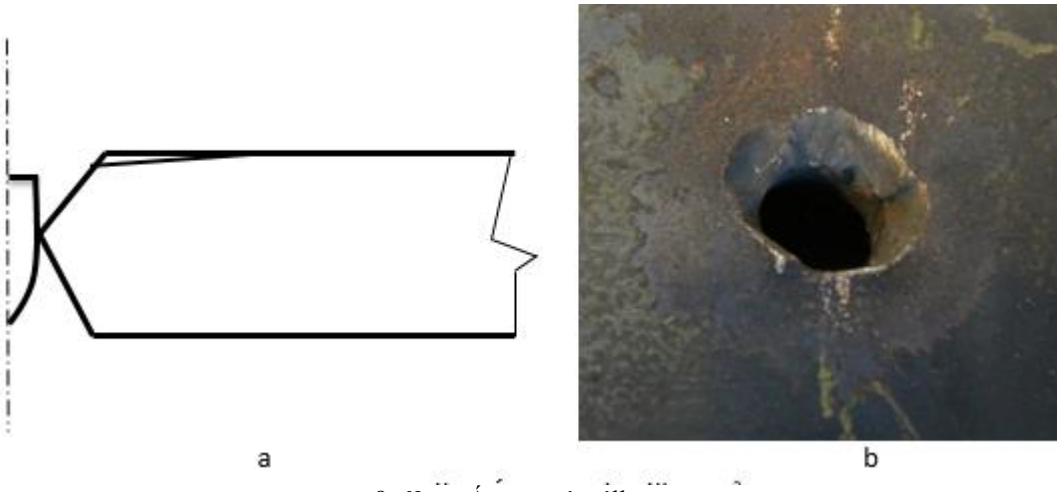


8. ábra. Referencia lemez átütése
a: elvi vázlat; b: fénykép

A páncélanyagok a nagyobb szilárdság elérése érdekében közel 0,3 % C-t, és 1,2 -1,3% Mn-t tartalmaznak. Ezek az anyagok a gyengén ötvözött acélok kategóriájába sorolhatóak, aminek hatására a szívósságuk, alakváltozó képességük megmarad, miközben hőkezelés hatására a szilárdságuk jelentősen javul. A két páncélanyag közel hasonló összetételű a csiszolatok mikroszkópi képein jól látható a hasonló martenzites szerkezet, amely a hőkezelésnek köszönhető. A „B” páncél anyag teljes keresztmetszete homogén, ellenben az „A” páncél anyag felületén anyagszerkezeti változás figyelhető meg. Az „A” páncél anyag mind a két felületén egy lágyabb ferrites anyagszerkezet látható maximum 0,1 mm mélységig.

Áthatolásos lövés során a vizsgált páncél anyagok mindegyike először egy maradó alakváltozást szenved, amely során az anyag belsejébe hatoló lövedék gumiszalag módjára torzítja a hengerlési szálakat. A BZ és B32 lövedék magja nem torzul (a lövések után gyűjtött ép hegyű lövedékmag alapján), ezáltal a hegyénél kialakuló helyi feszültségcsúcs hatására repedéseket hoz létre az anyag egy pontján. A repedéseket kitágítva a lövedékmagja továbbhalad, de ekkor már ridegen kiszakítja az előtte lévő anyagmennyiséget, ezzel repeszhatást okozva. A kiszakított anyagrész környezetében a hengerlési szálak elhajlanak.

Legtöbbször anyag vastagságának középső részén található a kialakult lyuk legszűkebb része, amely az anyag túlsó oldala felé haladva tölcsérszerűen szélesedik. A lyuk legkisebb része a lövedék magjával megegyező méretű, így az áthaladása során súrlódás lép fel az anyagok találkozásánál. A kialakult súrlódás a lövedék magjának hátsó részét leszakítja. A lövés után gyűjtött páncéltörő magok mindegyikének le van szakadva a hátsó része. Ez a leszakadt rész is áthatol az anyagon, azonban a súrlódás okozta húzófeszültség hatására kettéválik. A átütött páncélanyagokat és az átütés keresztmetszetét mutatja a 9. ábra.



9. ábra. Átütött páncéllemez
a: elvi vázlat; b: fénykép

A 7,62 x 54R mm B32 lőszerek esetében az anyag belépő oldalán lövedék köpeny részéről anyagfeltapadás látható, míg 7,62 x 39 mm BZ lőszerek esetén ez kevésbé jellemző.

Olyan esetben, amikor a lőszer áthatolása megtörténik, akkor az „A” páncél anyagban a keletkezett lyuk környezete sima, csak néhány esetben látható a lyukkal párhuzamost repedés, amely továbbterjedve minden valószínűség szerint további repeszhatást idézne elő. Ugyan ezen energiájú lövések esetén, ha van áthatolás, akkor a „B” páncél anyag esetében legtöbbször az alapanyag gyártása során kialakult hengerlési szálakkal párhuzamos repedések jelennek meg. A becsapódási energia növekedésével a hengerléssel (a lap síkjával) párhuzamosan kialakult repedésekre merőleges az anyagrész kiszakadását okozó újabb repedések jelennek meg. A lőszer magjának áthaladása során fellépő az „A” páncél anyagénál nagyobb súrlódás következtében, amelyet valószínűleg az anyag nagyobb szilárdsága miatt nagyobb lőszermagot szorító erő miatt alakul ki, a hengerlési rétegek elszakadnak egymástól. Így a „B” páncél anyag esetében a kisebb keresztmetszet ugyanakkora áthatolási védettség mellett, ha bekövetkezik a lövedék áthatolása, nagyobb repeszhatás lép fel.

Az LPSZ lágymagos lőszerek áthatolása során a lövedék magja miközben behatol a céltárgyba és ott maradó alakváltozást okoz, maga is deformálódik. A mag deformációja jelentős mértékű, a kialakult „gombás” alak mérete, a lövedék eredeti keresztmetszetének mintegy kétszerese. Gombásodott lágyacél-magvas lövedékeket mutat a 10. ábra.

10. ábra. Gombásodott LPSZ lövedékek

3. ÖSSZEFOGLALÁS, TOVÁBBI KUTATÁSI CÉLOK

A jelenlegi munkában a nagyszámú és széles spektrumú, lőtéri vizsgálatok mellett sikerült feltérképezni a vizsgált anyagokon, a lövedék becsapódásának vagy áthatolásának következményeit. Lehetőség van a lövedék becsapódás hatásának számítógépes szimulációjára azonban ehhez szükséges a jelenlegi munka alapján további, de már szűkített tartományú vizsgálatok elvégzése. A Haditechnikai Kutatóműhely kísérleti és kutatási tevékenysége során megteremtette azokat az alapokat, amelyek vizsgálatsorozat lehetséges kibővítését, folytatását szolgálják. A további kutatási irányok lehetnek:

- számítógépes szimuláció számára adatszolgáltatás különböző lőtávolságok esetén (különösen a páncéltörő lőszerek több típusával folytatott kísérletek eredményeinek összevetése, abból a szempontból, hogy milyen távolságon nyújt védelmet a célanyagból kialakított ballisztikai védőelem);
- a ballisztikai védőelemek kialakításakor szükséges, de anyagszerkezeti változást okozó munkák következményeinek vizsgálata különböző lőtávolságok esetén (a páncélozott járműveken az utólagosan felszerelt vagy hegesztett eszközök gyengíthetik a védelmi képességeket, ennek feltérképezése fontos terület lehet);
- repeszhatás vizsgálata adott lövedéktípus esetén különböző lőtávolságokon (a becsapódó, vagy áthatoló lövedék mozgási energiájának egy részét a páncélból leváló repeszeknek, melyek sebesítő hatását érdemes vizsgálni);
- az áthatoló lövedék pályájának, mozgásának, energiájának, ölő illetve sebesítő hatásának vizsgálata lőtávolság, lőszer típus és a célanyag függvényében.
- a páncéllemez védőképességének vizsgálata (mekkora lőtávolságon akad meg a lövedék a páncéllemezben, lőszertípus, lőtávolság illetve páncéllemez anyag és vastagság függvényében)
- a növekvő lőtávolság során a csökkenő sebességű lövedék által okozott torzulás mértékének vizsgálata, a lemezek hengerlési-szál torzulásának mérésével.

A becsapódások, áthatolások felvétele gyorskamerával lehetővé teszi a lövedék, a páncéllemez, az esetleges repeszek mozgásának vizuális rögzítését. Méretbeosztással rendelkező háttér elhelyezésével az időparaméter rögzítésével a mozgó szilánkok, vagy lövedék sebessége kiszámítható.

Felhasznált irodalom

[1] Sebők, I., Gávay, G. Destructive testing of metallic and non-metallic material MECHANICAL ENGINEERING LETTERS: R AND D: RESEARCH AND DEVELOPMENT 9: pp. 28-33. (2013)

[2] MSZ K Standard 1114-1 (1999) Body armours. Bulletproof vests

[3] NIJ Standard 0101.06 (2008) Ballistic Resistance of Body Armor

[4] Gyarmati, J., Kalácska, G., Szakál, Z., Gávay, G. – Sebők, I., Lövedék páncéllemezen történő áthaladás metallográfiai vizsgálata, Tanulmány, Nemzeti Közszolgálati Egyetem „Egyetemi Kutatóműhely Támogatása" Pályázat, Támogatási szerződés száma: NKE - SIRH-PI-10-3/2013 Budapest, 56 p., 2014.

[5] Löfe/104, 7,62 mm-es PKM és PKMSZ Kalasnyikov géppuska anyagismereti és lőutasítása, Honvédelmi Minisztérium, 1976.

[6] НАСТАВЛЕНИЕ по СТРЕЛКОВОМУ ДЕЛУ 7,62-мм МОДЕРНИЗИРОВАННЫЙ АВТОМАТ КАЛАШНИКОВА (АКМ и АКСМ) Из*дание третье, исправленное и дополненное* Ордена Трудового Красн ого Знамени ВОЕННОЕ ИЗДАТЕЛЬСТВО МИНИСТЕРСТВА ОБОРОНЫ СССР Москва -1970

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Lukács Lóránd
lukacsl@iit.bme.hu

AUGMENTED REALITY FOR AIRCRAFT CONTROL

Abstract

The paper presents a low computational cost system engineering solution which can be used for the control and navigation of airplanes in low visibility when Instrumental Flight Rules apply. The application presented in the paper uses the orientation and navigation information of a glider aircraft superimposed on images acquired with a wide angle lens camera during flight. Using this method of displaying data, the crucial information needed for aircraft control such as orientation, heading, airspeed, vertical speed, altitude, angle of attack and slip angle of the aircraft can be viewed by pilots without requiring them to lose sight of their visual viewpoints. The paper emphasizes on determining the correct position of the main visual elements on the image plane required for maintaining the desired heading and attitude of the aircraft. The developed method can also be applied for UAVs controlled via video link.

A tanulmány légi járművek irányításához szükséges alacsony számítási költségekkel járó megoldást mutat be, ami alkalmazható rossz látási körülmények közötti vezérlésénél vagy olyan esetekben, amikor műszerrepülési helyzetek lépnek fel. A bemutatott alkalmazás egy vitorlázó repülőgép példáján becsült orientációs és navigációs adatokat helyez széles látószögű videó kamera által rögzített képekre repülés közben. Ez az adatmegjelenítési módszer a repülőgép vezérléséhez szükséges elengedhetetlen információkat, mint orientáció, útirány, repülési sebesség, vertikális sebesség, magasság, állásszög és oldalcsúszási szög értékeket jelenít meg anélkül, hogy a pilóta kényszerítve legyen, hogy szem elől tévessze a repüléshez szükséges vizuális referenciáit. A cikk fő hangsúlya a repülőgép orientációjához szükséges főbb vizuális elemek képsíkon való helyének meghatározására esik. A módszer videó kapcsolaton keresztül vezérelt embernélküli légi járművek irányításánál is alkalmazható.

Keywords: *heads up display, artificial horizon, aircraft control, UAV control ~ homloküveg kijelző, mesterséges horizon, repülés irányítás, UAV irányítás*

INTRODUCTION

In case of a conventional aircraft or Unmanned Aerial Vehicle (UAV) controlled via video link, by implementing a heads-up display for aircraft control, the critical information required to fly the aircraft is presented in the pilot's forward field of view, which eliminates the need of continual transition from head-down instruments to head-up, out-the window view during critical phases of flight. With the eyes of the pilot focused out in front of the aircraft and viewing the presentation of airspeed, altitude, aircraft heading and attitude, flight path, flight path angle, pilots can achieve greater precision and situational awareness at all times.

The paper presents a head-up display design method on the example of a glider aircraft with an added video camera, GPS and IMU sensory information. Some details of state estimation [9], [10] and image processing [7] used in the paper can be found in earlier publications.

Since the method uses a wide angle lens camera, this approach can be best implemented on unmanned aerial vehicles or UAVs. The main scope of the paper is the determination of correct artificial horizon and velocity vector placement on the image plane when a wide angle lens camera is used as the means for flying the aircraft by instrumental flight rules (IFR).

Commercial fixed mounted head-up displays typically project the visual data on an angled flat transparent surface (also called a combiner) located directly in front of the pilot. Acting as a beam splitter, this redirects the projected image from the projector in a way that allows the pilot to see the field of view and the projected image at infinity at the same time. Combiners may have special coatings that reflect the monochromatic light used to project the necessary imagery and symbology to be displayed while allowing all other wavelengths of light to pass through. The employment of a head-up display system has the proven result of allowing higher piloting precision while having a standardized HUD system enables easier transition between different types of aircraft.

Early head up displays had been employed on military aircraft and were focused on computed gunnery solutions, using aircraft information such as airspeed and angle of attack, thus greatly increasing the accuracy pilots could achieve in air to air battles. Today, we also see HUD's being increasingly available on commercial passenger aircrafts.

Despite showing substantial flexibility in the use of head-up displays on commercial aircraft, basic HUDs displays use the following symbols:

- airspeed, altitude, vertical velocity
- a horizon line (artificial horizon)
- aircraft attitude indicator in the form of a so called 'ladder', displaying the aircraft's pitch and roll relative to the ground's level/horizon in degrees
- turn/bank and slip/skid indicators
- waterline symbol or aircraft boresight- shows where the nose of the aircraft is actually pointing
- course and/or heading – where heading is defined by the angle between the direction in which the vehicle's nose is pointing and a reference direction (e.g. true north)
- Flight Path Vector (Velocity Vector Symbol) - shows where the aircraft is actually going, which is useful for example, in a situation where the aircraft is pitched up but is losing energy. Here, the waterline and velocity vectors do not overlap as the former is above, while the latter is below the horizon line. This information is particularly useful on landing approach, where the pilot can visualize the location on the runway where the aircraft will touch down. The velocity vector symbol also shows if the aircraft is slipping/skidding, a situation that reduces aerodynamic efficiency. Keeping the velocity vector symbol on the waterline symbol allows the pilot to perform level turns at various angles of bank.

Unmanned aerial vehicles lack a pilot in the cockpit and are controlled using a specialized data link with live video feed. The video system of the aircraft consists of one or more video cameras for aircraft control. The limitations of using video cameras for manual aircraft control consist mainly in the narrow field of view of the employed camera system which limits the UAV operator's situational awareness. This problem can be addressed to a certain degree by using a wide angle lens camera to increase the pilot's field of view.

The two problems to be overcome when using wide angle lens cameras are the heavy distortion of the lens and the need of a 1:1 scaling of the displayed image so that the projected HUD elements overlay those of the outside world. This presents a nonlinear problem accentuating the difficulty in determination of relevant HUD symbol positions on the image plane.

The chosen platform for flight data gathering was the R26S-Góbé type two-seater sailplane (glider). The visual images have been supplied by a wide angle lens camera externally mounted on the vertical stabilizer of the aircraft, facing in the direction of flight.

Regarding the terminology of the paper, the usual ECI, ECEF, NED and ABC (Aircraft Body or shortly Body) coordinate systems (frames) used for aerial navigation are used, see Figure 1. The frames are referred to by the indexes i, e, n, b.

Lacking an onboard navigation system, an external sensory system had been fitted on the aircraft in the form of an accelerometer, angular velocity meter, magnetometer (IMU) and differential GPS receivers. State estimation for the aircraft is based on a two level Extended Kalman Filtering with an additional external correction loop. The state estimator also supplies the data needed for displaying the Flight Path Vector in the form of flight path angle and drift information in degrees.

The problems to be solved are:

- accurately show the direction at which the nose of the aircraft is pointing (Boresighting);
- overlapping the vertical horizon line on the visible horizon line of the images supplied by the wide angle lens camera;
- displaying a set of compass values on the virtual horizon line so that the virtual cardinal directions shown overlap the actual cardinal directions seen from the aircraft;
- displaying the actual direction of flight by the means of a Flight Path Vector (FPV) by taking into account the drift and actual angle of attack of the aircraft.

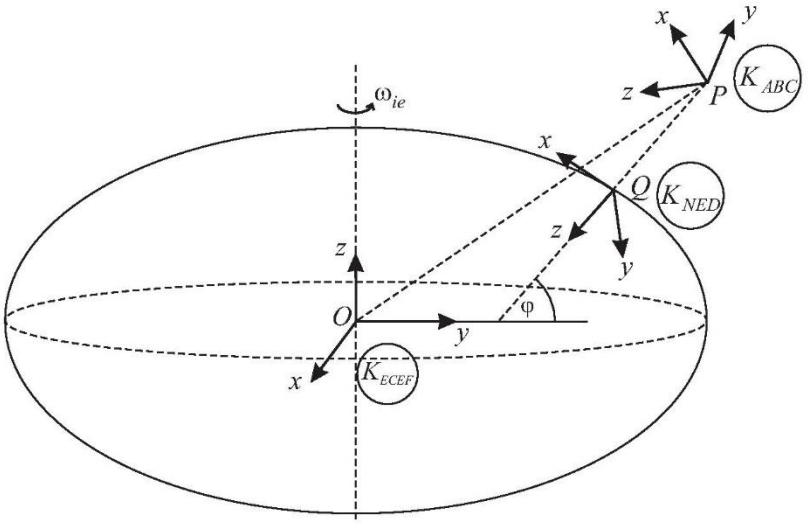


Figure 1. Coordinate systems used in navigation

The signals belonging to the body frame are shown in Figure 2, where Φ, Θ, Ψ denote the Euler (roll, pitch, yaw) angles, U, V, W represent the velocity, P, Q, R the angular velocity, X, Y, Z the force and L, M, N the torque components, v_T is the magnitude of the velocity, α is the angle of attack and β is the sideslip angle.

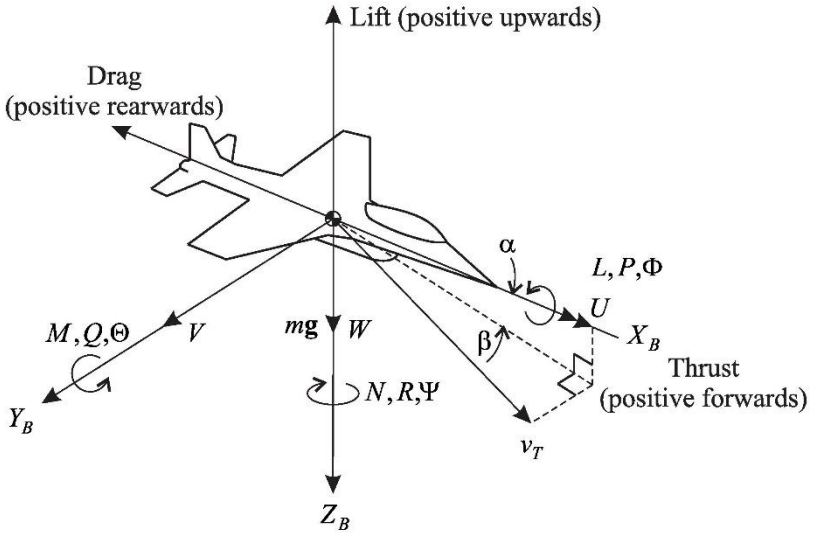


Figure 2. Aircraft frame and kinematic force/torque variables

DATA USED FOR DISPLAYING INFORMATION ON THE HEADS UP DISPLAY

For accurately displaying information needed to fly the airplane or unmanned aerial vehicle, the variables on the HUD use the data supplied by the state estimator. The supplied data consists of the following:

- measured GPS position in the K_e frame in $[m]$
- estimated velocity in the aircraft's K_b frame of reference along its three axis in *m/s*
- quaternion based orientation in K_b

The data supplied by the state estimator undergoes a transformation that allows it to be used on the HUD. Firstly, the position of the aircraft measured in the K_e frame has to be converted to the K_n frame used in aerial navigation. When displaying the height of the aircraft, the 'Down' axis position can be used. For using the QFE altimeter settings, the stationary position of the aircraft has been used as a reference point to zero the altimeter.

The velocity of the aircraft is displayed according to its x_b values and converted from m/s to km/h. Since the sensors available are not capable of measuring wind speed and direction, these values are also estimated and taken into account when displaying the velocity of the aircraft. Due to the fact the velocity of the aircraft is estimated in K_b and the wind speed in K_n, the following conversion needs to be implemented in order to get the correct data in K_b. By knowing the direction and intensity of the wind, the projections of the wind effect on the x_n, y_n axes are obtained:

$$v_{wind\_n} = \begin{pmatrix} v_{wind} \cdot C_{wind\_dir} \\ v_{wind} \cdot S_{wind\_dir} \\ 0 \end{pmatrix} \quad (1)$$

Where the short forms C_{wind_dir} and S_{wind_dir} denote $\cos(x)$ and $\sin(x)$ respectively.

The aircraft velocity corrected for wind effects will be:

$$v_{a\_w\_n} = v_{a\_n} + v_{wind\_n} \tag{2}$$

Finally, the velocity of the aircraft corrected for wind effects in K_b will take the form of:

$$v_{aircr\_b} = {R_{b2n}}^T \cdot v_{a\_w\_n} \tag{3}$$

where:

$$v_{aircr\_b} = \begin{pmatrix} U_b \\ V_b \\ W_b \end{pmatrix} \tag{4}$$

and:

v_{wind} – wind direction and intensity in K_n
$v_{a\_w\_n}$ – aircraft velocity corrected for wind effects
v_{a_n} – estimated aircraft velocity
v_{wind_n} – estimated wind speed
${R_{b2n}}^T$ – transpose of K_b to K_n transformation matrix

The vertical velocity indicator of the HUD uses the aircrafts velocity along its 'Down' axis in *m/s* after a conversion to the K_n frame.

The quaternion based orientation of the aircraft is firstly converted to Euler's RPY angles in degrees and converted from K_b to the K_n frame using (5). This information is used to display heading and the virtual horizon elements of the HUD. In this article the notation for the RPY Euler angles will use Φ, Θ and Ψ.

$$\hat{q}_b \xrightarrow{R_{B2N}} \Phi_n, \Theta_n, \Psi_n \tag{5}$$

The β slip angle and α angle of attack is calculated according to the following [3]:

$$\alpha = atan\left(\frac{W_b}{U_b}\right) \tag{6}$$

$$\beta = asin\left(\frac{V_b}{v_{abs}}\right) \tag{7}$$

where:

$$v_{abs} = \left\| v_{aircr\_b} \right\| \tag{8}$$

VIDEO CAMERA CALIBRATION AND BORESIGHTING

To be able to display the required data accurately, the internal and external parameters of the video camera have to be known. The internal parameters of the camera are: image size, focal length, principal point, skew, radial and tangential distortion coefficients. The video camera's internal parameters are a priori identified using a chess board like picture rendition and the camera's K matrix is regarded as known [5]:

$$K = \begin{bmatrix} f_x & \alpha_c \cdot f_x & c_x \\ 0 & f_y & c_y \\ 0 & 0 & 1 \end{bmatrix} \tag{9}$$

where:

f_x, f_y - identified focal length in pixels

c_x, c_y - principal point of the camera

α_c - skew

Viewing the complete distortion model of the lens it can be seen that a relevant radial distortion of up to 250 pixels is present in certain areas.

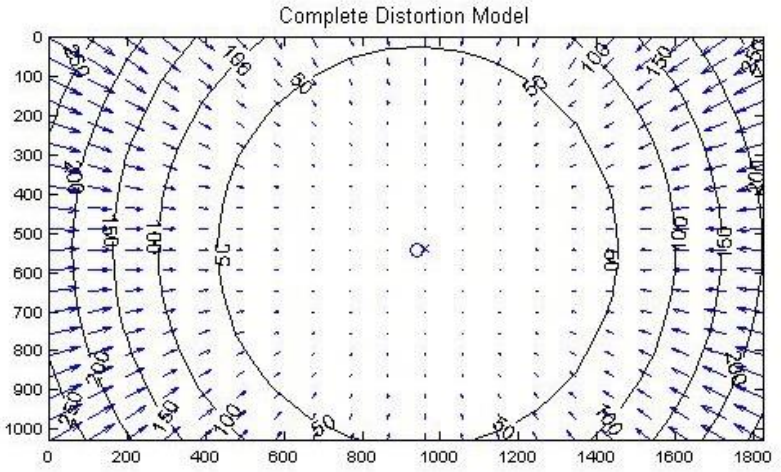


Figure 3. Identified complete distortion model of the wide angle lens camera

In order to obtain accurately aligned HUD elements, the aircraft, its sensors and the camera system need to be aligned with the aircraft's three axes – a process referred to as boresighting – so that the displayed data conforms to the reality of the captured image of the video camera. This allows the display to show the pilot exactly where the horizon is, the position of the cardinal directions as well as the aircraft's projected path with great accuracy.

The location of the IMU relative to the video camera is also known and taken into account and has its axes are aligned with the axes of symmetry of the aircraft.

Since the video camera had been mounted on the vertical stabilizer of the aircraft, a number of reference points can be singled out which are fixed to the aircraft's body coordinate system and are visible by the video camera. These reference points are required to be non-coplanar. The world coordinates of the 15 reference points are calculated based on the airplane design and are considered having the location of the video camera as the point of origin. The reference points can also be located on the captured images of the video camera (see Figure 4) so their pixel-coordinates can be measured. By knowing both the reciprocal world- and pixel coordinates of these reference points and the internal parameters of the wide angle lens video camera, the orientation of the video camera relative to the airplane can be determined. This process takes into consideration the internal camera parameters and uses the Least Squares method forming an abstract optimization problem. This can be solved with the Lagrange multiplier method and yields an optimal result with the use of singular value decomposition. The method is described in more detail in [1] and [7]. With the resulting R_{opt} rotation matrix the Φ and Ψ angular offsets of the HUD can be corrected.

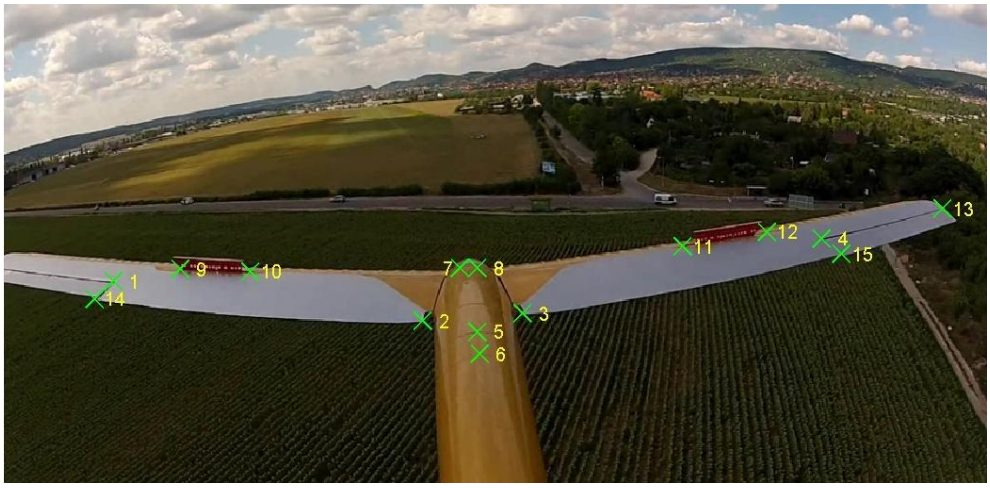


Figure 4. Visual reference points used for Head Up Display boresighting

The arrangement of the video camera, the inertial measurement units and spatial arrangement of the visual reference points used for boresighting the Heads Up Display elements can be seen in Figure 5 as a 3D rendering of the mentioned points (the view of the 3D plot is from behind the airplane).

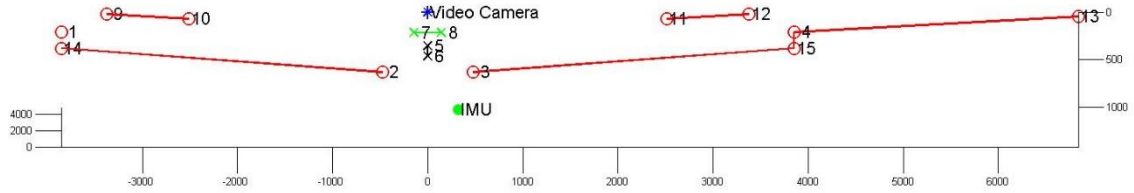


Figure 5. 3D rendering of reference points used for Head Up Display boresighting [mm]

PROJECTING THE VIRTUAL HORIZON LINE ON THE IMAGE PLANE CONSIDERING THE DISTORTION OF THE WIDE ANGLE LENS

While the display of altitude, airspeed, vertical velocity and heading on the HUD are mostly straightforward, the display of the artificial horizon also has to take into account the internal parameters of the wide angle lens camera. In order to have a useable system, the position and orientation of the artificial horizon line displayed on the image plane of the HUD has to be superimposed on the actual horizon line visible on the camera recording. The rendering of the virtual horizon line's vertical position uses the Θ angle for pitch, while its slope is based on the Φ bank angle, both derived from quaternions and converted in the NED frame.

The problem lies in the nonlinear distortion originating from the construction of the lens. As it can be seen in Figure 3, the distortion of the lens is mainly radial. For example, in level flight when $\Theta = 0$ and $\Phi = 0$, with a camera having its axes aligned with the axes of symmetry of the aircraft, we would have the rendering of the virtual horizon line in the center of the image plane superimposing the horizon line visible by the camera. But as the pitch of the aircraft is changed, a linear change in the vertical position of the virtual horizon line will present a nonlinearly increasing error in the difference between the positions of the actual and virtual horizon lines due to the radial distortion of the camera. Similarly, the spacing of the attitude indicator (or 'ladder') elements has to follow the nonlinearity of the distorted image even though they represent linear $10^{\mathbf{o}}$ increments of pitch. The cardinal directions on the virtual horizon line have to be placed in a way that they overlap the actual cardinal directions seen

from the aircraft and displaying the position the Flight Path Vector symbol showing the actual direction that the aircraft is going. In short, a solution needs to be found that converts the Θ and Φ angles supplied by the state estimator to the correct u, v pixel values while reducing the actual camera model to a pinhole camera. The transformation is illustrated in Figure 5.

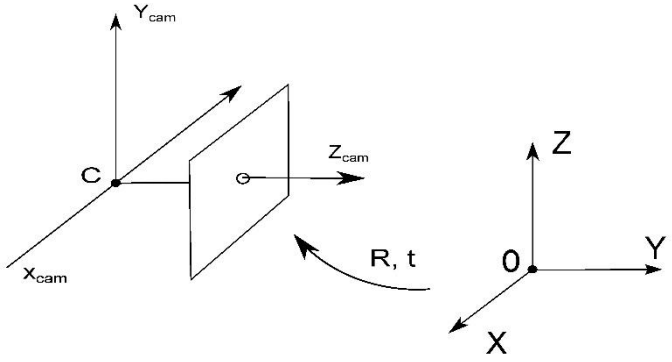


Figure 5. Transformation between world and camera coordinate frames

According to [2], the direct method for a Euclidian transformation between world and camera coordinate frames is used which also takes into account the mentioned lens distortion.

The position and orientation of the camera is also considered:

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = R \cdot \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} + \begin{bmatrix} t_x \\ t_y \\ t_z \end{bmatrix} \tag{10}$$

Where:

R - represents the camera orientation matrix acquired using the boresighting process

$(X, Y, Z)^T$ - world coordinates of the point P to be transformed to u, vpixel coordinates

$\left(t_x, t_y, t_z\right)^T$ - translation matrix of the camera

The mapping of the $(X, Y, Z)^T$ point from world coordinates to image plane is done by:

$$\begin{aligned} x' &= \frac{x}{z} \\ y' &= \frac{y}{z} \end{aligned} \tag{11}$$

Using the notations:

$$\begin{aligned} x'' &= x'(1 + k_1 r^2 + k_2 r^4) \\ y'' &= y'(1 + k_1 r^2 + k_2 r^4) \end{aligned} \tag{12}$$

where:

$$r^2 = x'^2 + y'^2 \tag{13}$$

The transformed u, v pixel coordinates will be:

$$\begin{aligned} u &= f_x \cdot x'' + c_x \\ v &= f_y \cdot y'' + c_y \end{aligned} \tag{14}$$

By definition, the horizon line is the line that separates earth from sky and has a critical importance in aviation in that it gives pilots a visual reference when keeping the wings of the aircraft leveled in horizontal flight or gives a visual indication of bank angle and pitch of the aircraft. Even though the actual horizon line is perceived as curved at higher altitudes and its curvature is accentuated due to the distortion effect of the wide angle lens, the virtual horizon line projected on the HUD needs to be a straight line. As a straight line, its position on the HUD image plane can be described using the vertical position of a single point P_H transformed to u, v image coordinates, in combination with the slope of a line intersecting P_H. In this paper, the

vertical position of P_H is in direct correlation with the Θ pitch angle, while the slope is being determined by the Φ bank angle.

As it can be seen in Figure 6, an optimal alignment of the camera has its X_C, Y_C, Z_C axes running parallel to the Y_b, Z_b, X_b axes of the aircraft body. Any possible misalignments between the mentioned axes are detected by the boresighting method presented in the previous section. As mentioned before, the actual horizon line perceived by the wide angle lens camera is a straight line only when it is parallel with the X_C axis and runs through the principal axis of the camera. In any other case, the horizon line is perceived as either a convex or a concave curve depending on weather it is above or below the Z_C principal axis. This way, the rendition of the virtual horizon line on the HUD image plane is taking P_H as the point of tangency of a straight line to the actual horizon line with P_{H0} set on the principal axis of the camera when $\Theta = 0$.

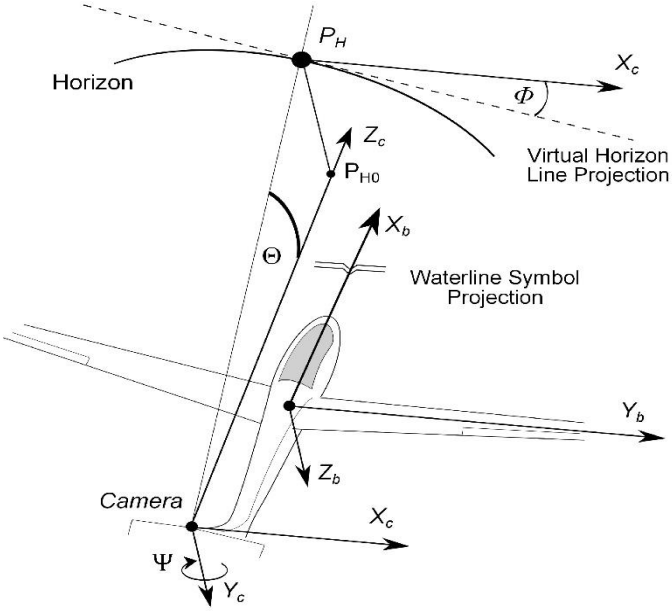


Figure 6. Video camera setup and Virtual Horizon Line projection concept

EXPERIMENTAL SETUP FOR VIRTUAL HORIZON LINE REPROJECTION ON IMAGES TAKEN WITH THE WIDE ANGLE LENS CAMERA

Once the transformation method from 3D world coordinates to u, v pixel coordinates is established, an experimental setup has been elaborated that reproduces the visual effect of the horizon as perceived by the airplane mounted camera. The concept for the experimental setup is based on the image of the actual horizon line as perceived by the camera. By studying the captured frames it is evident that the by changing the Θ pitch angle of the aircraft, the horizon line performs a translational movement across the image plane as shown in Figure 7.

Figure 7. Movement of the horizon on the image plane as perceived by the wide angle lens video camera

This simplification is performed with regards to the fact that for pitch control the position of a single point P_H relative to the X_C axis of the camera is sufficient, noting that P_H is formed by the intersection between the visible horizon line and the Y_C, Z_C plane (see Figure 6). Due to the fact that P_H is a point, no perspective issues arise.

This has been modeled using the wide angle lens camera facing a chessboard like picture rendition, where the distance from camera to chessboard and the dimensions of chessboard squares are known. The modeling concept shown on Figure 8 has Z_1 as the distance from camera center to chessboard, and Y_1 and X_1(not shown) are the distances from P_0 to P_1 in world coordinates. Point P_0 is set on the principal axis of the camera, having $X_1 = 0, Y_1 = 0$ and $t_{Y1} = 0, t_{X1} = 0$ where the $X_1, Y_1, Z_1, t_{X1}, t_{Y1}, t_{Z1}$ values are the ones used in (9) with the boresight correction angles contained in the R matrix.

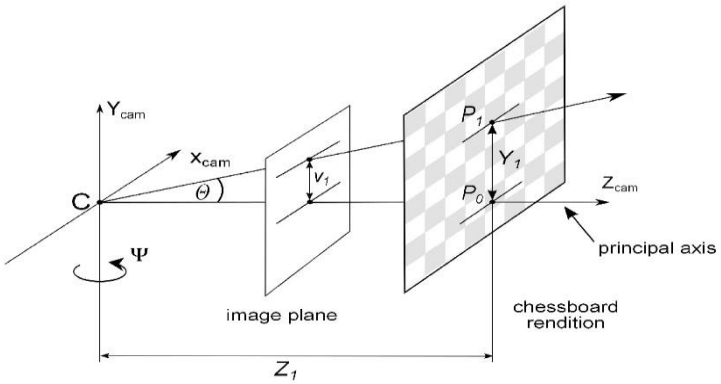


Figure 8. Re-projection of point P_1 on the image plane using a chessboard image

By using the proposed transformation method from world to pixel coordinates with the experimental setup and knowing the world coordinates of P_1, its undistorted u, v coordinates can be obtained with Θ derived from the C, P_0, P_1 triangle. Conversely, considering the C, P_0, P_1 triangle if the Θ angle and the X_1, Z_1,world coordinates of P_1 are known, then the vertical position of point P_1, described by Y_1 can be calculated, reprojecting the point on the image plane, superimposing P_1. Since the tangent function is not linear, its linearization is needed in order to precisely follow the chessboard pattern.

The reprojection method has been verified by re-generating the chessboard tile corners on the image taken with the wide angle lens camera. The results when the chessboard tiles are aligned with the X_{cam}, Y_{cam} axes of the camera are shown in Figure 9. Even in the areas of heavy distortion, the markers are superimposed on the intersections of chessboard tiles. The magenta + marker in the middle of the image is set on the principal point, while the green × marker is the first visual marker to be superimposed on the image. Its position is moved to the nearest intersection and all subsequent markers are generated using the iteration of linearized Θ, Ψ angles. The positioning of the starting marker to the intersection nearest the principal point is performed by the fine tuning of t_{X1}, t_{Y1} values.

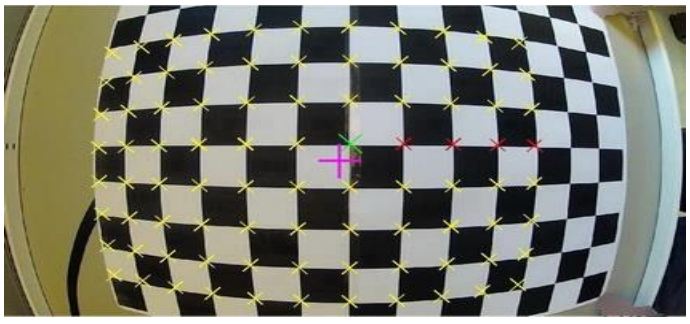


Figure 9. Reprojected world coordinate points on the image plane

In the event the aircraft presents a certain Φ roll angle, the slope of the virtual horizon line is performed by changing the roll angle in the camera orientation matrix R to the value of Φ. This is followed by the rendition of the virtual horizon line according to the pitch angle of the aircraft as described previously. The laboratory results can be verified using Figure 10, where the projected visual markers overlap the intersections of the chessboard tiles with the chessboard having a 69 deg. roll angle around the Z_{cam} camera axis.

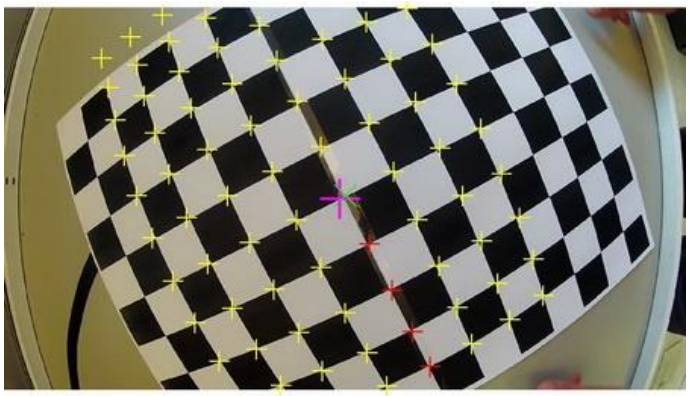


Figure 10. Reprojected world coordinate points on chessboard image with $\Phi = 69°$

The transition from laboratory setup to real world application is based on the hypothesis that in the real world, the actual horizon line is always at a fixed distance from the aircraft: at a constant altitude, objects beyond the horizon line come into view at the traveling speed of the aircraft.

This way considering the C, P_{H0}, P_H, and C, P_0, P_1 seen in Figure 11, it can be concluded that the two are similar right angle triangles sharing the Θ acute angle. Here, C represents the camera center, P_0, P_1 are seen as the world coordinate points found on the chessboard rendition with $(C, \widehat{P_0, P_1}) = 90°$. Similarly P_{H0} represents a point on the horizon line when $\Theta = 0$ and P_H is the same point on the horizon line when the attitude of the aircraft changes to a nonzero Θ. In this concept $(C, \widehat{P_{H0}, P_H})$ is considered as a right angle.

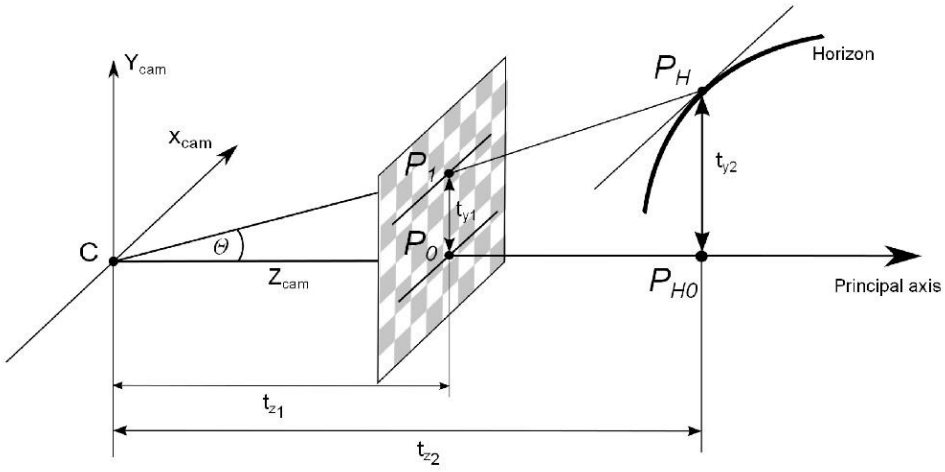


Figure 11. Linking the laboratory setup with the real world application

By viewing the horizon line reprojection problem as a similar right angle triangle problem, at any given Θ, the required t_{z2}, t_{y2} distance variables to be used for the transformation of point P_H from world to image coordinates can be substituted with the pre-calibrated t_{z1}, t_{y1} distances of the laboratory setup.

HEADS UP DISPLAY APPLICATION USING ACTUAL FLIGHT DATA

Besides laboratory testing, the presented method has been verified by constructing a working Heads Up Display using the aircraft mounted wide angle lens video camera during flight and actual flight data.

The HUD elements superimposed on the images taken with the wide angle lens video camera can be seen in Figure 12 having the encircled numbers in the figure replaced by brackets in the text. As described in the introduction, the main HUD element responsible for helping the pilot maintain the orientation of the aircraft is the virtual horizon line {2} with the attitude indicator or 'ladder' {3}. These are used in conjunction with the waterline symbol to maintain the desired attitude of the aircraft. The application uses the position and inclination of the virtual horizon line as determined using the presented algorithm. Similarly, the spacing between 'ladder' elements is calculated the same way using 10 degree Θ angle increments above and below the virtual horizon line. The waterline symbol {1} represents a small aircraft symbol positioned on the image plane in a way that its center is projected on the X_b axis of the aircraft and has its 'wings' parallel to Y_b (see Figure 6.). The position of this symbol on the image plane is determined in the boresighting phase.

When instrumental flight rules apply, in order to maintain a level flight all the pilot has to do is to align the 'wings' of the waterline symbol with the virtual horizon line. In level flight, the bank angle can be determined visually by the angle between the wings of the waterline symbol and virtual horizon line. Similarly, a desired pitch angle can be achieved by the pilot by aligning the waterline symbol with the 'ladder' element corresponding to the desired Θ. Due to the fact that the ladder elements are always parallel with the virtual horizon line, in case the horizon is not in view of the camera and the virtual horizon line cannot be projected on the image plane, the ladder elements are to be used as secondary virtual horizon lines for control of the aircraft. The use of the aircraft attitude indicator and waterline symbol is presented in Figure 12, where the aircraft has a 13.5 degree pitch angle and a bank angle of 38 degrees.

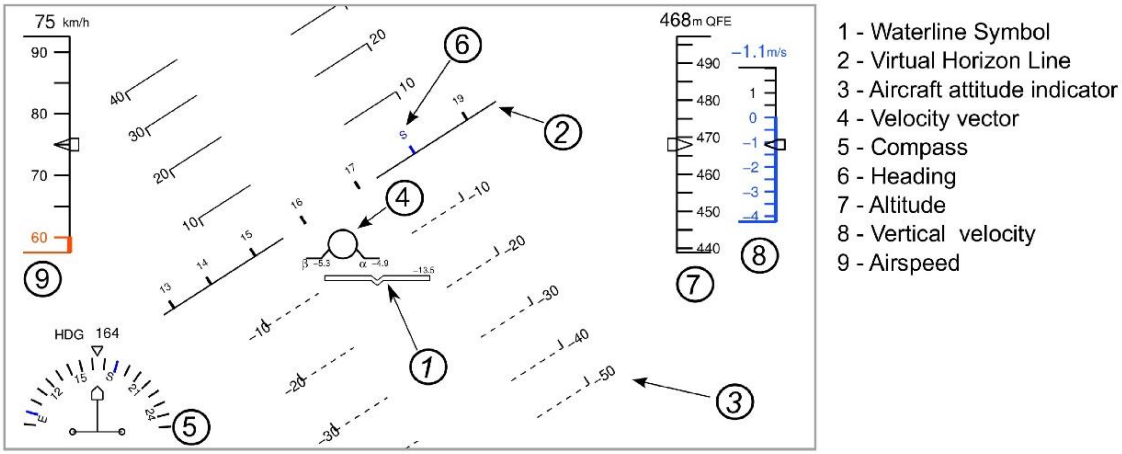


Figure 12. Projected Heads Up Display elements using actual flight data

As for the heading of the aircraft, the pilot can take visual cues from two HUD elements, a compass with a moving bezel {5} or from the heading values projected above the virtual horizon line {6} the position of which overlap the reference points of actual cardinal directions that are visible from the aircraft. The positioning of the cardinal values on the image plane is achieved using the presented method with a horizontal spacing of 10 degrees between compass points on the image. By placing the waterline symbol on a heading value projected on the virtual horizon line, the desired heading can be achieved.

The airspeed {9}, altitude {7} and vertical velocity {8} indicators have moving bezels with the actual values displayed numerically above the indicator boxes. All three indicators have scales moving behind a fixed arrow found in the middle of the indicator boxes. Moving scales have an advantage over numerical displays in being able to conveniently display the operating ranges of the aircraft, for example, by using a color coding on the airspeed indicator.

In this case, the 60 km/h stall speed of the aircraft is visible in orange and helps the pilot to intuitively determine how close the aircraft is to a stall. Minimum and maximum flaps and landing gear retraction and extension speeds can also be displayed using this method.

The Flight Path Vector or FPV {4} shows the aircraft as seen from behind and represents the direction the aircraft is actually moving as this does not always coincide with the direction the nose of the aircraft is pointing (Waterline symbol). Its use significantly reduces pilot workload on landing approaches and when flying in crosswinds. The position of the FPV coincides with that of the waterline symbol in cases when the angle of attack $\alpha = 0$ and the slip angle $\beta = 0$. The position of the FPV on the image plane and its deviation from its neutral position is also determined with the presented method according to the angular values of α and β.

Placement of the FPV along the pitch axis indicates the Flight path angle (FPA). When the FPV is on the horizon line, the FPA is zero (level flight). If the FPV is above the horizon line, the airplane is climbing; below the line, the airplane is descending regardless where the nose of the aircraft is pointing. The angle of climb or descent corresponds to where the center of the FPV intersects the pitch scale so flying the FPV to 3° below the horizon always produces a 3° glidepath. In the case presented in Figure 12, as a left hand turn is performed, even though its nose is pointing to -13.5 degrees, the flight path angle of the aircraft is only -4.5 degrees.

In the case presented in Figure 12, the FPV also shows that the aircraft is slipping, meaning that it is sideways to the relative airflow. This undesirable state can thus be visualized and corrected using the FPV.

RESULTS

By using the proposed method with a wide angle lens video camera mounted on a glider airplane during flight, together with gathered flight data, a useable Head Up Display has been realized containing all basic instrumentation required to operate a simple aircraft. The presented projection of HUD elements on the image plane had been applied to each frame captured by the video camera during flight, which resulted in a video recording. A frame from the video recording, showing the HUD elements seen in Figure 12 is presented on Figure 13.

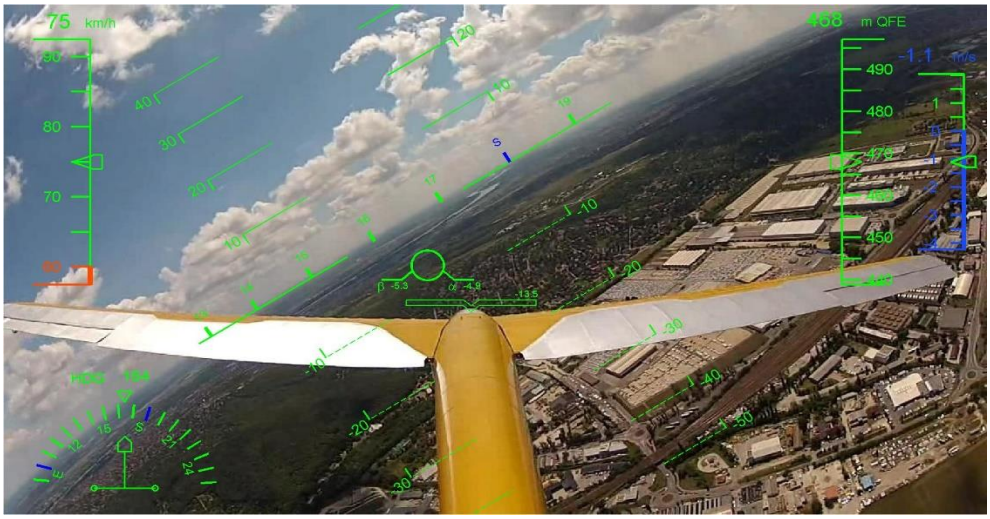


Figure 13. Screenshot of HUD projected on the wide angle lens camera recording

The validation of the proposed method had been performed in two ways. Firstly, by visual verification of the alignment of the actual horizon with the position of the virtual horizon line, and secondly, by means of image processing.

The image processing algorithm firstly determines the pixel position of the horizon line on the image plane. Since, at times this line appears curved due to the distortion effect of the wide angle lens camera, a least squares approximation of multiple points found on the horizon is used to determine the position of point P_H. Point P_H is the point on the horizon set on the $X_b Y_b$ plane, as seen in Figure 6. By using the inverse of the proposed method, angle Θ can be obtained while Φ can be calculated using the slope of the line determined with the least squares approximation. The image processing algorithm is performed on every frame of the video recording and the obtained Φ, Θ angles are converted to K_n using equation (5). A screenshot of the image processing video can be seen in Figure 14, with the green dot representing point P_H, while the yellow line is the least squares approximation of the horizon line.

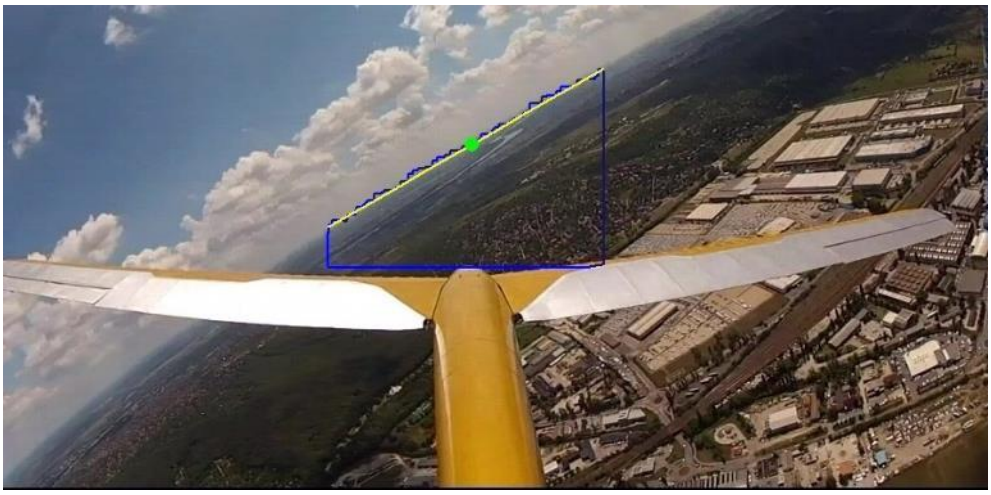


Figure 14. Image processing for horizon position and bank angle determination

Since the horizon line is not always visible due to the obstruction from view of the aircraft wings, data in these few cases is disregarded in later analysis.

Using the Φ, Θ angle data obtained from image processing and from estimated flight data, the correlation of the two respective data sets has been determined to be 0.901 for the Θ angle and 0.926 for Φ as shown in figures 15 and 16. However, since the flight data is obtained by a state estimator, the quality of obtained data is largely determined by the fine tuning of the multiple extended and classical Kalman filters. By improving the quality of estimated data, the correlation between the two data sets can be further improved.

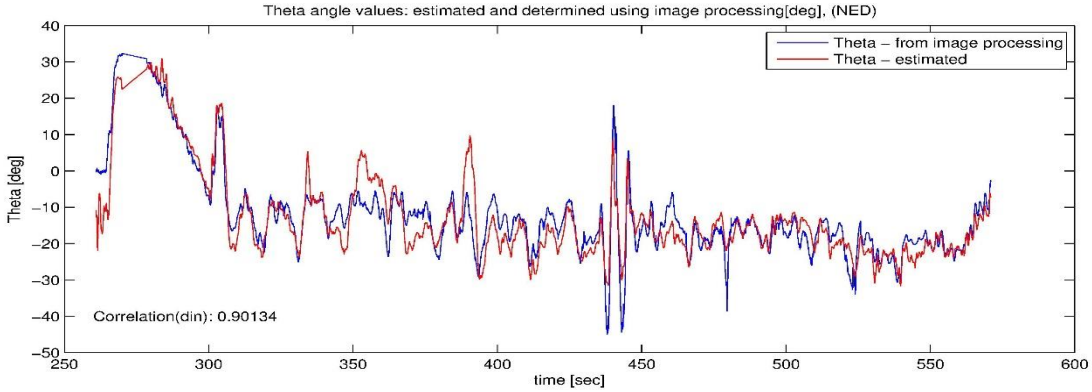


Figure 15. Correlation of Θ angles, estiamted vs. determined by image processing

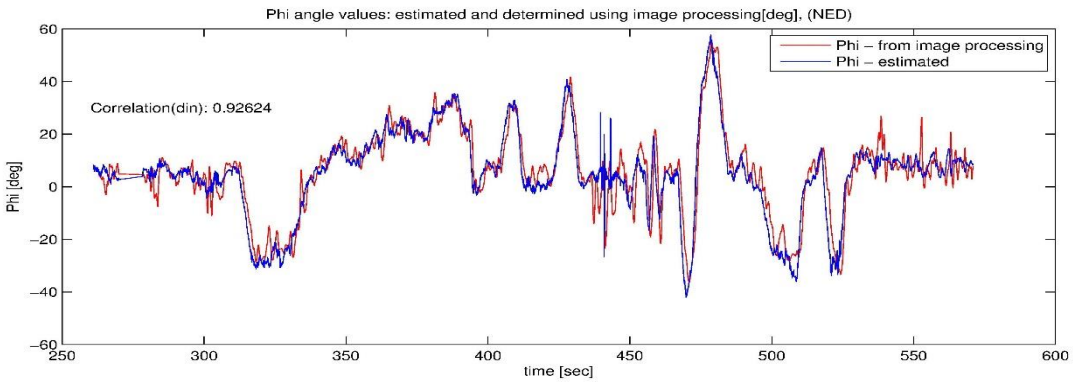


Figure 16. Correlation of Φ angles, estiamted vs. determined by image processing

CONCLUSION

The paper presented methods and algorithms to solve the problem of a Heads Up Display projection on images taken with a wide angle lens camera. The method can prove especially useful in unmanned aerial vehicle control, where the use of a wide angle lens increases the field of view of the pilot thus increasing situational awareness. However, the use of a wide angle lens camera introduces severe distortion effects, a nonlinear problem that needs to be solved when placing the HUD elements responsible for attitude control on the image plane.

The paper gives a viable method for overcoming this problem, while realizing the 1:1 scaling of the displayed images so that the projected HUD elements overlay those of the outside world.

This is achieved at a low computational cost implementable on portable systems.

References

[1] Tél F, *Stereo Image Processing System for Robotic Applications*, PhD Thesis. Budapest University of Technology and Economics, Department of Control Engineering and Information Technology, Budapest, 2009

[2] R. Hartley and A. Zissermann, *Multiple View Geometry in Computer Vision.* Cambridge University Press, 2003

[3] B. Lantos and L. Márton, *Nonlinear Control Of Vehicles and Robots.* London: Springer, 2011

[4] Zhengyou Zhang, *On the Epipolar Geometry Between Two Images With Lens distortion,* Proc. Int'l Conf. Pattern Recognition (ICPR), Vol. I, pages 407-411, Aug. 1996, Vienna

[5] Zhengyou Zhang, *A Flexible New Technique for Camera Calibration,* IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 22, No. 11, November 2000

[6] Heikkila, J. and Silven, O, *A four-step camera calibration procedure with implicit image correction.* CVPR97, 1997

[7] L. Lukács and B. Lantos, *Data Fusion and Primary Image Processing for Aircraft Identification.* Periodica Polytechnica, electrical Engineering and Computer Science, 56/3, pages 83-94, Budapest 2012

[8] Ed. Cary R. Spitzer, *The Avionics Handbook.* Boca Raton, CRC Press LLC. 2001

[9] L. Lukács, State Estimation Method For Aircraft Identification Purposes. 9-th IEEE Symposium on Applied Computational Intelligence and Informatics, pages 31-35, May 15-17, Timisoara 2014

[10] L. Lukács and B. Lantos, *Identification of the nonlinear dynamic model of sailplanes involving state estimation and image processing for actuator signal computation.* 12-th IEEE International Symposium on Intelligent Systems and Informatics, accepted for publication, September 11-13, Subotica 2014

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Bárdos Zoltán - Muhoray Árpád
bardos.zoltan@katved.gov.hu - muhoray.arpad@uni-nke.hu

A TELEPÜLÉSEK VÍZKÁR ELLENI VÉDEKEZÉSI FELADATAINAK VÁLTOZÁSA A MEGVÁLTOZOTT JOGSZABÁLYI KÖRNYEZETBEN

Absztrakt

Az ár-és belvizek veszélyeztetése miatt elengedhetetlen a lakosság élet-és anyagi javai, valamint a nemzeti vagyon védelme érdekében az árvízmentesítést, és a védekezést hatékonyan megszervezni. A vizek kártételei elleni védekezés sikeres végrehajtása érdekében, a vonatkozó jogszabályok a kor kihívásaihoz igazodva átdolgozásra kerültek. Az ár-és belvíz, valamint a helyi vízkárok elleni védekezés a vízgazdálkodásról szóló 1995. évi LVII. törvényben foglaltak szerint az állami szervek és a helyi önkormányzatok kötelessége, de a civil társadalomnak is megvan a szerepe és feladata. Írásunkban a jogszabályi változások alapján vizsgáljuk az önkormányzatok védekezési feladatainak gyakorlati megvalósulását. Elemezzük a 2013. évi árvíz alkalmával érintett Fejér Megyei települések védekezési tevékenysége során az új, és a módosult jogszabályok gyakorlati alkalmazását és beválását.

It is necessery to organise efficient defense systems to protect human life, material needs, and national property because of floods and inland-water threat. In case of the succesfull implemetation of flood defense, relevant laws have been adaptated to fit the present's challenge. According to the LVII.law about the water management in 1995 defensing flood, inland-water and local water damages is the duty of the state organizations and the local governments as well the civil community has a role in the protection as well. In this article we examine the practival fulfilment of the local government's protection tasks based on the law changes. We analyse the application and efficiency of the new and changed laws among the damaged settlements in Fejér county during the flood in 2013.

Kulcsszavak: *ár-és belvíz veszélyeztetettség, önkormányzati védekezés, vízkárelhárítás ~ risk of damage caused by flood and inland water, local governmental protection, water damage defence*

BEVEZETŐ

Magyarország földrajzi fekvése, medence jellege és az elmúlt évtized rendkívül szélsőséges hidrológiai eseményei következtében súlyos ár-és belvizek, valamint a helyi vízkárok alakultak ki hazánkban. Ezek a katasztrófák (2006-ban dunai és tiszai árvíz, 2010-ben borsodi árvíz és országos belvizek és helyi vízkárok, 2013-ban dunai árvíz) egyértelművé tették, hogy az emberi élet és az anyagi javak védelme, az élhető környezet biztosítása érdekében, az állami szerveken túl, a településeknek is jelentős feladataik vannak a vízkárelhárításban. Magyarország vízkár veszélyeztetettsége Európában egyedülálló, hazánk a Kárpát-medence magas hegyekkel körülhatárolt területének nagyjából a közepén helyezkedik el. A felszíni vizek 96 %-a külföldről érkezik az ország területére, ebből adódik, hogy a folyók vízgyűjtő területei döntően a határokon kívül helyezkednek el. Ennek az a következménye, hogy amikor nagy folyóink vízgyűjtőjén jelentős csapadék esik (pl. 2013. június eleje Duna németországi és ausztriai vízgyűjtője), az hazánkban súlyos áradást okozhat. A nyugat-európai óceáni, a dél-európai mediterrán és a kelet-európai kontinentális időjárás egyaránt kifejti hatását, ezért az időjárás szeszélyes, jelentős szélsőségek is előfordulnak. Az éghajlati és domborzati viszonyaink miatt hazánk területén lehulló csapadék (2010. május-júniusi időszak) következtében, bármely folyónkon és bármikor kialakulhatnak heves és tartós árvizek. A csapadékok nagysága, időbeli és térbeli eloszlása miatt, a nagy intenzitású esőket, zivatarokat, felhőszakadásokat követően helyi vízkárok alakulnak ki a településeken.[1]

Statisztikai átlagok alapján 2-3 évenként kisebb vagy közepes, 5-6 évenként jelentős, 10-12 évente pedig rendkívüli árvizek kialakulására lehet számítani hazánkban. Amíg, az árvizek által az ország területének mintegy 25%-a van közvetlenül veszélyeztetve, addig szélsőséges időjárási események következményeként hazánk bármely településén, az év bármely szakaszában keletkezhetnek elöntések és károk, veszélyeztetve a lakosok élet- és vagyonbiztonságát.[1]

A vizek kártételei elleni védelem magában foglalja - védművek építését, fenntartását, üzemeltetését és a védekezést -, amely a Vízgazdálkodásról szóló törvény[1] (továbbiakban: Vgtv.) szerint az állam, a helyi önkormányzatok, illetve a károk megelőzésében vagy elhárításában érdekeltek kötelezettsége.

Az árvíz elleni szervezett védekezési tevékenység a Vgtv. végrehajtására kiadott kormányrendelet[2] szerint két, jól elkülöníthető tevékenységcsoportra osztható, melyeket nevezik a védekezés szerkezeti és nem szerkezeti elemeinek is.

E feladatok egyrészt a védekezés műszaki feladatainak szervezésére, irányítására és ellátására irányulnak, másrészt a védekezés államigazgatási feladatait foglalják magukban. Jól láthatóan elkülönülnek a védekezés időszakában a védelmi létesítményeken folyó azon tevékenységek, amelyek a védművek ellenőrzését, védelmi teljesítőképességük megőrzését, azaz szükség esetén a terheléssel szemben lokálisan fellépő védőképességi hiányosságoknak a védekezési munkával, ideiglenes védelmi létesítmények kiépítésével való pótlását foglalják magukba. Ezt a feladatrendszert a Vízgazdálkodásról szóló törvény[3] szerint a vízügyi igazgatási szervek, azaz a Vízügyi Igazgatóságok, a vízgazdálkodási társulatok, a helyi önkormányzatok, az érdekelt tulajdonosok és az ingatlant egyéb jogcímen használók kötelesek elvégezni.

A védekezési feladatok másik része a védekezés államigazgatási feladatainak szervezésére, irányítására és ellátására irányul. E tevékenységen belül kettő időszakot különböztethetünk meg. Egyik időszak, amikor az ár-és belvízvédekezés végrehajtásához különleges jogrend nem került kihirdetésre, ekkor a vízügyi szervek irányításáért felelős miniszter végzi az országos irányítást.

[1] 1995. évi LVII. törvény a vízgazdálkodásról 16. § (1) bekezdés és a 35. § (1) b) pontja
[2] 232/1996. (XII. 26.) Korm. rendelet a vizek kártételei elleni védekezés szabályairól 1. § (2-3) bekezdés
[3] 1995. évi LVII. törvény a vízgazdálkodásról 16. § (4-6) bekezdés és a 34. § (1) pontja

Másik időszak, amikor a vízkárelhárítás végrehajtásához olyan szintű vezetésirányítási koncentráció szükséges, amely megvalósulhat egyrészt a katasztrófaveszély kinyilvánításával, illetve a veszélyhelyzet kihirdetésével, amely időszaki feladatokat a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény[4] szabályoz. Ekkor a védelmi igazgatás rendszere országos szinten működésbe lép és az államigazgatási feladat- és hatásköröket a külön jogszabályokban foglaltak szerint gyakorolják.

A cikkben hazánk ár-és belvíz veszélyeztetésből adódó vízkárelhárítási feladatok során vizsgáljuk a védekezés irányítási rendszerét, valamint az önkormányzatok helyét, szerepét és feladataikat. Kiemelten elemezzük a jogszabályok változását követően az önkormányzati védekezési tevékenység módosulását.

A VIZEK KÁRTÉTELEI ELLENI VÉDEKEZÉS SZABÁLYOZÁSA ÉS VÉGREHAJTÁSA

A fejezet címéből adódóan, a védekezési tevékenység egy összetett feladatrendszert foglal magában. A bevezetőben már leírtuk, hogy a Vgtv. meghatározza, a vizek kártételei elleni védekezéskor kiknek és milyen feladatokat kell végrehajtania. A törvényben a vízügyi igazgatási szervek, (vízügyi igazgatóságok) feladat és hatásköre részletesen megfogalmazásra került. Ezek többek között: a folyók vízkár-elhárítási célú szabályozása, a kettőnél több települést szolgáló vízkár-elhárítási létesítmények építése, - ezeknek, valamint az állam kizárólagos tulajdonában lévő védműveknek a fejlesztése, fenntartása, azokon a védekezés ellátása.

A jogszabály alapján a *vízügyi igazgatóságok* vízkárelhárítással összefüggő feladatai[5] között a vízkárelhárítás műszaki, igazgatási teendőinek irányítása, illetőleg ellátása mellett a védekezés tervezése és szervezése is szerepel. A továbbiakban a helyi önkormányzatok vízkár-elhárítási tevékenységével kapcsolatos szakmai irányítási feladatok, a vízkár-elhárítási és fejlesztési tervek elkészítéséhez és felülvizsgálatához adatok szolgáltatása, valamint a folyók menti nyílt ártéri települések esetében a vízkár-elhárítási tervek elkészítése és a meglévő tervek felülvizsgálata is feladatuk. A *vízitársulatok* vízkár-elhárítási tevékenységének szakmai irányítása szintén a feladatuk közé tartozik.

A Vízgazdálkodásról szóló törvény alapján a *helyi önkormányzatok* feladata, a legfeljebb két település érdekében álló védőművek létesítése, a tulajdonukban lévő védőművek fenntartása, fejlesztése és azokon a védekezés ellátása. A települések feladata, belterületen a patakok és csatornák áradásának, továbbá a csapadék- és egyéb vizek által okozott kártételek megelőzése érdekében kül-és belterületi védőművek építése, a védőművek fenntartása, fejlesztése és azokon a védekezés végrehajtása.

A törvény feladatokat fogalmaz meg az állami, vagy helyi önkormányzati feladatkörbe nem tartozó tevékenységek ellátása vonatkozásában is, itt az érdekelt *tulajdonosok*, illetve az ingatlant *egyéb jogcímen használók* feladatává teszi a vízkárelhárítási feladatokat.

A VÉDEKEZÉS IRÁNYÍTÁSI RENDSZERE

Országos szintű irányítás

Az ár-és belvízvédekezés, valamint a helyi vízkár-elhárítás államigazgatási feladat- és hatáskörével kapcsolatosan a szabályozást szintén tartalmazza a Vgtv.

A törvény konkrétan meghatározza az ár-és belvízvédekezés országos irányítási rendszerét, amely során kitér a rendkívüli védekezési készültség előtti és a rendkívüli védekezési készültség

[4] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról 3. § 9. pontja, 43. § aa)-ab) pontja

[5] 1995. évi LVII. törvény a vízgazdálkodásról 16. § (4-6) bekezdése

alatti irányítási rendre. A törvény alapján a saját szervezettel védekező települések által fenntartott műveken a védekezés műszaki feladatait a település közigazgatási határain belül – a vízügyi igazgatóságok szakmai irányításával – a polgármester (Budapesten a főpolgármester) a polgármesteri (főpolgármesteri) hivatal útján látja el.

Területi és helyi védekezés irányítása

Az árvíz- és belvízvédekezés, valamint a helyi vízkár-elhárítás államigazgatási feladat- és hatáskörét – a külön jogszabályban meghatározottak szerint – a megyei, fővárosi védelmi bizottság elnöke, illetőleg a polgármester, fővárosban a főpolgármester látja el. Ez a része a szabályozásnak tisztázza a területi és helyi szintű irányítási feladatok felelősségének megosztását, amely a védelmi igazgatás rendszerének az irányítási rendszerével megegyező az ár-és belvízvédekezések esetén is. Az irányítási jogkörből adódóan lakosságvédelmi intézkedések elrendelésére – kitelepítés, a kimenekítés, a visszatelepítés –, és az azzal kapcsolatos egyéb feladatok végrehajtására is jogosultak.

A vizek kártételei elleni védekezés részletes feladatait, módját és a vízügyi igazgatási szervek irányításáért felelős miniszter jogkörét a Kormány rendeletben állapítja meg[6].

Települési védekezés

A településeken az ár- és belvízvédekezéssel kapcsolatos államigazgatási feladatokat a polgármester (főpolgármester) irányítja, amelynek során a különleges jogrend kihirdetése előtt közreműködik az árvíz- és belvízvédekezési feladatok irányítására létrehozott területi bizottság jogszabályban meghatározott feladatainak végrehajtásában. Feladata a településen a közerők – ezen belül a polgári védelmi szervezetbe beosztottak és a közfoglalkoztatottak –, továbbá a védekezéshez szükséges anyagok, eszközök és felszerelések összeírása, nyilvántartása, szükség szerinti mozgósítása, továbbá a közerők – ezen belül a polgári védelmi szervezetbe beosztottak és a közfoglalkoztatottak – általános ellátása. Amennyiben kitelepítés elrendelésére kerülne sor, akkor feladata a kitelepítés, a kimenekítés, a visszatelepítés végrehajtásának szervezése. Gondoskodnia kell az élet- és vagyonbiztonság, valamint a mentés érdekében szükséges egyéb intézkedések megtételéről. Felelős a védekezésben részt vevők egészségügyi ellátásáért, továbbá a kitelepítés, a kimenekítés, a mentés és visszatelepítés során a járványok megelőzésével és elhárításával kapcsolatos intézkedésekért, az egészségügyi államigazgatási szerv közreműködéséért. Felelős az árvíz és belvíz által okozott, valamint a védekezéssel kapcsolatban keletkezett károkkal összefüggésben meghozott szükséges intézkedésekért.[1] Az előzőekből jól látható, hogy a konkrét feladatok a legalsó szinten jelentik várhatóan a legtöbb végrehajtandó feladatot.

A Vgtv. végrehajtási rendelete a vizek kártételei elleni védekezés szabályaival foglalkozik, tehát egy teljes önálló jogszabály dolgozza fel a témát. A cikk tartalmából adódóan a kormányrendeletből a vízkár elleni védekezés irányítási rendjét vizsgáljuk, azt is az államigazgatási és a műszaki irányítás szempontjából. Kiemelten kezeljük a területi és helyi szintű irányítási rendszert, hiszen ez érinti közvetlenül a településeken lakókat, valamint a védekezésben résztvevőket (beavatkozókat).

[6] 232/1996. (XII. 26.) Korm. rendelet a vizek kártételei elleni védekezés szabályairól

A VÍZKÁR ELLENI VÉDEKEZÉS MŰSZAKI IRÁNYÍTÁSI RENDJE

Országos irányítás[7]

A vízügyi igazgatási szervek védekezésre történő felkészülési feladatait, valamint az árvíz- és belvízvédekezéssel kapcsolatos tevékenységét - a készültség időszakában - a vízügyi igazgatási szervek irányításáért felelős miniszter (továbbiakban: miniszter) határozza meg. A miniszter és a Kormány az árvíz- és belvízvédekezés műszaki feladatainak országos irányítására Országos Műszaki Irányító Törzset (továbbiakban: Törzs) hoz létre.

Az egyes tárcák a védekezéssel összefüggő saját szakmai és államigazgatási feladataikat a Törzs mellett a miniszter által kinevezett állandó tárcamegbízottak koordinációjával és közreműködésével végzik.

Amennyiben a veszélyeztetés helyi polgári erők mozgósításával nem biztosítható, a miniszter kezdeményezi a katasztrófavédelemről, valamint a honvédelemről szóló törvény szerint – a honvédelemért felelős miniszter, a rendészetért felelős miniszter, a katasztrófák elleni védekezésért felelős miniszter útján – a honvédség, a rendvédelmi szervek és a Nemzeti Adó- és Vámhivatal hivatásos állománya közreműködését.

A miniszter feladata[8]

A rendkívüli védekezési készültség elrendeléséről és megszüntetéséről a miniszter dönt, ha veszélyhelyzet kihirdetésére nem kerül sor, a vizek kártételei elleni védekezés országos irányítása is a miniszter feladatkörébe tartozik.

A rendkívüli védekezési készültség tartama alatt a miniszter feladata a rendkívüli terhelésnek kitett védművek azonnali felülvizsgálatának elrendelése, a kritikus védműszakaszok és a szükséges beavatkozások meghatározása. Feladata még a megnövekedett vízügyi szakfeladathoz szükséges személyi létszám biztosítása, valamint az ártérre kivezetett vizek elszigeteléséről, a kártételek lehető legszűkebb körre korlátozásáról, a víznek a mederbe történő visszavezetéséről és az ezekkel kapcsolatos munkák elvégzéséről való gondoskodás és intézkedés a védekezés során megrongálódott védőművek azonnali helyreállítására.

A katasztrófavédelemről szóló törvényben meghatározott veszélyhelyzeti feltételek fennállása esetén a veszélyhelyzet kihirdetésének kezdeményezése történhet a vízügyi igazgató (a továbbiakban: VIZIG igazgató), a Törzs útján. A honvédelemről szóló, valamint az új katasztrófavédelmi törvény (Kat. tv.) szerint pedig a fővárosi, megyei védelmi bizottság (a továbbiakban együtt: védelmi bizottság) elnöke, a főpolgármester, valamint a polgármester a védelmi bizottság és a BM OKF főigazgatója útján tesz javaslatot a miniszternek a veszélyhelyzet kihirdetésének kezdeményezésére. Úgy a szakmai, mint a védelemigazgatási kezdeményezés esetén szükséges a széleskörű együttműködés és egyeztetés.

A Kormány feladata az árvíz- és belvízvédekezés során

Veszélyhelyzet kihirdetése esetén, a vizek kártételei elleni védekezés országos irányítása a Kormány feladata. Ha a Kormány az irányítási jogosítványai körébe tartozó döntésének meghozatalában átmenetileg akadályoztatva van, a miniszter köteles megtenni azokat az azonnali intézkedéseket, amelyek hiánya a sikeres védekezést veszélyeztetné.

A miniszter a megtett intézkedéseiről haladéktalanul tájékoztatja a Kormányt.

[7] 232/1996. (XII. 26.) Korm. rendelet a vizek kártételei elleni védekezés szabályairól 3. §
[8] 232/1996. (XII. 26.) Korm. rendelet a vizek kártételei elleni védekezés szabályairól 4. §

Területi irányítás, a megyei védelmi bizottság[9]

A vizek kártételei elleni védekezési területi bizottság feladat- és hatáskörét az illetékességi területén a megyei védelmi bizottság látja el. A védelmi bizottság az illetékes vízügyi igazgatóság vezetőjének javaslatára dönt a vizek kártételei elleni védekezés céljait szolgáló gazdasági és anyagi szolgáltatási kötelezettségek tervezéséről és igénybevételéről. Ezek zömmel az új Kat. tv.-ben szereplő polgári védelmi kötelezettség alapján kerülnek lebiztosításra az állampolgárok, valamint a gazdálkodó szervezetek részéről, igényvételüket a polgármester beosztó határozata szabályozza.

A védelmi bizottság a szervezeti-és működési szabályzata és tervei alapján, a saját munkaszervezetének (katasztrófavédelmi operatív munkacsoport) bevonásával gondoskodik a védekezés területi szintű összehangolásáról. A védelmi bizottság tagja a működési terület szerinti VIZIG igazgatója is. Ha a kialakult védelmi helyzet a vízügyi igazgatóság területén több megyét érint, a vízügyi igazgatóság gondoskodik arról, hogy az egyes védelmi bizottságokban intézkedésre jogosult képviselője legyen (szakaszmérnök). A védelmi bizottság operatív munkaszervezetének a vizek kártételei elleni védekezéssel kapcsolatos működését a VIZIG igazgató, vagy a katasztrófavédelmi igazgató javaslatára a védelmi bizottság elnöke rendeli el és szünteti meg.

A védekezés műszaki feladatainak helyi irányítása[10]

A műszaki irányítás szempontjából három időszakot különböztet meg a jogszabály. Első az I. - III. védekezési fokozatok elrendelése esetén a védekezés, második a rendkívüli védekezés időszaka, harmadik pedig a veszélyhelyzet kihirdetését követő védekezés.

A kettőnél több települést szolgáló vízkár-elhárítási védműveken, valamint az állam kizárólagos tulajdonában lévő védműveken:

- az I., II. és III. védekezési készültség tartama alatt a védekezés és a vízkárelhárítás feladatainak ellátása a VIZIG igazgató felelőssége,
- a rendkívüli védekezési készültség tartama alatt, ha veszélyhelyzet kihirdetésére nem kerül sor, a VIZIG igazgató vagy a miniszter által kirendelt megbízott irányít,
- a veszélyhelyzet idején a miniszter által kirendelt megbízott végzi az irányítást.

A helyi önkormányzati tulajdonban lévő védőműveken:

- az I., II. és III. védekezési készültség tartama alatt a polgármester vagy a polgármester által kijelölt és a VIZIG igazgató által jóváhagyott védelemvezető,
- a rendkívüli védekezési készültség tartama alatt, ha veszélyhelyzet kihirdetésére nem kerül sor, a polgármester vagy a vízügyi igazgatási szervek irányításáért felelős miniszter által kijelölt személy,
- a veszélyhelyzet időtartama alatt a miniszter által kijelölt személy látja el.

A vízitársulat üzemeltetésében lévő védőműveken, ha az nem tartozik az önkormányzati tulajdonba:

- az I., II. és III. védekezési készültség tartama alatt a vízitársulat intéző bizottsága által kijelölt és a VIZIG igazgató által jóváhagyott személy,
- a rendkívüli védekezési készültség tartama alatt, ha veszélyhelyzet kihirdetésére nem kerül sor, a miniszter által kijelölt személy,
- a veszélyhelyzet időtartama alatt a miniszter által kijelölt személy látja el.

[9] 232/1996. (XII. 26.) Korm. rendelet a vizek kártételei elleni védekezés szabályairól 7. §
[10] 232/1996. (XII. 26.) Korm. rendelet a vizek kártételei elleni védekezés szabályairól 6. §

A védekezés műszaki feladatainak helyi irányítója a védekezés végrehajtására alkalmas védekezési szervezetet hoz létre, amelyet a magasabb védekezési fokozatban is alkalmazni kell, a vizek kártételei leküzdése érdekében kezdeményezheti a polgári védelmi szervezetek alkalmazását. Ilyenkor a köteles polgári védelmi szervezetek mellett az önkéntes polgári védelmi szervezetek is jelentős létszámban bevonhatók a védekezésbe, ahogy történt ez a 2013-as dunai árvíz alkalmával.

Az árvízvédelmi és belvízvédelmi szakaszokon a védekezés műszaki feladatainak irányításával szakasz-védelemvezetőt kell megbízni.

Összefüggő árvízvédelmi műveken és belvízvédelmi rendszerekben a különböző védekező szervek műszaki tevékenységének összehangolása a vízügyi igazgatóság (a továbbiakban: VIZIG) feladata.

A védelemvezető feladatai

A megbízott védelemvezető (szakasz-védelemvezető) köteles a védekezés érdekében szükséges minden intézkedést megtenni és a kormányrendeletben meghatározott feladatokat végrehajtani[11]. Ezek magukban foglalják mindazon műszaki feladatokat, amelyek a védműveknél jelentkező káros árvízi jelenségek megszüntetésére irányulnak. A továbbiakban, feladata a mentesített területre betört káros vizek elvezetése, valamint a védekezéshez szükséges munkaerő biztosítása is.

Az előzőekben foglaltakon kívül a vízügyi igazgató feladatai közé tartozik, a folyamatos kapcsolattartás a katasztrófavédelemmel, az érintett települések polgármestereivel, a vízitársulatokkal és a környezetvédelmi felügyelőséggel. A nagyobb kár elhárítása érdekében intézkedik és meghatározhatja a belvizek levezetésének sorrendjét, a befogadóba vezetését ideiglenesen korlátozhatja vagy szüneteltetheti. Rendkívüli védekezési készültség időszakában, a védelmi bizottság elnökének egyetértésével, a Törzs útján vízkár-elhárítási célú tározó igénybevételére javaslatot tehet a miniszternek.

A helyi szintű védekezés során a polgármester, illetőleg az általa kijelölt védelemvezető a védekezés műszaki feladatait a vízügyi igazgatósággal együttműködve látja el. A védekezés felelős vezetői egymást kölcsönösen tájékoztatják.

A TERÜLETI IRÁNYÍTÁSI RENDSZER MŰKÖDÉSE A VÉDEKEZÉSI KÉSZÜLTSÉGI FOKOZATOKBAN ÉS A MŰSZAKI IRÁNYÍTÁS FELADATAINAK ELLÁTÁSA SORÁN[12]

A védekezési készültségi fokozatokban az egyértelmű alá és fölé rendeltség nagyon fontos az egységes védekezés végrehajtása érdekében. Ennek megfelelően az alá fölé rendeltségi viszonyok a jogszabályban leszabályozásra kerültek, hogy félreértések még véletlenül sem legyenek.

A polgármester vagy az általa kijelölt védelemvezető a Helyi Védelmi Bizottság elnöke útján közvetlenül a Megyei Védelmi Bizottság elnökének, az önkormányzathoz kirendelt vízügyi műszaki irányító közvetlenül a vízügyi igazgatónak van alárendelve.

A vízügyi igazgató a Törzs útján a miniszternek van alárendelve.

A vízitársulat védelemvezetője a vízügyi igazgatóság szakasz-védelemvezetőjének, a vízügyi igazgatóság szakasz-védelemvezetője vízügyi igazgatónak van alárendelve.

Rendkívüli védekezési készültség időszakában, amikor a veszélyhelyzet kihirdetésére nem kerül sor, a vízügyi igazgató vagy a miniszter által kirendelt megbízott, továbbá a polgármester, főpolgármester vagy az általa kijelölt védelemvezető a Törzs útján a miniszternek van alárendelve.

[11] 232/1996. (XII. 26.) Korm. rendelet a vizek kártételei elleni védekezés szabályairól 15. §
[12] 232/1996. (XII. 26.) Korm. rendelet a vizek kártételei elleni védekezés szabályairól 16. §

Az új Kat. tv. alapján a *helyi védekezés* irányításában az új irányítási rend elemeként veszélyhelyzetben az irányítást a településen a polgármestertől a katasztrófavédelmi területi szerv vezetője által kijelölt személy veszi át. [7]

A MÓDOSULT JOGSZABÁLYOK ALKALMAZÁSA A 2013. ÉVI DUNAI ÁRVÍZ ALKALMÁVAL ÉRINTETT FEJÉR MEGYEI TELEPÜLÉSEK VÉDEKEZÉSI TEVÉKENYSÉGE SORÁN

Az árvízi védekezésre történő felkészülés

2013. május 30. és június 3. közötti négy napon a Duna és mellékfolyói vízgyűjtőjén a bajor és osztrák területeken területi átlagban is igen nagymennyiségű csapadék hullott. Elsősorban az Inn vízrendszerének igen heves áradása következtében, a Dunán legnagyobb vízállás (továbbiakban: LNV) körüli vagy azt is meghaladó vízszintek alakultak ki. Az előrejelzések szerint, a Duna magyarországi szakaszán minden idők legnagyobb árvízi védekezésére kellett felkészülni. Hazánk területén a Duna felső szakaszán, már június 4-től Nagybajcsnál III. fokú árvízi védekezés lett elrendelve.

A védekezésre történő felkészülés érdekében június 3-án összehívásra került Fejér Megyében a Megyei Védelmi Bizottság (továbbiakban: MVB) Katasztrófavédelmi Operatív Munkacsoportja, ahol a résztvevők értékelték a várható helyzetet. Az MVB katasztrófavédelmi elnök-helyettesének javaslatára, az MVB rendkívüli ülését június 4-re összehívta az MVB elnöke. Az ülésen a várható árvízi helyzetre történő felkészülés érdekében a védekezésben érintett szervezetek (Közép-dunántúli Vízügyi Igazgatóság, Fejér Megyei Katasztrófavédelmi Igazgatóság) tájékoztatóját követően, a lakosság védelméhez szükséges védekezési feladatok megkezdéséhez elengedhetetlenül fontos döntéseket a bizottság meghozta. A kiadott MVB határozatban foglaltak helyi szintű végrehajtására, az árvíz által érintett járási Helyi Védelmi Bizottságok (továbbiakban: HVB-ok) (Dunaújváros, Martonvásár) június 5-én és június 6-án megtartották üléseiket. A bizottsági ülésekre meghívottak körét úgy alakították ki, hogy a lehető legszélesebb körben tudják a védekezési feladatokat megbeszélni és a döntéseket meghozni, valamint mindenki jelen legyen, akinek a HVB feladatot határozhat meg. Az üléseken elfogadott határozatok részletesen tartalmazták a védekezésben résztvevő szervezetek és a települések feladatait, melyet a védekezésben résztvevők és a települések azonnal megkaptak.

Ezek alapján kezdődtek meg az árvíz által érintett településeken a védekezési munkálatok. A megye vonatkozásában a dunai árvíz kettő helyi védelmi bizottság hét települését érintette, amelyből öt folytatott védekezést. A Martonvásári HVB illetékességi területén Ercsi város, a Dunaújvárosi HVB területén Adony, Kulcs, Rácalmás, Baracs és Kisapostag települések, valamint Dunaújváros megyei jogú város.

Az árvízi előrejelzések alapján a Duna Fejér Megyei szakaszán az LNV-t meghaladó árhullámon bekövetkező tetőzésre kellett felkészülni, a védekezésben résztvevőknek, a vízügyi szakembereknek és az érintett önkormányzatoknak. A megyei dunai szakaszon kettő vízmérce található Adonyban és Dunaújvárosban, az itt mért értékek adják a szükséges információkat. Az árvíz által érintet területen lévő települések polgármesterei és a KÖDU VIZIG szakemberei ismerik a terület elöntés általi veszélyeztetettségét, ez nagy segítséget jelentett a felkészülésben.

A Fejér megyei árvízi felkészülési feladatok koordinálása és irányítása céljából a Fejér Megyei Katasztrófavédelmi Igazgatóság (FMKI) igazgatója elrendelte a megyei Veszélyhelyzet-kezelési Központ aktivizálását. A Központ működését 2013. június 5-én 14.00-kor kezdte meg az FMKI bázisán folyamatos 24 órás váltásban. A HVB-ok székhelyén szintén elrendelésre került a folyamatos ügyeleti szolgálat a védekezési feladatok irányításához.

A védekezési feladatok végrehajtása

Az árhullám megyei Duna szakaszra érkezése előtt a védelmi igazgatás rendszere időben meghozta a területi és helyi szintű döntéseket, amely alapján megkezdődtek és az árhullám megérkezésekor folyamatosan folytak a települési védekezések. A döntések végrehajtásához szükség volt a hét érintett településen a polgármesterek megfelelő hozzáállására, valamint a katasztrófavédelmi igazgatóság állományából kijelölt védekezési irányítókra, akiket az MVB elnöke a katasztrófavédelmi igazgató javaslata alapján jelölt ki[13]. A Közép-dunántúli Vízügyi Igazgatóság az állami védvonalakon végzett védekezési feladatai mellett minden településre biztosított szakembert a védekezés műszaki feladatainak támogatására, ez a védekezés szakmaiságát nagymértékben javította és Kisapostag településen a kazettás védekezést így lehetett szakszerűen megvalósítani.

A védelmi igazgatás helyi szervezete és rendszere még új volt, a polgármesterek és a védelmi bizottságok számára is[14]. A települések tökéletesen és pontosan hajtották végre a HVB határozataiban foglalt utasításokat. A települési védekezési feladatok hatékonyságát növelte a katasztrófavédelmi vezetőnek kijelölt katasztrófavédelmi tisztek alkalmazása a településeken. A települési vezetők megelégedettséggel szóltak az álaluk végzett munkáról. Kiemelték, hogy figyelembe vették és felhasználták a helyben meglévő ismereteket.

A helyszínen a katasztrófavédelmi tisztek, a polgármesterek, a vízügyi szakemberek minden esetben szakmailag korrekt módon végezték feladataikat, ennek eredménye lett a védvonalak megbízható kiépítése és a lakott ingatlanok időben történt kiürítése. A településeken védekező hivatásos szervezetek, önkéntesek, közfoglalkoztatottak munkájának szervezése, feladatok kiosztása ellátásuk megszervezése magas fokú koordinációt és szervezettséget igényelt. Ezt a feladatot ebben a szervezeti formában lehetett a leghatékonyabban és eredményesebben végrehajtani.

A Duna adonyi szelvényében a vízállás 2013. június 8-án 10 órakor elérte a III. fokú árvízvédelmi készültséghez tartozó 700 cm-es vízállást, ezért ekkortól III. fokú árvízvédelmi készültséget rendelt el a vízügyi igazgató a 04.04. Adony–Ercsi árvízvédelmi szakaszra.

Az árhullám a Duna megyei szakaszán június 10-én délelőtt 10.00-kor haladta meg az LNV-t, (adonyi vízmércénél 762 cm-en, eddigi LNV 739 cm volt) ekkor a Kormány 191/2013 (VI.10.) számú határozatában 2013. június 10-én 12 órától *veszélyhelyzetet* hirdetett ki Fejér megyében a Martonvásári járás és a Dunaújvárosi járás közigazgatási területére. Ennek megfelelően elrendelésre került a megye dunai árvízvédelmi szakaszára a rendkívüli árvízvédelmi készültség.

Védekezési feladatok végrehajtása veszélyhelyzet idején

A veszélyhelyzet kihirdetését követően a katasztrófavédelmi tisztek átvették a védekezés irányítását[15], a települések vezetői a polgármesterek továbbra is segítségükre voltak és biztosították a szükséges erőforrásokat. A védekező és helyreállítást végző településeken, a helyszínen lévő katasztrófavédelmi tisztek és a települések polgármestereinek a kapcsolata megfelelő volt és jól segítette a hatékonyságot és eredményességet.

A megújult védelmi igazgatás rendszere teljes vertikumában először működött megyénkben kettő héten keresztül, amely lehetőséget teremtett arra, hogy minden szegmensének a működéséről tapasztalatot szerezzünk. Az MVB határozatban foglalt feladatok lejuttatását és annak végrehajtásának irányítását és ellenőrzését területi szinten az MVB Katasztrófavédelmi Operatív Munkacsoport végezte. A kettő HVB-nál szintén működött az operatív

[13] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról 13.§
[14] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről 27. §-28. §
[15]2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról 46.§ (3) bekezdés

munkaszervezet, akik a helyi feladatok koordinálását hatékonyan végezték. Települési szinten a katasztrófavédelmi tisztek a polgármesterekkel és a helyszínen lévő vízügyi szakemberekkel végezték a védekezés irányítását. A védművek kiépítését a településeken lakók, érkező önkéntesek, a hivatásos, az önkormányzati tűzoltók, az önkéntes tűzoltó egyesületek állománya végezte folyamatosan. Az önkéntesek szervezésének koordinálását a katasztrófavédelmi igazgatóság végezete.

A védekezési feladatok során a HVB-okkal és a településekkel a kapcsolattartás infokommunikációs eszközökkel a megyei katasztrófavédelmi operatív munkacsoport részéről folyamatos volt. Az MVB és HVB-ok által meghozott döntések (kiadott határozatok) aláírást követően azonnal megküldésre kerültek a településekhez e-mail-on keresztül. A jelentések a települések és a HVB-ok operatív munkacsoportjai között elektronikus úton, valamint szükség szerint telefonon azonnal megtörténtek. Az MVB katasztrófavédelmi operatív munkacsoportjába a jelentések elektronikus formában kerültek megküldésre, szükség esetén telefonon. A katasztrófavédelem és a rendőrség helyszíni irányításban résztvevő állományával EDR rádión keresztül valósult meg az operatív irányítás.

A KÖZÉP-DUNÁNTÚLI VÍZÜGYI IGAZGATÓSÁG VÉDEKEZÉSI TEVÉKENYSÉGE

A hatályos jogszabályok alapján a KÖDU VIZIG az állami fővédvonalakon felel a védekezés megszervezéséért és végrehajtásáért. A KÖDU VIZIG védelmi törzsének felállítását követően (megyénkben a törzs az Ercsi védelmi központban működött) folyamatosan kapcsolatot tartott az Országos Műszaki Irányító Törzzsel, a társ vízügyi igazgatóságokkal, a megyei és helyi védelmi bizottságokkal, a katasztrófavédelemi igazgatósággal és az önkormányzatokkal.

Folyamatosan készítettek munkatársaiknak az igazgatóság működési területére vonatkozó tájékoztatókat, jelentéseket és vízállás előrejelzéseket. A védelmi szakaszokon az elrendelt fokozatnak megfelelő 24 órás figyelő-jelentő szolgálatot működtettek, 2 óránkénti vízállásjelentéssel. A szakemberek folyamatosan figyelték a töltések állapotát, a megjelenő fakadóvizeket és a lehetséges árvízi jelenségeket. Egyes szakaszokon több helyen tapasztalhatóak voltak az ún. árvízi jelenségek pl. fakadóvíz, talpszivárgás. A jelenségek helyét az őrszolgálatot ellátó szakemberek rögzítették, illetve zászlóval kijelölték és állapotukat folyamatosan figyelemmel kísérték.

A Duna projekttel érintett területekre külön műszaki irányítókat jelöltek ki. Váli víz jobb partján fóliás rézsűvédelem került kialakításra a töltés védelme érdekében. A dunai fővédvonalon az árvízi jelenségek kezelésén túl árvízi védekezési feladatokra nem volt szükség, mivel a védvonal jól kiépített és a műtárgyak állapota a karbantartásnak köszönhetően jó.

Az adonyi szivattyútelepen a szivattyúk - a zsilip lezárását követően - napi több órán át dolgoztak. Június 9-től kialakításra került Ercsi védelmi központnál az állami homokzsáktöltő hely, amely a homokzsák ellátást tudta biztosítani. Az árvíz által leginkább veszélyeztetett települések közül Kisapostag, Rácalmás, Adony, Ercsi önkormányzatok részére műszaki irányítókat rendeltek ki, akik folyamatos tájékoztatást adtak a kialakult és várható hidrológiai helyzetről és segítséget nyújtottak a védművek kiépítésének műszaki kérdéseiben. A homokzsákokból felépített védművek állapotát folyamatosan figyelemmel kísérték, szükség esetén intézkedtek a megerősítésükre.

AZ ÁRVÍZI VÉDEKEZÉS LOGISZTIKAI BIZTOSÍTÁSA

A védekezés sikeres és eredményes végrehajtásának elengedhetetlen feltétele, hogy a szükséges *anyagok, eszközök és felszerelések*, az adott helyen a szükséges mennyiségben, időben rendelkezésre álljanak. Ennek a megszervezése és biztosítása összetett, komoly feladatot jelentett. Ennek végrehajtását a települések polgármesterei, a vízügyi igazgatóság, a katasztrófavédelmi igazgatósággal együttműködve a jogszabályok alapján hajtották végre. Minden településen a védekezéshez szükséges *homokzsák* mennyiséget a KÖDU VIZIG rendelkezésre bocsájtotta, a települések szállító eszközöket biztosítottak az elszállításukhoz, a katasztrófavédelmi igazgatóság a készleteiből szintén tudott homokzsákot biztosítani a települések részére. A védekezési munkálatok során a megye területén mindösszesen 113.400 db homokzsák került beépítésre.

A települések részére a katasztrófavédelmi igazgatóság már a védekezés megkezdése előtt megadta a *homokbányák* listáját, ahonnan a szükséges mennyiségű és minőségű homokot biztosították. A védekezésben résztvevők *étkezési* ellátását, a települési önkormányzatok, valamint a karitatív szervezetek bevonásával valósították meg. Fontos volt a *kéziszerszámok*, *munkaeszközök*, *védő és esővédő*, valamint a *világító felszerelések* biztosítása is.

Speciális feladat volt a védekezés *pénzügyi elszámolása* és ennek megszervezése, amely a hatályos a vis maior támogatás felhasználásának részletes szabályairól szóló 9/2011. (II. 15.) Korm. rendelet alapján történt meg. Ez komoly feladatot jelentett az önkormányzatoknak, mivel a *védekezési napló* pontos vezetésén túlmenően, valamennyi szolgáltatásról és az ellátás érdekében megvásárolt anyagról számlákra volt szükség és a védekezés során azok szükségességét a katasztrófavédelmi igazgatóság jelen lévő munkatársának igazolnia kellett. A védekezési feladatok során felmerült tényleges költségeiket, a pályázat beadását és elbírálását követően települési önkormányzatok megkapták.

A cikk terjedelméből adódóan részletesen az árvízi védekezés feladatainak módosult jogszabályi hátterével, valamint a 2013. évi dunai árvíznél a Fejér Megyében végrehajtott védekezési feladatok kérdéskörével foglalkoztunk. A jogszabályi háttér változásának vizsgálatával a célunk az volt, hogy a védekezés feltételeire milyen módon hatott a jogszabályok módosulása. Ez azért is volt fontos, mivel az Állami Számvevőszék a 2010. évi borsodi árvíz után az akkor hatályos jogszabályok tükrében vizsgálatot folytatott le „a természeti katasztrófák megelőzésére és elhárítására, következményeik felszámolására kialakított rendszer ellenőrzéséről”. A vizsgálatról 2011-ben készült jelentés[16], amelyben több területen tettek megállapításokat és fogalmaztak meg javaslatokat a települési polgármesterek, a katasztrófavédelem, a védelmi igazgatás és a vízügy vízkárelhárítás feladatainak jobbítására. Észrevételezték az önkormányzatok felkészültségének problémáját a hatékony katasztrófa elhárításra, ennek a központi szabályozásának a hiányát, ezen túl a védekezési tervek hiányát. A vízügyi igazgatás területén problémaként merült fel, hogy mikortól állami feladat a vízkárelhárítási tevékenység és kinek milyen védekezési tervekkel kell rendelkeznie. A védelmi igazgatás területén szintén többszörösen áttételesen megjelenő feladatokat fedeztek fel, amelyet javasoltak egyszerűsíteni. A jelentésben összegzett következtetésként a katasztrófavédelem és a károk felszámolásának vonatkozásában az állami szerepvállalás erősítését fogalmazták meg. [7]

[16]Állami Számvevőszék 1107 jelentése a természeti katasztrófák megelőzésére és elhárítására, következményeik felszámolására kialakított rendszer ellenőrzéséről

ÖSSZEGZÉS

Hazánkban a szélsőséges időjárási és vízjárási adottságok következtében évszázados küzdelem folyik a vizek kártételei ellen. Az utóbbi években a védekezés folyamatos operatív feladatot adott a katasztrófavédelemnek, a vízügyi szerveknek, a helyi önkormányzatoknak és a lakosságnak. A települések és az egyes emberek kiszolgáltatottságát a vizek kártételei ellen csakis közös összefogással lehet elfogadható mértékűre csökkenteni. Ehhez szükséges az állami, önkormányzati szerveknek, vízi társulatoknak és az egyes embereknek is a maga területén lépéseket tenni. A védekezési feladatok sikeres végrehajtásához szükséges egy egységes irányítási rendszerben tevékenykednie az előzőekben szereplő valamennyi résztvevőnek. A védekezési feladatokra történő felkészüléshez, a sikeres és eredményes védekezés végrehajtásához minden résztvevőnek ismernie kell a felelősségét és a feladatát.

Az alaptörvény elfogadásával, valamint a védelmi igazgatás, katasztrófavédelem és a vízkárelhárítási feladatok területére vonatkozó sarkalatos törvények elfogadásával 2011-ben a jogszabályi alapok megteremtődtek a védekezés végrehajtásához.

A cikkben a vízkárelhárítási feladatok megváltozott jogszabályi környezetéből indultunk ki. A vízkárelhárítás azonban nem önmagában való tevékenység, hanem szervesen érinti a települési önkormányzatokat, a katasztrófavédelmi feladatokat, a védelmi igazgatás rendszerét is. Ebből adódóan a jogszabályi környezet módosulása területén szükséges volt vizsgálnunk az adott területeket szabályozó törvényeket és végrehajtási rendeleteiket is. A védekezési feladatok irányítása és a kár felszámolása egy vízkár bekövetkezésekor nagyban függ a káresemény nagyságától, az elrendelt védekezési fokozattól. Ennek megfelelően egy-egy védekezéskor a kárfelszámolásba bevont szervezetek változnak, mindig a várható kockázatokkal arányos irányító, erő és eszköz kerül kijelölésre és igénybevételre.

Az írásunk második részében a 2013-ban bekövetkezett évszázad dunai árvizénél a Fejér Megyében végrehajtott védekezési feladatoknál vizsgáltuk a módosult jogszabályok alkalmazását. Megállapítottuk, hogy a jogszabályok alapján megváltozott a vízügyi védekezési irányítás rendszere, amely egy egységes rendszerben összpontosul. A védekezési fokozatok emelésével a *katasztrófaveszély* megállapításával a védelmi rendszer lehetőségei kibővültek és szélesebb kör vonható be a feladatokba. Ezt nagyon jól példázza a 2013-évi dunai árvíz, amikor a védvonalak megerősítése már jóval az árhullám megérkezése előtt megtörtént. A különleges jogrend időszakában, *a veszélyhelyzet* adta jogszabályi lehetőségek keretei között, a védekezés minden feltétele biztosított volt. A védelmi igazgatás rendszere jól vizsgázott és bizonyította, hogy a képes feladatát maximálisan végrehajtani az adott keretek között.

Cikkünkben a vizek kártételei elleni védekezés jogi szabályozásának megújulását és a gyakorlatban történő alkalmazását vizsgáltuk. Hazánk földrajzi adottságaiból adódóan és az időjárás várható szélsőségesebbé válásának következtében, az elkövetkező években is számolhatunk kisebb-nagyobb árvizek, vízkárok kialakulásával. A hatályos jogszabályok alapján az állami szerepvállalás elsődlegességével, az árvízi védekezés sikeresen megvalósítható.

Felhasznált irodalom

[1] Bárdos Zoltán: A területi rendeltetésű árvízvédelmi komplex polgári védelmi szervezetek szakkiképzésének szerepe az önkormányzati ár-és belvíz elleni védekezésben Hadmérnök V. Évfolyam 3. szám (264-280. oldal) http://hadmernok.hu/2010_3_bardos.pdf letöltés ideje: 2014. 05.28.

[2] Muhoray Árpád: A katasztrófavédelem aktuális feladatai, Hadtudomány on-line 2012. IV. szám. www.mhtt.eu/hadtudomany/2012/2012_e_Muhoray_Arpad.pdf

[3] 1995. évi LVII. törvény a vízgazdálkodásról

[4] 232/1996. (XII. 26.) Korm. rendelet a vizek kártételei elleni védekezés szabályairól

[5] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

[6] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről

[7] Állami Számvevőszék 1107 jelentése a természeti katasztrófák megelőzésére és elhárítására, következményeik felszámolására kialakított rendszer ellenőrzéséről http://www.asz.hu/jelentes/1107/jelentes-a-termeszeti-katasztrofak-megelozesere-elharitasara-kovetkezmenyeinek-felszamolasara-kialakitott-rendszerek-ellenorzeserol/1107j000.pdf letöltés ideje: 2014. 05.28.

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Halász László - Lucas Grégory
gregory.luc4s@gmail.com

REVIEW OF AIRBORNE LASER MEASUREMENTS OF CHEMICALS AND RADIATIONS

Abstract

This article aims at reviewing the existing laser measurement technologies and methods applied in the airborne detection of radiations and chemicals. The first part introduces the main concepts and provides the reader with a general orientation. Each of the following chapters aim at describing a measurement method, its capacities and fields of application. Differential absorption LiDAR (DIAL), Tunable Diode Laser (TDL) spectrometry are successively considered with the measurement of chemicals. Concerning the ionizing radiation measurements, the bibliographic research demonstrated that active laser airborne measurements are presently not applied, neither have they been tested. Nevertheless, some stand-off measurement techniques under development are reviewed and their adaptations to airborne measurement are considered. Spectroscopic measurement of radiation-induced radical, active detection by the detection of frequency modulation and standoff detection of alpha radiation via the measurement of energy absorbed by excited state molecules are introduced.

Jelen cikk célja a meglévő lézeres mérési technológiák és módszerek bemutatása, amelyeket a vegyi anyagok és sugárzások légi felderítésében alkalmaznak. Az első rész áttekinti a legfontosabb fogalmakat, és az olvasónak egy általános orientációt nyújt. A következőkben minden egyes fejezet leírást ad egy mérési módszerről, annak teljesítményéről és alkalmazási területeiről. A vegyi anyagok mérésére áttekintjük a differenciális abszorpciós LIDAR (DIAL), állítható lézer dióda (TDL) spektrometria módszereket. Az ionizáló sugárzás méréseinek vizsgálata során a bibliográfiai kutatások kimutatták, hogy az aktív légi lézeres méréseket jelenleg nem alkalmaznak, nem is tesztelték még korábban. Ugyanakkor a kutatók egyéb fejlesztés alatt álló mérési technológiákat és azok távérzékelési alkalmazásainak lehetőségeit vizsgálják. Elsőként a sugárzás által kiváltott szabad gyök spektroszkópiai mérését, majd a frekvencia moduláció érzékelésének aktív felderítését, végül a gerjesztett molekulák által elnyelt energia mérésével az alfa sugárzás távoli felderítését mutatjuk be.

Keywords: *Airborne, laser measurement, DIAL, LIDAR, radiological material, ionizing radiation.*

INTRODUCTION

In the second half of the twentieth century, awareness arose about the presence of chemicals in the atmosphere and their consequences. Scientists discovered that heavy industries and more generally human activities hugely impact on the biotopes via the transfers of part of the chemicals in the atmosphere, thus generating air quality concerns but also environmental changes.

At the local scale for example, high concentration of particles and chemicals in the air pose seasonal pollution problems in the capitals and dense urban areas (ozone pollution peaks in winter and summer). Pollution from industrial plumes or transmission exhaust gases became a concern for the public health. The air pollution generated in the largest cities also impact at the regional scale by transfer. Last but not least, global concerns are also in scope. Greenhouse gases (like H_2O, CO_2, CH_4, N_2O, O_3) generating an increase of the average temperature on Earth. Increase of desertification, extreme meteorological phenomena, seasonal calamites in agriculture, the melting of the pole ice, the average mean sea level, the loss of arable land, etc. are nowadays proven and visible consequences of the climate change. A second example illustrates very well how a new concern can appear and how in time apprehension of the phenomenon (through adequate measurement methods and response) is useful to limit global negative impacts. In 1985 scientists discovered the stratospheric ozone depletion over the Antarctic. The various measurement methods applied demonstrated the large scale and fast dynamic of the phenomenon and allow the identification of the origin of the problem: man-made organohalogen compounds, especially chlorofluorocarbons (CFCs) and bromofluorocarbons. In 1996 all countries of the world finally agreed to ban the uses of the CFCs and industrial production of CFCs was stopped.

Worrying environmental changes are arising and incredible challenges are to come. Our ability to live in favorable environmental circumstances in the second half of the 21st century will depends on the scientific capacity to react and to which extent the society will be able to adapt itself and evolve. As a consequence, understanding how those complex mechanisms are working, how much extent and dynamics will be necessary to react. The understanding of the phenomenon whether they are local, regional or global requires advanced methods for their measurements. In the mid-60s the development of computer technologies with transistor-based machines increased the reliability. Computers were smaller, faster, and cheaper to produce and required less power. Later in the 70s, the integrated circuit technology and the subsequent creation of microprocessors further decreased size and cost and further increased speed and reliability of computers and triggered the development of airborne measurement methods. Airborne measurements are powerful tools in the sense they allow three dimensional spatial and temporal mapping.

This article aims first at considering how laser technologies can be used for the aerial measurement of chemicals. In a second part radiological airborne measurements are considered.

REMOTE SENSING OF CHEMICALS IN THE AIR

Differential absorption lidar (DIAL) technique

Short historical introduction

The methodology of DIAL has been developed in the late 1960s and 1970s. [1] DIAL was first employed in 1966 for remote measurement of water vapor (H_2O). The first aerial measurements with DIAL technique were realized by Schotland in 1974. [2] Since, differential absorption LiDAR systems have evolved significantly and have been used for the measurement of ozone, water vapor and aerosols from aircrafts for over 34 years. [3] They have yield new insights into atmospheric chemistry, composition and dynamics in large-scale field experiments. [3]. In 1994, the LITE experiment successfully managed a space-base LIDAR measurement mission

completing the ground, air and space cycle. [4] A LIDAR system was carried by the space shuttle "Discovery" for 9 days. [5] The latest space development was related to the CALIPSO satellites, that carried a LIDAR system for the global measurement of clouds and aerosols. [6]

Year	Type	Measurement of species
Late 60s	Ground based	Water vapor
Late 70s early 80s	Airborne	Aerosols, clouds, winds
1978	Airborne	Tropospheric ozone
1980	Airborne UV	Ozone profile
1982	Airborne	Water vapor
1994	Space borne	Ozone, water vapor, aerosols
2006	Space borne	Cloud-aerosol

Tab.1. Summary about historical developments of DIAL

Working principle

Differential absorption LIDAR is a remote sensing technique uses two laser beams in different wavelengths that can be reflecting from any field objects and the active beam can be absorbed in the investigated gas so the type and average concentration of the gas in the air can be determined. [4] This laser based technique is employed for the measurement and mapping of concentration of various molecules and mass emission in the atmosphere. [7]

The measurement relies on the unique absorption spectrum ("fingerprint") of each type of molecules. An absorption measurement is realized by sending a dual wavelength laser pulse in the direction of a target. [8] One wavelength is tuned to a strong absorption feature of the gas of interest, generally called the 'on' wavelength (λ_{on}) and the other tuned to a nearby wavelength with weak absorption by the gas, generally called the 'off' wavelength (λ_{off}). A sensitive detector detects the light backscattered by particles at the two different wavelengths. The value of the average gas concentration, N_A, in the range interval from R_1 to R_2, can be determined from the ratio of the backscattered LIDAR signals at λ_{on} and λ_{off} , as shown in Fig.1. (Browell, 2003) In that equation, $\Delta\sigma = \sigma_{on} - \sigma_{off}$ is the difference between the absorption cross-sections at the on and off wavelengths, and Pr_{on} (R_1) and Pr_{off} (R_2) are the signal powers received from range R at the on and off wavelengths, respectively. [4]

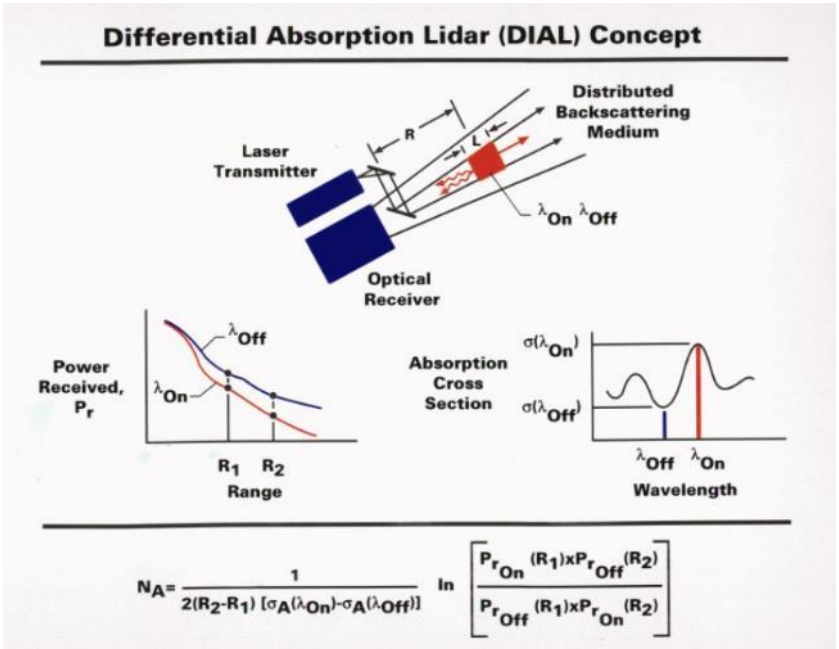


Fig.1. Differential Absorption LiDAR (DIAL) concept (from E.V. Browell, 2003)

This is essentially an application of the Beer–Lambert[1] law for an absorbing medium. The λ_{off} LiDAR return also provides important information on the molecular and aerosol scattering properties of the atmosphere. [4] The differential approach simplifies the calculation after the measurement process. [7]

The laser light is in short pulses and time resolution of the backscattered light (along with the speed of light) gives range resolution as in a simple LIDAR (light detection and ranging). [8]

Main differences existing with the different DIAL systems

Alvarez et al. 2011, provide a classification of the different DIAL systems based on their transmitter characteristics. [9] They mention the systems generally fall into two design classes. The first approach, pioneered by the National Aeronautics and Space Administration (NASA) Langley Research Center, uses high-power tunable dye lasers for the LIDAR transmitter. [10] The resulting system is extremely versatile, but is relatively large with high power consumption, and thus is restricted to large aircraft platforms, which are costly to operate. The second approach, which uses fixed-wavelength lasers, can be made more compact for operation on smaller aircrafts, but cannot be optimized to maximize the spatial and temporal resolution and minimize unwanted interferences. [11], [12], [13], [14] Recently, developments in tunable UV solid-state laser technology have bridged the gap between these two approaches. [15], [16], [17]

Systems can also be distinguished based on the wavelengths used. As shown in Tab. 2, many combinations are possible (UV, visible, NIR, LWIR).

Program carrier	**Circa**	**Channels**	**Laser(s) (*tunable)**	**Measurement of Species**
GND. based 48 inch	1970	2	Ruby @ 347&694 nm	Aerosols/N2
Aircraft Electra 990	1978	3	Ruby, YAG, YAG/Dye @ 1064, 720*,694,600*, 532, 347, 300* nm	Aerosols H2O/O3
LASE, ER 2	1994	3	Ti: Al2O3 @ 815 nm	H2O/Aerosols
LITE, Shuttle	1994	3	YAG @ 1064, 532, 355 nm	Aerosols/clouds Density
ESSP	TBD	3	YAG @ 1064, 532, 355 nm	Aerosols/clouds

Tab.2. Systems and wavelengths used.

Example of application of DIAL technology for chemicals detections

DIAL technology can be employed from local to global scale depending on the objectives of the measurements. Large scale applications can for example deal with water vapor and greenhouse gas distribution in the atmosphere for a better understanding of climate change. In many of these studies airborne LIDAR systems have played a key role by providing highly resolved measurements of the three dimensional distribution of ozone and aerosols. [9] Understanding the formation and transport of ozone and aerosols is of great interest because they negatively impact on air quality and also on climate. [9]

Global measurement example with ozone detection: TOPAZ is an airborne NADIR viewing system using three wavelengths DIAL system. It provides information about ozone and aerosol back scattered profiles from 400 m above airplane to near ground level (flights are generally conducted at an altitude varying from 3000 to 5000 m above sea level). Profiles are acquired at 10 sec intervals. [9]

1 The Beer Lamber law relates the absorption of light to the properties of the material through which the light is traveling. The law states that there is a logarithmic dependence between the transmission (or transmissivity), T, of light through a substance and the product of the absorption coefficient of the substance, α, and the distance the light travels through the material (i.e., the path length), ℓ.

Ozone concentration accuracy	Typically <5%, but can be as high as 15% under low signal-to-noise ratio conditions at ranges >2.5 km with high ozone concentrations
Ozone concentration precision	+/-(2-5) ppb (5%-8%) at close range (400-500 nm) falling to +/-(5-35) ppbv under low SNR conditions as noted above
Resolution: ozone concentration	Vertical: 90 m (with 450 m smoothing) Horizontal (time): 600 m (10 s at a flight speed of 60 $m.s^{-1}$)
Resolution: aerosol backscattered	Vertical: 18 m Horizontal (time): 600 m (10 s at a flight speed of 60 $m.s^{-1}$)
Minimum, maximum range	400m, 3000-5000 m
Laser specifications (per manufacturer) for 1000-Hz pulses	1053 nm, 527 nm, 263 nm. 283-310 nm
Power equipment	3 kW of 110 VAC
Size (volume), weight	Approximately 1.75 m^3, 400 kg total
Laser frame	1.4 m x m 0.76 m x 1.2 m, 185 kg
Cooler	0.70 m x 0.38 m x 0.59 m, 76 kg
Rack-mounted electronics and computers	Total of 1.4 m eight of rack space needed for 0.48 m wide units (unit depths range from 0.05 to 0.46 m), 83 kg
Two racks to hold electronics	0.58 x 0.51 m x 1.0 m, 16 kg each
Nitrogen cylinder	0.2 m diameter, 0.7 m tall, 18 kg

Tab.3. Summary of TOPAZ LIDAR specification (from Alvarez, 2011)

Detection and measurement of chemical warfare agents: Differential absorption LIDAR can also be applied in the detection of chemical warfare agents which constitute a potential hazard. Their release in the atmosphere could happen under different scenarios like a chemical attack, an accident during their manipulation or also during their destruction. In case of an accidental release, a remote sensing system can be used to monitor relatively large geographic areas, replacing a network of point sampling analyzers and providing information about the size, location and direction of the toxic cloud. [18]

Tests were performed using a tunable CO_2 laser designed for helicopter platform (VTB-2) measuring in the 9.2–10.8 μm range. Tab. 4. shows the sensitivity values for two different integration times of 1s and 30s at 2.5 km range. [18]

Material	**Sensitivity (mg/m3)**	
	1s integration time	**30s integration time**
Tabun	342	62
Sarin	247	45
Soman	297	54
Cyclosarin	277	51
Vx	806	147

Tab.4. Sensitivity at 2.5 km range, topographical backscattering (from Halász, 2002)

The sensibility of the detection method varies from 50 to 150 ppm with the longest integration time (30 s).

Detection and measurement of a pollutant over urban areas: Examples of small scale applications are the tracking of a pollutant in the atmosphere near a point source, plume modelling and hot spot detection. [19] Additionally the concentrations can be converted into mass emissions by making a series of scans with the DIAL along different lines within a plume and combining these with meteorological data. These measurements are then used to produce a mass emission profile for a whole site, for instance for fugitive emissions from an oil refinery. [9]

Data have been used to visualize the aerosol pollutant structure throughout the lower Fraser Valley. While the majority of the pollution in the valley is from the urbanized sector around Vancouver, the survey revealed there were at least seven additional point source emitters which impact the valley in a significant way. [20]

Validation or calibration of models: Last DIAL can be used to gather measurements useful later on for the calibration of other methods or assessing predictive pollutant models. As an example, a field experiment (Pacific '93) was carried out in Vancouver, British Columbia, in 1993. The purpose of the experiment was to provide data on the three-dimensional extent and movement of pollutants in a complex topographic regime so that predictive pollutant models could be assessed. [20] Similar measurements made with water vapor helped to improve general circulation models (GCM) and numerical weather prediction (NWP). [1] Airborne measurement campaigns were also performed in order to assess the precision of satellite measurements.

Use of high Resolution Doppler LIDAR as a complementary tool: High Resolution Doppler LIDAR is an additional active measurement tool using laser technology coupled with Doppler to measure the speed of air, convection movement etc. If such systems do not detect or measure chemicals, they help in the understanding of chemicals movement by providing information about air velocity. Such information can be used later on as input in predictive models.

Wavelength	2.0218 μm (fully eye-safe)
Pulse energy	1.5 mJ
Pulse rate	200 Hz
Frequency stability	0.2 MHz
Scan	Upper hemisphere
Range Resolution	30 m
Time Resolution	0.02 s (for 10 pulse average)
Velocity Precision	5 cm/s
Minimum range	0.2 km
Maximum range	2 - 9 km (typically 3 km)
Laser	Tm:Lu,YAG diode-pumped, injection-seeded laser
Platforms	ground, ship, aircraft

Tab.5. Characteristics of High Resolution Doppler LiDAR

Summary about DIAL detection capacities and field of use:

Species	Application	Spectral range	Uncertainties
H_2O (water vapor)	Meteorology		
CO_2 (greenhouse gas)	Global climate		
Ozone, aerosols	greenhouse gas, pollution	UV (from 283 to 310 nm)	several ppbv. or around 5% in good SNV conditions
SO_2			
NH_3	acid rain		
Hg	pollutant		
CO	greenhouse gas		
CH_4 (methane)	greenhouse gas		
N_2O	greenhouse gas		
Tabun, Sarin, Soman, Vx	Chemical warfare agents	Middle infrared tunable from 9.2–10.8 μm	30-85 mg / m^3

Tab.6. Summary table with the different species, wavelength used and the detection capacities

Tunable diode laser (TDL) spectrometry

Working principle

Tunable diode laser absorption spectroscopy (TDLAS) is a technique for measuring the concentration of certain species in a gaseous mixture using tunable diode lasers and laser absorption spectrometry. On the difference with the instruments presented above which performed stand-off or remote sensing measurements, tunable diode laser instruments are designed for in situ trace-gas measurements. In the case of airborne measurements this means that air around the

aircraft is sampled and measured. The advantage of TDLAS over other techniques for concentration measurement is its ability to achieve very low detection limits (of the order of ppb).

A classic TDLAS setup consists of a tunable diode laser light source, transmitting optics, a gas chamber containing the absorbing medium to be measured, receiving optics and detectors.

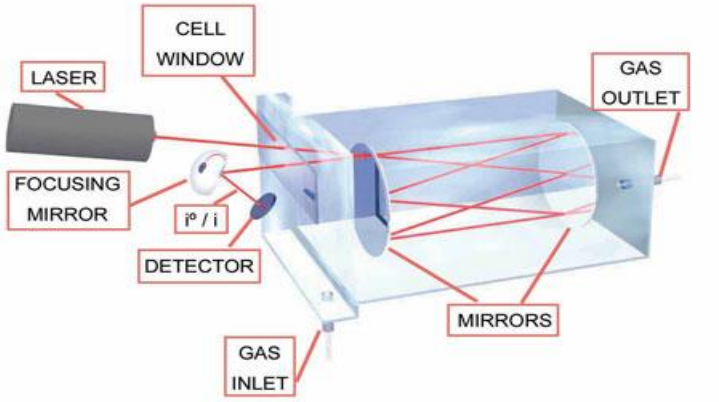


Fig. 2. Gas moisture TDLS detector (image from Servomex)

The principles are straightforward: gas molecules absorb energy at specific wavelengths in the electromagnetic spectrum. At wavelengths slightly different than these absorption lines, there is essentially no absorption. By transmitting a beam of light through a gas mixture sample containing a trace quantity of the target gas, and tuning the beam's wavelength to one of the target gas's absorption lines, and accurately measuring the absorption of that beam with a photodiode, one can deduce the concentration of target gas molecules integrated over the beam's path length. This measurement is usually expressed in units of ppm-m. [21]

The transmitted intensity is related to the concentration of the species present by the Beer-Lambert law, which states that when a radiation of wavenumber passes through an absorbing medium, the intensity variation along the path of the beam is given by:

$$\ln (I_0/I) = S*L*N$$

where I is the measured beam intensity when tuned to the absorbing wavelength of moisture; I_0 is the reference measured beam intensity when tuned away from the moisture absorbing wavelength; S is the fundamental absorption line strength and is a fixed constant; L is the path length of the beam through the sample and is a fixed constant; N is the number of molecules contained in the beam path passing through the sample.

Different variations between the instruments:

Distinctions can be done with the technology used in the laser source. Two main systems are mentioned in the literature. First, distributed feedback lasers (DFB) which is the most common transmitter type in DWDM-system. Distributed feedback diode laser serves as a spectrally bright light source having a well-defined but adjustable wavelength. The structure of a DFB laser includes a grating-like optical element that forces the laser to resonate in a single electromagnetic mode.

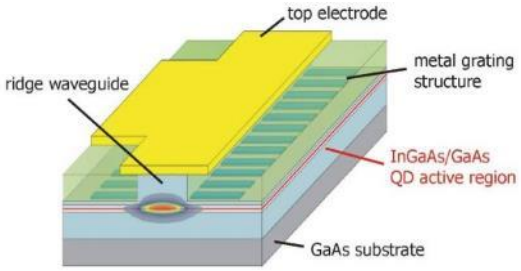


Fig.3. Structure of a distributed feedback laser

The laser emits near-infrared radiation (1.2 - 2.5 μm, or 4000 - 8500 cm^{-1}) with a line width less than 0.003 cm^{-1}, which is considerably narrower than molecular absorption line widths (typically 0.1 cm^{-1} at atmospheric pressure). By accurately controlling the laser temperature and the electrical current that powers the laser, the laser wavelength may be tuned precisely to a specific molecular absorption line that can be selected to be free of interfering absorption from other molecules. [21]

A second type, the vertical-cavity surface-emitting laser (VCSEL) is a type of semiconductor laser diode with laser beam emission perpendicular from the top surface, contrary to conventional edge-emitting semiconductor lasers (also in-plane lasers) which emit from surfaces formed by cleaving the individual chip out of a wafer.

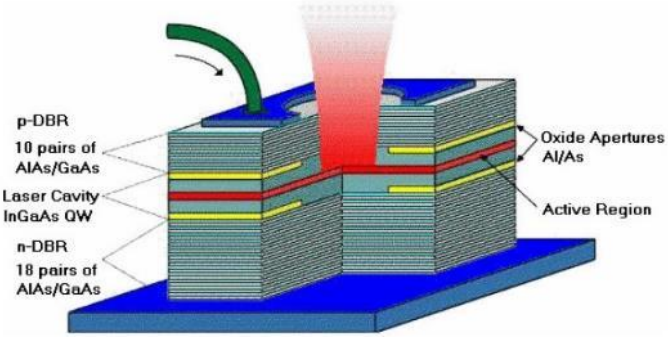


Fig.4. Structure of a vertical cavity surface emitting laser

The high reflectivity mirrors, compared to most edge-emitting lasers, reduce the threshold current of VCSELs, resulting in low power consumption. However, as yet, VCSELs have lower emission power compared to edge-emitting lasers. The low threshold current also permits high intrinsic modulation bandwidths in VCSELs.

A multipass optical cell (Herriot cell) may be utilized to provide a long optical path length within a small volume, in many cases yielding sub-ppm sensitivity with one second or faster response. [22]

Furthermore, techniques known as frequency or wavelength modulation spectroscopy (WMS) and Balanced Ratiometric Detection (BRD) are frequently employed in TDLAS instruments to make them exquisitely sensitive to even very weak absorption of the laser power. [21]

Example of application of TDLAS technology for chemicals detections

An airborne tunable laser absorption spectrometer was used in two polar ozone campaigns, the Airborne Antarctic Ozone Experiment and the Airborne Arctic Stratospheric Expedition, and measured nitrous oxide from an ER-2 high-altitude research aircraft with a response time of 1s and an accuracy ≤ 10%. Laser-wavelength modulation and second-harmonic detection were employed to achieve the required constituent detection sensitivity. [23]

Physical Sciences Inc. has developed hand-held Standoff TDLAS sensors for the inspection of municipal natural gas pipelines. In standoff devices, passive reflectance of a laser beam projected onto walls and other structures enables measurement of path-integrated target gas concentrations over distances up to a few tens of meters. These sensors can be adapted to sense any of the gases listed in Table 7. [21]

Gas	Detection Limit(ppm-m)
HF	0.2
H2S	20.
NH3	5.0
H2O	1.0
CH4	1.0
HCl	0.15
HCN	1.0
CO	40.
CO2	40.
NO	30.0
NO2	0.2
O2	50.
C2H2	0.2

Tab.7. Species routinely detection with stand-off TDLAS technique and detection limits

Combining EDFA and WMS provides a long range and robust and modest cost stand-off sensor. They are for example used in the aerial detection of leaks. [25]

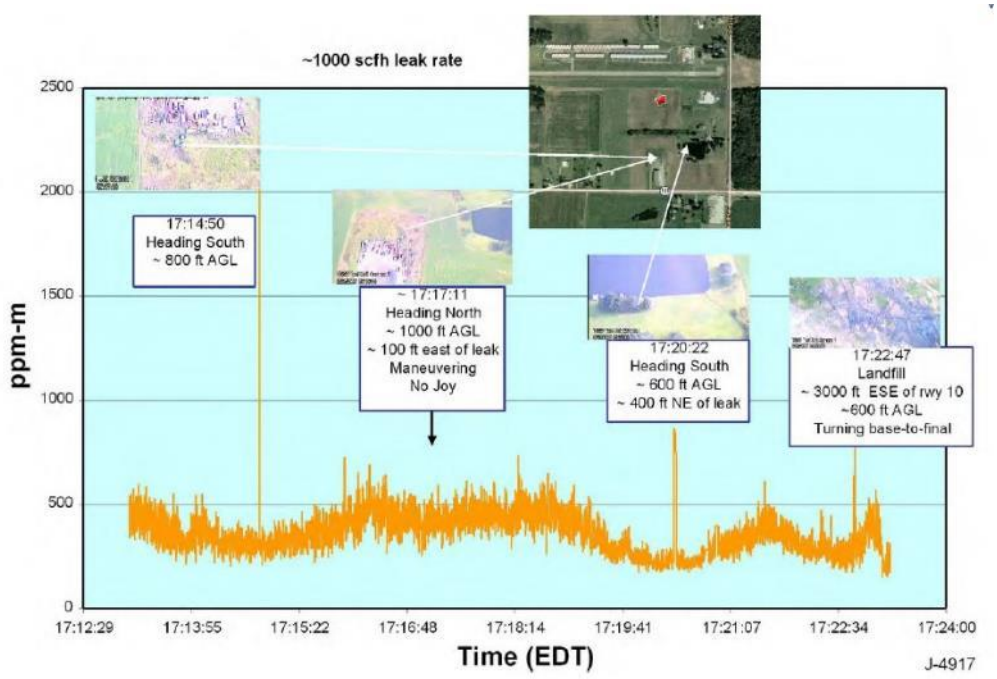


Fig.5. Results from an aerial remote methane leak detection [26]

The table below summarizes the different species measured with TLDAS technology, the accuracy of the measurement and the associated response time.

CO	precision of approximately 3.6% for the TDLAS. Precisions of 1.5 ppbv	5s response time	[28] [27]
CO and CH4	0.1% CH4, 1 % CO	5s response time	[28]
formaldehyde (CH2O)	40-60 pptv 80- 120 pptv 55 pptv	4.5 min 55 sec 20 sec	[34]
NO	measured nitrous oxide with a response time of 1s and an accuracy ≤ 10%.		
N2O, CH4, CO or O3	Accuracy: 10% (2s) ± 1ppbv (for N2O) Resolution: 1ppbv Location on ER-2: Spear Pod, right wing	1s	ATLAS
N2O, H2O isotopes, H2O, CO, CH4, CO2 isotopes, HCl	1 ppb		ALIAS
CO, CH4, N2O			ARGUS
CH3OH, CH2O			NASA Dual Channel Airborne tunable diode Laser Spectrometer [25]

Table 8. Some gases measured by TDLASM

Ammonia	Arsine	Boron trichloride
Boron trifluoride	Carbon disulfide	Chlorine
Diborane	Ethylene oxide	Fluorine
Formaldehyde	Hydrogen bromide	Hydrogen chloride
Hydrogen cyanide	Hydrogen fluoride	Hydrogen sulfide
Nitric acid, fuming	Phosgene	Phosphorus trichloride
Sulfur dioxide	Sulfuric acid	Tungsten hexafluoride

Proven
Likely
Possible
Unknown

Tab. 9. Ability of TDLAS to detect high priority TICs. [26]

RECENT DEVELOPMENTS IN THE DETECTION OF IONIZING RADIATIONS WITH LASER TECHNOLOGY AND THEIR ASSESSMENT IN THE PERSPECTIVE OF AIRBORNE APPLICATION

General orientation about radiation detection

Ionizing radiations can neither be seen by human sense, nor directly measured by instruments. Nevertheless, ionizing radiation interacts with matter, generating some changes of its physical properties (ionization, excitation). In some controlled cases the change or effect can be converted into a numerical value and it can be correlated to the quantity of energy that interacted with the matter, providing a quantitative indication about the quantity of ionizing radiation.

One could distinguish two different strategies with the detection process. In the first one the particles are the target of the detection. Particles travel from the radiological sources to the sensor where they interact with material constituting the sensor (they are trapped). The materials are chosen based on their capacities to convert the energy received from the particles into measurable physical values (light pulse or electric discharge/pulse). All the sensors belonging to this category (crystals, semiconductors and ionization chamber) are passive.

The second strategy considers the ionized molecules as the targets. It considers the quantity of ionized or excited molecules as an indicator of the importance of the ionizing radiation. Any

mean estimating the concentration of excited molecules or ions falls in this category (whether they are active or passive). The measurement can be realized with the direct measurement of the molecules concentration (in a plume for example) or by remote detection. In this last case, a medium participate in the detection process. In the case of airborne laser detection, remote detection is favored with the detection of induced emission (fluorescence), reflection or absorption on specific bands of the electromagnetic spectrum.

After the extended bibliographic research we conducted, we can conclude that in the specific case of airborne detection of ionizing radiations, presently only aerial gamma spectrometry is routinely used. Until now it has also been the lonely method to have been recommended by the IAEA[2] for airborne detection. The other methods, concepts or patents we are presenting in the paragraphs below proved to be well founded by theory and experiments but where not yet adapted and applied in the airborne detection. Even airborne experimentations are not mentioned by literature.

Main form of ionizing radiations and strategies with laser detection

Several types of ionizing radiations should be distinguished depending on their characteristics.

Gamma radiation is constituted by high energy photons (energy above 100 keV). As those particles have no charge and a small size they have an important penetration range in the air and a very low specific ionization. As a consequence the ionization products are largely spread in the space and specific ionization is the lowest. Consequently it theoretically requires an important sensitivity in the detection method.

Alpha radiations are constituted by charged particles comparable to a helium nucleus. Alpha particles combine an important size with a double charge which results in the highest specific ionization and the lowest penetration range in the air (several centimeters only). As a consequence, the ionized and excited molecule density around radiological material is maximal in the case of alpha source, which theoretically result in the best opportunity for their detection. As the ionized or excited molecules usually have a particular response for emission or absorption of light, they can theoretically be detected by optical remote sensing methods.

Beta radiations also have a finite range in the air but a more important penetration range compared to alpha particles (several meters). As a consequence the specific ionization is low and the ion cloud around radiological materials has a larger footprint.

Type of radiation		**Ionizing radiation**	**Charge**	**Speeds**	**Range in the air**	**Specific ionization (ion pairs/cm) [35]**
Electro-magnetic radiations	Ind. ionizing	Gamma ray	0	Speed of light	decrease exponentially, never stopped	5-8
Particles		Neutron	0			
	Directly ionizing	Electron/particle β-	-1	25-99% speed of light	2-8 meters	50-500
		Positron/particle β+	+1		2-8 meters	
		Ion 4He/particle α	+2	3200-32000km/s	5-6 cm	20 000-50 000

Tab.10. Main characteristics of the ionizing radiations.

Depending on the physical characteristics summarized above, particles follows different paths and the ions and excited atoms or molecule are distributed in the space around radiologic materials very differently. Their distribution compared to the sensor sensitivity is an important point to be considered in the detection approach. The figure below proposes a schematic spatial

[2] International Atomic Energy Agency

repartition of the excited/ionized component in the space for alpha, beta and gamma radiation. Alpha radiation leads to the most dense ionization cloud. Beta is similar but more diffuse (on a bigger volume) whereas gamma is totally diffuse. In these conditions – where the goal is to capture lights affected by ionization products – alpha and beta radiation detection seems the most promising.

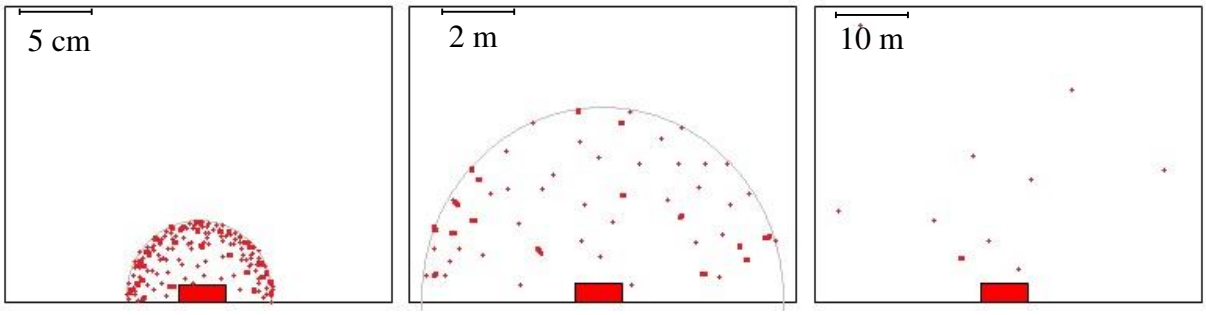


Fig.6. Schematic spatial repartition of ionized and excited molecules for α, β and ɣ radiations

Details about the ionization process and consequences for detection

$X \rightarrow X^+ + e^-$

Ionization happens when the ionizing particle free an electron from an atom. Ionization mechanism leads primarily to the production of an ion pair with a positively charged molecule (or atom) and an electron. The radical can enter secondary reactions -oxidation is the main expected reaction to be expected in the air- leading to more stability.

	N2	**O2**
Ionization	N2→N2++ e-	O2→O2+ + e- O2+ + 2O2 → 2 O3 N2O, HNO3, H2NO2 and NO2.
Excitation	N2→N2*	O2→O2*

Tab.11. Ionized and excited Nitrogen and oxygen and recombination products

Depending on the ionization and the stability of the ionization product, it could be worth not to spot to the measurement of the primary products but to also consider secondary products, whether they are more stable or whether they are more responsive to the detection process.

Importance of chemical kinetics and species' reactivity for the detection process

The detection process target specific species (excited or ionized molecules) into a gas mixture with a very low volumetric (or molar) fraction. [36] In this context the choice of the target specie (or species) should be strategically done in order to reach the highest detection threshold.

Two strategies are relevant to the detection process. The first one is selecting specie with a really specific effect on light (absorption, emission (fluorescence)). Yao has for example noticed that the reactivity of the free radicals to laser light could vary from 5% to 95%.

The second one is selecting specie with the most important population in order to again enhance the detection threshold as much as possible. This last one depends on the life time of the specific specie, which depends on its reactivity (excited and ionized species) and/or stability (mainly for excited species). This can be known from the study of chemical kinetics. Last but not least, the volumetric fraction depends on the mother molecule proportion. In the air, N_2 derivates are the most interesting followed by O_2 derivates.

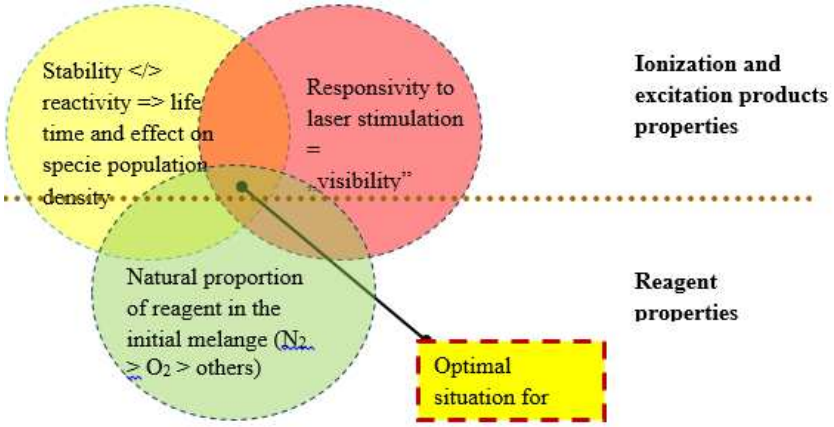


Fig. 7. Optimizing detection strategy

Application of LIDAR with the measurement of laser induced fluorescence in the surroundings of radiological materials

The system indirectly measures radiation by detecting the fluorescence UV light emitted by the ions and excited molecules primarily created by ionizing radiations and secondarily activated by the energy of the laser beam. [37]

The systems employs a DIAL technic with a pulsed laser transmitter, a telescope receiver, and associated control and acquisition systems. [37]

Light propagates out from the laser transmitter and is directed into the volume surrounding the radioactive source, or the "ion cloud." The ion cloud absorbs the transmitted light. This absorption induces otherwise undetectable, non-fluorescing ions to fluoresce. Light from the ion cloud is then backscattered and the telescope receiver subsequently collects the photons from the backscattered light. The intensity of the fluorescence (determined by the photon count) is measured, which provides an indication of the number density of the ionized atoms.

This strategy – which consists into an activation process with laser ligth of the of ions species that otherwise would not fluoresce – rise the fluorescence rate from 5% to 95%. [37]

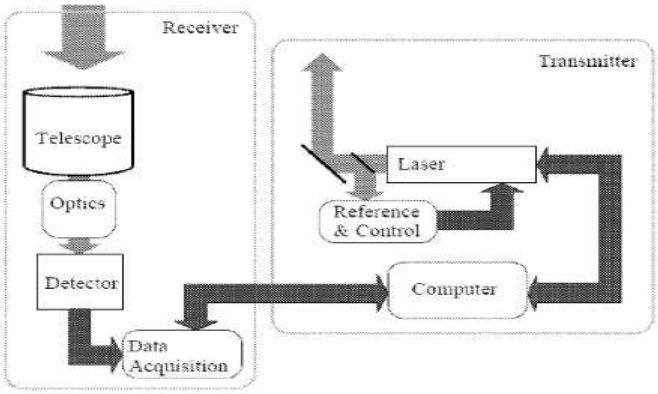


Fig.8. Picture taken from US patent US 20120112076 A1

Algorithms can then be used to relate the measured ionization rates to the source activity.

The invention use active detection of UV light. Contrary to many of the current techniques which use passive detection of ultraviolet (UV) light, the active detection can be used to detect radiation during daylight. The system enables the remote detection of radiation source ranging from 1-1000 m. The preferred wavelength for the laser light is slightly temperature dependent and varies between 390.5 nanometers (nm) and 391.5 nanometers. [37]

The detection range announced in the patent seems compatible with an airborne application under the condition that atmosphere does not absorb UV photons differently than the condition tested in the patent. Adaptation should be considered regarding two components of the system.

First the laser transmitter should be adapted to be able to scan the environment under the carrying platform. The same kind of application is routinely used in LIDAR laser scanning devices utilized in the acquisition of elevation data. Second the telescope should be replaced by an optical system covering a larger foot print on the ground. Another difficulty is to have an acquisition frequency of the detector matching with the scanning rate of the laser transmitter. The last aspect to be considered is the flight speed (and associated platform to be used) to have the required accuracy. [37]

Radiation remote-sensing method based on laser spectroscopic measurement of radiation-induced radicals

Laser spectroscopy could constitute a solution for the measurement of intense radiation fields such as around nuclear reactors, high energy accelerators or nuclear disasters. Tomita et al developed a reliable radiation sensing method with high radiation resistance. They proposed a novel radiation remote-sensing method based on high sensitive cavity ring-down (CRD) laser spectroscopic measurement based on the detection of radiation induced radicals. To verify the detection principle they first have made basic experiments on the CRD spectroscopic measurement of the radiation induced ozone concentration in the air irradiated by ^{60}Co gamma-rays. Secondly they have developed a calculation model to estimate the yields of radiation induced radicals by solving simultaneous rate equations numerically. Through comparison between the experiments and the calculations, they have confirmed the detection principle and the validity of the calculation model, where the results show that the detectable range for the absorbed dose rate range from 4.8×10^{-2} to 3.2 Gy/s with time resolution of 35 sec by controlling the flow rate of the irradiated air. [38]

Such a system could find application on UAV because such platform can first go where radiation level is quite important without risking human life and secondly it can fly at lower speed, even making stationnnary flight (a condition necessary to have sufficient integration time). Two aspects should be considered in the specific case of UAV application. First the energy consomption as laser system is an important energy consumer. Secondly the load of the detection system plus its energy supply should be compatible with available carriage capacity of current UAV. Nethertheless, it should be noticed that in the case of intense radiative environment, aerial gamma spectrometry already fullfil the requirements.

Active remote detection of radioactivity based on the frequency modulation of a probe beam by the rise of electron density induced by laser radiation

The concept uses a laser radiation as a photo-detaching beam and a probe beam to detect electromagnetic signatures in the vicinity of radioactive material. [39]

Radioactive materials emit gamma rays that ionize the surrounding air. The ionized electrons rapidly attach to oxygen molecules, forming superoxide (O_2^-) ions. The elevated population of O_2^- extends several meters around the radioactive material. Electrons are photodetached from O_2^- ions by laser radiation and initiate avalanche ionization, which results in a rapid increase in electron density. The rise in electron density induces a frequency modulation on a probe beam, which becomes a direct signature for the presence of radioactive material. Gamma rays emitted by radioactive material will increase the free electron density as well as the O_2^- density. The concept makes use of laser beams to photoionize the O_2^-, thus providing the seed electrons for air breakdown. [39]

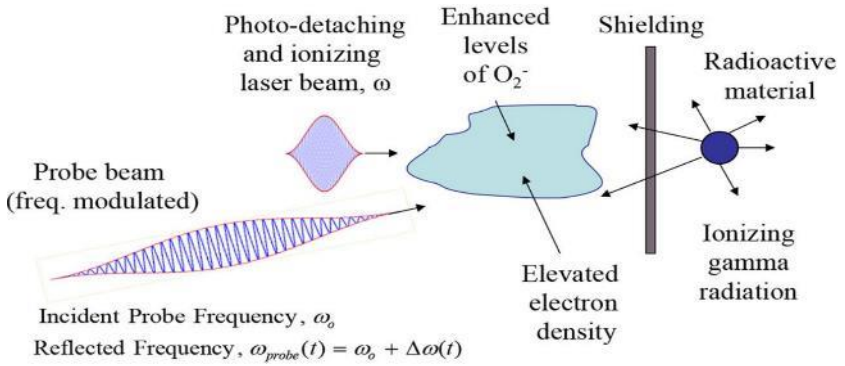


Fig. 9. The effect of laser beam on the ionized air by gamma radiation

As an example of this method of detection, the case is considered where the ionizing laser has a peak intensity of 160 GW/cm^2 and pulse duration of 1ns. The probe beam is a millimeter wave source of frequency 94 GHz. In the absence of radioactive material there is no frequency modulation of the probe. For $\alpha_{rad} = 10^3$ and a probe-beam interaction distance of 10 cm, the fractional frequency modulation is significant, around 5%, which is readily detectable. In other words, the frequency shift is the sought-for electromagnetic signature of radioactive material and can be measured. [39]

The author stated that standoff detection can be done from distance geater than 100 m. In the experiment presented in the paper, the distance probe source is 10 cm and allow a detection of 5 percent of fractional frequency modulation. [39]

The author considers the detection of enhanced levels of O_2^- generated by a shielded gamma radiation source. If considering Alpha or Beta source without shielding, the α_{rad} would be much more favorable for the detection in the volume where alpha and beta ray are ranging.

Standoff alpha radiation detection via the measurement of energy aborbed by excited state molecules.

Yao emphasizes the fact that methods employing the detection of faint light (fluorescence) or backscattered laser light (in DIAL application) have limited detection capacities when the distance between the laser source and the target is increased. [40] The reason is that spontaneous emission radiates uniformly within an entire 4p solid angle, so its intensity drops rapidly according to 1/r^2 law, where r is the standoff distance. The same intrinsic problem of propagation loss happens with backscattered laser light and still limits the distance of the standoff detection. [40]

To overcome these limitations, Yao proposes to base the alpha radiation detection on the measurement of the transmitted laser energy in order to determine (by subtraction) the quantity of absorbed energy at specific wavelength. Since the probe beam is a collimated beam, its propagation does not suffer the fundamental limitation of 1/r^2 propagation loss. [40]

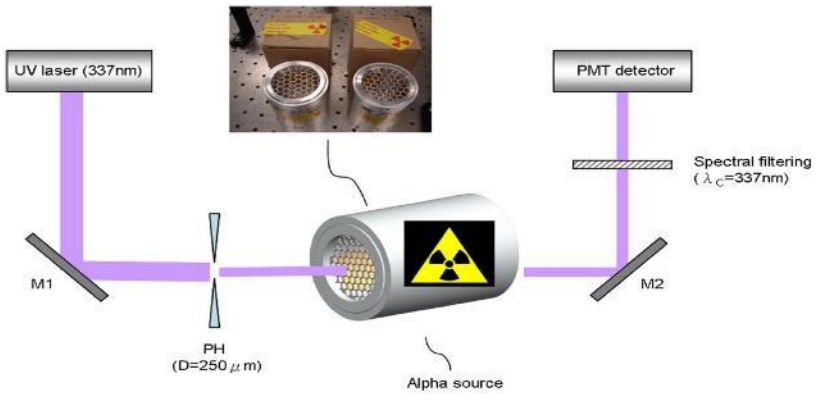


Fig. 10. Schematic illustration of the experimental setup

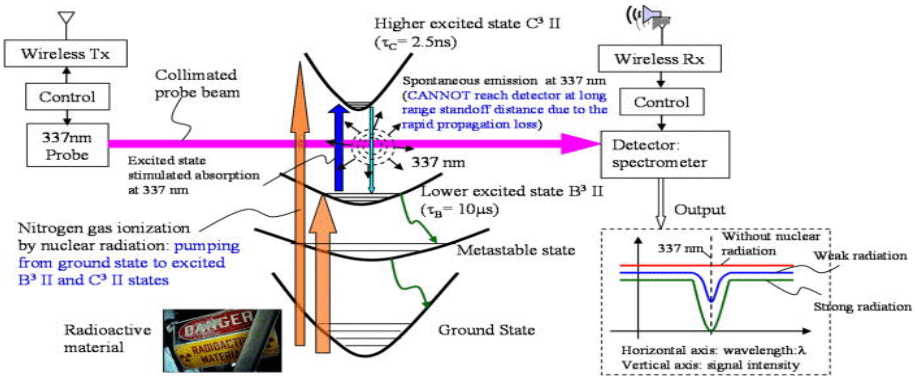


Fig. 11. Conceptual illustration of standoff detection of radiation via excited state absorption of radiation excited/ionized air

Experiments were done at distance of 0.5 and 10 m with a 337 nm UV probe beam through a 40 mCi Po-210 alpha source. The detected signal as a function of time is not sensitive to the separation distance between the light source and alpha radiation source. [40]

This technology has a potential to realize long range standoff detection but because of the bi-static measurement dispositive – in which the UV radiation source and the detector are on the

opposite sides of the beam path – this technique is applicable only for stationary measurements. Consequently application in airborne detection and measurement is excluded.

CONCLUSION

The review of airborne applications of laser measurement methodologies demonstrated both the numerous specialties where it is applied – like environmental monitoring, chemical warfare protection, pollution detection and monitoring, meteorology – and the diverse species of chemical measured like water vapor, aerosols, nerve agent, greenhouse gases. The technics introduced deserve different goals with different detection capacities. DIAL technology range from several hundred ppm to ppt detection capacity and allows an integrated measurement approach (layer or profile approach). TDLS provides punctual but very precise measurements (ppb or ppt detection measurements).

The extended bibliographic researches conducted about the airborne radiation detection first of all highlighted that laser detection is not currently employed neither airborne experimentation was mentioned in the literature. Only aerial gamma spectrometry is routinely employed for this purpose. The reasons are twofold: gamma radiations are the most penetrating radiations so they better allow the detection from distance and most of the radiological materials can be detected from the gamma radiations they or their daughter products emit. Nevertheless methods employing active laser technology were developed and patented for the standoff or remote detection of alpha, beta and gamma radiations. With further developments or adaptations they could potentially find application in airborne detection. Important concepts emerged from our analysis. Only systems employing light backscattering have the potential to be adapted to airborne measurement. This results in a propagation loss that follows a $1/r^2$ law which limits the range for detection. Expectations for alpha and beta airborne measurement should be based upon that. Then several innovative ideas could be extracted from the measurement systems:

- The possibility to push target molecules to fluoresce by pumping electrons to an energy level that naturally does not occur.
- Exploring further the effect of ionization on the fractional frequency modulation.
- Targeting free radical species which have longer lifetime and associate denser population.

References:

[1] M. Wirth, A. Fix, P. Mahnke, H. Schwarzer, F. Schrandt, G. Ehret: The airborne multi-wavelength water vapor differential absorption lidar WALES: system design and performance. Applied Physics B. Volume 96, Issue 1 , pp 201-213. 2009-07-01. DOI 10.1007/s00340-009-3365-7

[2] R.M. Schotland, J. Appl. Meteor. **13**, 71–77 (1974)

[3] E.V. Browell, S. Ismail, W.B. Grant: Differencial Absorption Lidar (DIAL) measurements from air and space. Applied Physics - Laser and optics. p. 399-410 (1998)

[4] E.V. Browell, S. Ismail and W.B. Grant: LIDAR | DIAL, In Encyclopedia of Atmospheric Sciences, edited by James R. Holton, Academic Press, Oxford, 2003, Pages 1183-1194, ISBN 9780122270901, http://dx.doi.org/10.1016/B0-12-227090-8/00204-9.

[5] Space lidar http://www.nasa.gov/centers/langley/news/factsheets/LITE.html

[6] COLIPSO http://www.nasa.gov/pdf/137028main_FS-2005-09-120-LaRC.pdf

[7] http://www.spectrasyne.ltd.uk/html/about_dial.html

[8] http://www.spectrasyne.ltd.uk/html/technique.html

[9] R. J. Alvarez II, C. J. Senff, A. O. Langford, A. M. Weickmann, D. C. Law, J. L. Machol, D. A. Merritt, R. D. Marchbanks, S. P. Sandberg, W. A. Brewer, R. M. Hardesty, R. M. Banta: Development and Application of a Compact, Tunable, Solid-State Airborne Ozone Lidar System for Boundary Layer Profiling. *Journal of Atmospheric and Oceanic Technology* **28**:10, 1258-1272. Online publication date: 1-Oct-2011. L.

[10] E. V. Browell, A. F. Carter, S. T. Shipley, R. J. Allen, C. F. Butler, M. N. Mayo, J. H. Siviter Jr. and W. M. Hall: NASA multipurpose airborne DIAL system and measurements of ozone and aerosol profiles. Appl. Opt., 22, (1983) 522–534.

[11] E. Uthe , J. Livingston, and N. Nielsen: Airborne lidar mapping of ozone concentrations during the Lake Michigan ozone study. J. Air Waste Manage. Assoc., 42, (1992), p.1313–1318.

[12] R. J., II Alvarez, C. J. Senff, R. M. Hardesty, D. D. Parrish, W. T. Luke, T. B. Watson, P. H. Daum, and N. Gillani: Comparisons of airborne lidar measurements of ozone with airborne in situ measurements during the 1995 Southern Oxidants Study. J. Geophys. Res., 103, (1998), 31 155–31 171.

[13] G. Ancellet, and F. Ravetta: Compact airborne lidar for tropospheric ozone: Description and field measurements. Appl. Opt., 37, (1998), p. 5509–5521.

[14] M.H. Proffitt and A.O. Langford: Ground-based differential absorption lidar systemfor day or nightmeasurements of ozone throughout the free troposphere. Appl. Opt., 36, (1997) p. 2568–2585.

[15] Coutts, D., and A. J. S. McGonigle: Cerium-doped fluoride lasers. IEEE J. Quantum Electron., 40, (2004) p. 1430–1440.

[16] K. A. Elsayed, S. S. Chen, L. B. Petway, B. L. Meadows, W. D. Marsh, W. C. Edwards, J. C. Barnes, and R. J. DeYoung: High-energy, efficient, 30-Hz ultraviolet laser sources for airborne ozone-lidar systems. Appl. Opt., 41, (2002) p. 2734–2739.

[17] A. Fix, M.Wirth, A.Meister, G. Ehret, M. Pesch, and D. Weidauer: Tunable ultraviolet optical parametric oscillator for differential absorption lidar measurements of tropospheric ozone. Appl. Phys. B, 75, (2002) p.153–163, doi:10.1007/s00340-002-0964-y

[18] L. Halász: The role of remote sensing equipment in air monitoring systems. In: NATO Series of Disarmement Technologies, Vol. 13, Kluwer, Dodrecht, 1997, p. 241–253

[19] L. Halasz, I. Pinter, A. Solymar Szocs: Remote sensing in the biological and chemical reconnaissance. AARMS, vol 1. Issue 1 (2002), 39-56.

[20] R.M. Hoff, M. Harwood, A. Sheppard, F. Froude, J.B. Martin, W. Strapp: Use of airborne LiDAR to determine aerosol sources and movement in the Lower Fraser Valley (LFV), BC, Atmospheric Environment, Volume 31, Issue 14, July 1997, Pages 2123-2134, ISSN 1352-2310, http://dx.doi.org/10.1016/S1352-2310(96)00302-0.

[21] http://www.tdlas.com/theory.shtml

[22] http://www.tdlas.com/applications.shtml

[23] J. Podolske, M. Loewenstein: Airborne tunable diode laser spectrometer for trace-gas measurement in the lower stratosphere, Appl. Opt. 32, 5324-5333 (1993) http://www.opticsinfobase.org/ao/abstract.cfm?URI=ao-32-27-5324

[24] Physical Inc. http://www.psicorp.com/pdf/library/VG07-187.pdf

[25] https://airbornescience.nasa.gov/instrument/DCALS

[26] M. B. Frish, R. T. Wainner, M. C. Laderer, B. D. Green and M. G. Allen: Standoff and Miniature Chemical Vapor Detectors Based on Tunable Diode Laser Absorption Spectroscopy. http://www.psicorp.com/pdf/library/SR-1343.pdf

[27] J. S. Holloway, R. O. Jakoubek, D. D. Parrish, C. Gerbig, A. Volz-Thomas, S. Schmitgen, A. Fried, B. Wert, B. Henry, J. R. Drummond: Airborne intercomparison of vacuum ultraviolet fluorescence and tunable diode laser absorption measurements of tropospheric carbon monoxide. Journal of Geophysical Research: Atmospheres (1984–2012). Volume 105, Issue D19, pages 24251–24261, 16 October 2000.

[28] G. W. Sachse, J. E. Collins, Jr., G. F. Hill, L. O. Wade, L. G. Burney et al.: Airborne tunable diode laser sensor for high-precision concentration and flux measurements of carbon monoxide and methane, Proc. SPIE 1433, Measurement of Atmospheric Gases, 157 (May 1, 1991); doi:10.1117/12.46162; http://dx.doi.org/10.1117/12.46162

[29] A. Fried, P. Weibring, D. Richter, J. Walega, C. Roller et al.: tunable diode laser and difference frequency generation absorption spectrometers for highly sensitive airborne measurements of trace atmospheric constituents, Proc. SPIE 6378, Chemical and Biological Sensors for Industrial and Environmental Monitoring II, 63780F (October 17, 2006); doi:10.1117/12.691318; http://dx.doi.org/10.1117/12.691318

[30] B. P. Wert, A. Fried, and J. R. Drummond: Airborne measurements of tropospheric formaldehyde by tunable diode laser absorption spectroscopy, Proc. SPIE 2834, Application of Tunable Diode and Other Infrared Sources for Atmospheric Studies and Industrial Process Monitoring, 175 (October 21, 1996); doi:10.1117/12.255323; http://dx.doi.org/10.1117/12.255323

[31] https://www.servomex.com/Servomex/web/web.nsf/en/delta-f-moisture-technology

[32] http://212.201.48.1/course/c320352/Presentation/NS%20Vertical%20Cavity%20Surface%20Emitting%20Laser.pdf

[33] Aerial Methane Leak Detection. Asel-Tech http://asel-tech.com/documents/Asel-Tech%20aRMLD.pdf

[34] A.n Fried, B. P. Wert, B. Henry, J. R. Drummond: Airborne tunable diode laser measurements of formaldehyde, Spectrochimica Acta Part A: Molecular and Biomolecular Spectroscopy, Volume 55, Issue 10, September 1999, Pages 2097-2110, ISSN 1386-1425, http://dx.doi.org/10.1016/S1386-1425(99)00082-7 (http://www.sciencedirect.com/science/article/pii/S1386142599000827)

[35] specific ionization of particles http://www.fas.org/nuke/guide/usa/doctrine/dod/fm8-9/1ch2.htm

[36] C. E., Moss, R. M. Goeller, D. F. Milligan, J. E. Valencia, J. Zinn: Remote sensing of radiation. Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, 422(1-3) (1999) 832 – 836.

[37] GEORGIA TECH RESEARCH CORPORATION, GEORGIA : Remote detection of radiation, US Patent US 20120112076 A1, issued 2012.01.11.

[38] H. Tomita, K. Watanabe, J. Kawarabayashi, T. Iguchi: Development of novel radiation remote-sensing method based on laser spectroscopic measurement of radiation-induced radicals, Proc. SPIE 5198, Hard X-Ray and Gamma-Ray Detector Physics V, 281 (January 20, 2004); doi:10.1117/12.506447; http://dx.doi.org/10.1117/12.506447

[39] P. Sprangle, B. Hafizi, H. Milchberg, G.S. Nusinovich, A. Zigler: Active remote detection of radioactivity based on electromagnetic signatures. 30 October 2013, SPIE Newsroom.

[40] J. Yao, J. Brenizer, R. Hui, S. S. Yin. Standoff alpha radiation detection via excited state absorption of air. Appl. Phys. Lett. 102, 254101, (2013); doi: 10.1063/1.4812338

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Kátai-Urbán Lajos - Kiss Béla
katai.lajos@uni-nke.hu - kiss.bela1979@freemail.hu

NUKLEÁRIS ERŐMŰVEK, MINT VESZÉLYES TECHNOLÓGIA ÉS AZ ORSZÁGOS NUKLEÁRIS BALESETELHÁRÍTÁSI RENDSZER

Absztrakt

Napjainkban a katasztrófavédelem területén dolgozó szakembereknek számos természeti és civilizációs katasztrófával kell tudniuk felvenni a harcot, ismerni az ellenük történő védekezés módszereit, feladatait és a védekezéshez felhasználható eszközrendszereket. Jelenlegi ismereteink szerint a nukleáris katasztrófa az egyik legsúlyosabb következményekkel járó civilizációs katasztrófák egyike, amelynek bekövetkezése esetén jelentős természeti és civilizációs károkkal lehet számolnunk. Cikkünkben a nukleáris energiatermelést és a vele járó veszélyforrásokat mutatjuk be. Ismertetjük az Országos Nukleárisbaleset-elhárítási Rendszer feladatát és felépítését.

Today, working in the field of disaster management professionals need to know to fight a number of natural and man-made disaster, recognized methods of protection against them, tasks and means of defence systems used. According to our knowledge the occurrence of a nuclear disaster can cause major natural and man-made damage to the environment. In our article we will introduce generally the nuclear power generations and the dangers associated with it. We will present the function and structure of National Emergency Preparedness System.

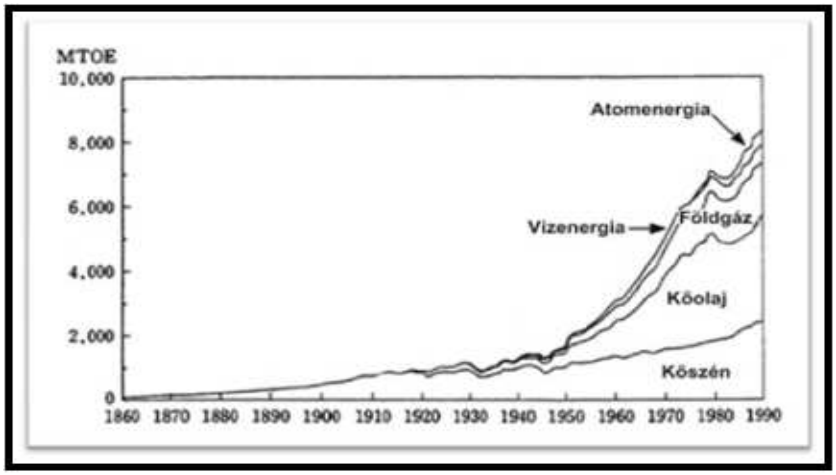
Kulcsszavak: *nukleáris energia, atomerőmű, iparbiztonság, nukleáris baleset-elhárítás, légi sugárfelderítés ~ nuclear energy, nuclear power plant, industrial safety, nuclear accident preparedness, aircraft reconnaissance jet*

BEVEZETÉS

Cikkünk első részében a nukleáris energiatermelés előnyeit, hátrányait, mint veszélyes technológiát és eddig megtörtént nukleáris balesetek tanulságait szeretnénk bemutatni és elemezni.

Az egyik legáltalánosabb tény, hogy az ember szerves része a természetnek, ezáltal nem tud kibújni és mentesülni annak törvényei alól. Adottságainak köszönhetően viszont a környezetét jelentős mértékben képes befolyásolni és jóval nagyobb léptékben képes rá hatni. A történelem során az emberiség célja a megalkotott vívmányokkal és általa folytatott tevékenységekkel mindig is a jobb megélhetés és a nagyobb mértékű túlélés volt. Azonban ha nem megfelelő módon használják ki e vívmányok által nyújtotta lehetőségeket, a felelőtlen magatartás akár az emberiség jövőjét is veszélybe sodorhatja. A közös érdekünk tehát azt diktálja, hogy felismert törvényszerűségeket figyelembe véve, használjuk ki és éljünk a lehetőségeinkkel.

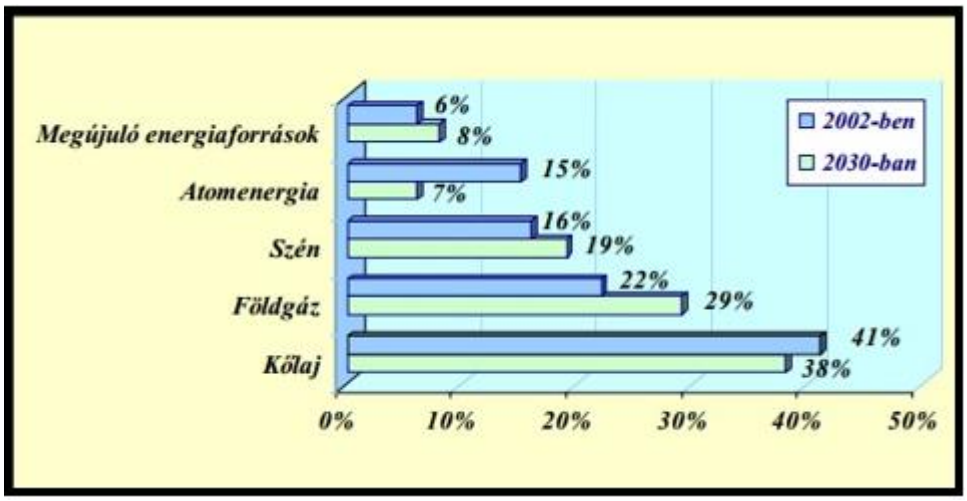
Az energia az emberiség létfenntartásához szükséges, hiszen ez által képes biztosítani az életfolyamatait. Ezen energia kinyerhető a napsugárzásból, vagy más élőlények által felépített anyagok lebontásából. Az emberiség történelmét áttekintve elmondhatjuk, hogy az ipari forradalom bekövetkezéséig az emberi tevékenységek hatása viszonylag kis területekre koncentrálódott, és e tevékenységek hatásai visszafordíthatóak voltak és nem befolyásolták a globális természeti folyamatokat.



1. ábra. A világ primer energiaigényének alakulása 1860-1990 között millió tonna kőolajra vonatkoztatva. [1]

Az 1. ábrán látható módon az ipari forradalom és az iparosodás megindulásával azonban mindez gyökeresen és visszafordíthatatlanul megváltozott. Az ipari forradalom hatására a világ motorja és mozgatórugója a gazdaság lett és soha nem látott léptékekben indult meg a technológiai és társadalmi fejlődés. Ezzel párhuzamosan a gazdaság egyre inkább energia központúvá vált és a fejlődés fenntartásához több energia előállítására volt szükség. A következő robbanás az energiafelhasználásban a II. világháborút követő időszakban következett be, amikor is a tudományos és technikai fejlődés vívmányait kezdték alkalmazni a gazdaságban, és a mindennapi életben, ezáltal egyre inkább elérhetővé vált a hétköznapi ember számára.

Az energiafelhasználás rohamos növekedése olyan új energiatermelő technológiák kifejlesztését tette szükségessé, mint a nukleáris energia felhasználása. A nukleáris energiatermelést elsősorban az elektromos áram termelésére kezdték használni és műszaki-gazdasági okokból elsősorban alaperőműként működtetni. Ezt követően az elmúlt 50 évben az atomenergetika jelentős fejlődésen ment keresztül. A haladást elsősorban az energetika általános fejlődése, az energetikával szemben támasztott gazdasági, környezetvédelmi és egyéb követelmények tették lehetővé. A jelenlegi gazdasági és társadalmi berendezkedésünk nem teszi lehetővé, hogy nélkülözze a koncentrált energiatermelést. Úgy tűnik, hogy a hivatkozott problémát a 2. ábrán látható módon a megújuló energiaforrásoknak és az atomenergiának együtt kell megoldaniuk.



2. ábra. Energiahordozók megoszlásának várható aránya az EU-ban. [2]

Ehhez azonban az atomenergetikának néhány kulcskérdést a lakosság és a politika számára is meggyőző módon meg kell oldania. Hatalmas különbségek mutatkoznak azonban az egy főre jutó energiatermelésben. A gazdaságilag fejlett és fejlődő országok átlagos állampolgárai között csaknem 60-szoros is lehet az eltérés. Napjaink egyik legfontosabb kérdése az, hogy képesek leszünk e kielégíteni a rohamosan növekedő energiafelhasználási igényt, milyen energiatermelő technológiákat fogunk előnyben részesíteni.

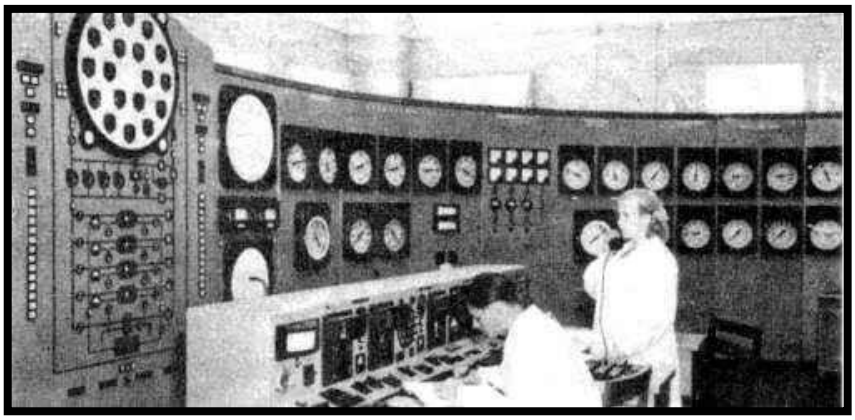
A nukleáris energiatermelés nyújtotta lehetőségeket sokan veszélyesnek tartják, dolgozatunkban arra a kérdésre keressük a választ valóban veszélyesnek mondható e, ez a fajta energiatermelési technológia? Számba vesszük az előnyeit, hátrányait, és az eddig előforduló nukleáris baleseteket. Végezetül a megismert tények alapján megpróbáljuk levonni a megfelelő konklúziókat azzal kapcsolatban, hogy lehet-e a nukleáris energiatermelés a jövőnk vezető energiatermelő technológiája?

NUKLEÁRIS ENERGIATERMELÉS, MINT VESZÉLYES TECHNOLÓGIA

A nukleáris energiatermelés története az első generációs atomerőművek megjelenésével kezdődött el az 1950-60-as években. Az 1. fényképen látható atomerőmű 1954. június 27-én kezdett el üzemelni a Moszkvától mintegy 100 km-re fekvő Obnyinszk városában, amely 10 éven át a Szovjetunió egyetlen atomerőműve volt és közel 48 év szolgálat után 2002-ben zárták be végleg.

Ezt követően a világon párhuzamosan jelentek meg és terjedtek el az Egyesült Államokban, a Szovjetunióban, az Egyesült Királyságban és Franciaországban. Ezek az erőművek a maguk idejében hatalmas szolgálatot tettek, de mára elavulttá váltak és jórészüket üzemen kívül helyezték, vagy felváltották őket a második generációs atomerőművek, amelyek a mai üzemelő erőművek 80-90 % adják. A második generáció kifejlesztésében elsősorban biztonsági és környezetvédelmi szempontok játszottak döntő szerepet. A fejlesztéseknek köszönhetően ezek az erőművek biztonságosabbá, gazdaságosabbá és üzembiztosabbá váltak.

A hazánkban üzemelő és a 2. fényképen látható Paksi Atomerőmű szintén a második generációs atomerőművek családjába tartozik. A Csernobili atomerőmű balesetének következtében (amely szintén a második generációs erőművekhez tartozott) a kutatókat a nukleáris energiatermelés koncepciójának teljes mértékű újragondolására kötelezte.



1. fénykép. 56 éve adták át a világ első atomerőművét a Szovjetunióban. [3]

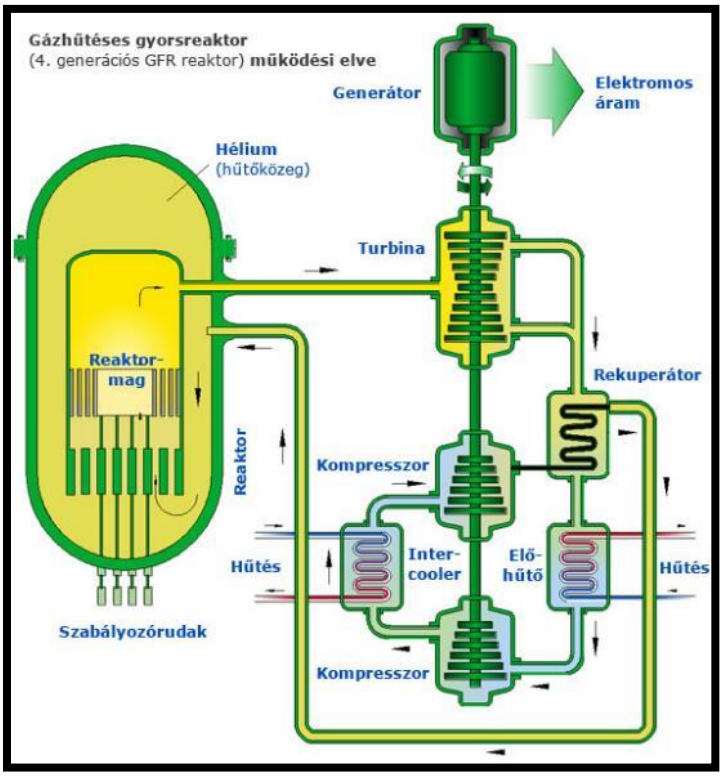
Ezen koncepciók és továbbfejlesztések következményeképpen a 90-es évek elejére megszületett a harmadikgenerációs vagy evolúciós atomerőműveknek is nevezett generációs család az atomerőművek történetében. A tervezés során elsősorban a belső biztonság teljesebbé tételére, a passzív rendszerek arányának növelésére törekedtek a tervező mérnökök. Fontos szempont volt szintén az erőmű élettartamának meghosszabbítása (amely 60 évre növekedett) és a zónaolvadásos balesetek kockázatának és valószínűségének a csökkentése.

2. fénykép. Két reaktor egy csarnokban, a háttérben a kiégett üzemanyagot szállító konténerek. [4]

Napjainkban tervezés alatt van a 2. ábrán látható elven működő atomerőművek negyedik generációja, amely annyiban fog különbözni a harmadik generációtól, hogy itt nem egy továbbfejlesztésről van szó, hanem teljesen új megoldásokat alkalmaznak és új biztonságtechnikai célokat kívánnak kielégíteni.

A negyedik generációs atomerőművek üzembe helyezésével megoldódhat az energiatermelés melléktermékeként keletkező nagy aktivitású hulladékok végleges elhelyezése is. A tervezés viszonylagosan magas költségigénye miatt nemzetközi kereteken belül zajlik több ország részvételével. Becslések szerint az első negyedik generációs atomerőmű üzembe helyezésére 2030-ban kerülhet sor.

Az energiatermelésben jelentős szerepet játszanak globális viszonylatban is az atomerőművek, az álltaluk termelt áram a világ energiatermelésének 16 %-át teszik ki és közel egy milliárd emberhez jut el. Igaz hogy ez az arány az elmúlt évtizedben nem változott, de a globális klímaváltozás következtében bekövetkező kockázatok ismét előtérbe helyezték az biztonságos energia ellátást. Ennek következtében újabb nukleáris beruházások indultak meg. A NAÜ 2005 adatai alapján elmondható, hogy a világon jelenleg 442 üzemelő atomerőmű van, amelyek beépített kapacitása 368 611 GW. Ezen kívül a világ 56 országában mintegy 284 kutatóreaktor üzemel.



3. ábra. Gázhűtéses gyorsreaktor működési elve. [5]

A NUKLEÁRIS LÉTESÍTMÉNYEK BIZTONSÁGA ÉS MEGBÍZHATÓSÁGA

A nukleáris energiatermelés talán egyik legfontosabb kérdése a nukleáris berendezések, köztük az atomerőművek biztonsága és megbízhatósága. E tekintetben már a második generációs atomerőművek is nagyon jók, a harmadik generációsok pedig még jobbak, ennek ellenére a biztonság és a megbízhatóság további folyamatos javítása a jövő nukleáris berendezések kifejlesztésének alapvető prioritása. Ez egyben az atomenergia lakossági elfogadtatását is megkönnyíti.

Az atomreaktorokra vonatkozó alapvető funkciók reaktivitás szabályozás, hő eltávolítás az aktív zónából, radioaktív anyagok kikerülésének korlátozása és sugárvédelem. Annak érdekében, hogy az innovatív nukleáris rendszerek így az atomreaktorok is teljesítsék ezeket a funkciókat, különböző alapelveket, illetve követelményeket kell kielégíteniük.

A megfelelő biztonság és üzembiztosság megteremtése során figyelembe kell venni, hogy annak új kihívásoknak (magasabb hőmérséklet, nagyobb üzemanyag-kiégetés, nagyobb besugárzások stb.) kell megfelelnie. Ez nem csak technikai feladatot, hanem a magas színvonalú üzemeltetés humán feltételeinek magas szinten tartását is jelenti mind a normál üzemeltetés, mind a balesetkezelés területén.[6]

Az atomerőművek biztonsági kérdése azonban nem csak a mérnökök dolga. A csernobili katasztrófához hasonló következmény elkerülése érdekében nemzetközi erőfeszítések születtek elsősorban a megerősített nemzetközi atombiztonsági szabályozás keretein belül. A szektor kockázatainak csökkentését szolgálja az államközi szerződések megkötése, globálisan elfogadott biztonsági szabványok és intézkedések kidolgozása és bevezetése, valamint a fentieket ellenőrző, kiterjedt felügyeleti és tájékoztatási rendszerek létrehozása.

3. fénykép. A csernobili szarkofág napjainkban. [7]

A nukleáris energiatermelés jövőjét érintő kérésre számos válasz látott napvilágot. Vannak, akik a megújuló energiaforrásokban, míg mások pedig az atomenergiában látják az energiatermelés jövőjét és olyanok is akadnak, akik egy teljesen új energiatermelési technológiában reménykednek. Az azonban biztos, hogy a Nemzetközi Atomenergia Ügynökség (IAEA) becslései szerint 2030-ig közel megduplázódhat a világ nukleáris energiatermelése, de a nukleáris energia részaránya a globális energiatermelésben ennek ellenére csökken. Az IAEA elemzői szerint a nukleáris energiatermelés előretörése leginkább a Távol-Keleten és Dél-Ázsiában figyelhető majd meg, elsősorban az óriási fejlődési ütemet produkáló, és ezért rendkívül energiaéhes Kínában és Indiában. [8]

A jelenleg a világon épülő 31 atomerőműből 16 fejlődő országokban létesül, főként Kínában és Indiában. Az IAEA két forgatókönyvet vázol: az egyik szerint csak a már építés, vagy fejlesztés alatt álló létesítmények kezdenek működni 2030-ig, ez esetben a nukleáris energiából nyerhető energiamennyiség csak negyedével nő a jelenlegihez képest a világon. A másik forgatókönyv viszont számos új létesítményt is valószínűsít addig, és ezzel a nukleáris energiatermelés 93 százalékkal haladná meg 2030-ra a jelenlegi szintet. 1960-ban a nukleáris energia a világ energiatermelésének kevesebb, mint 1 százalékát adta. Ez a nyolcvanas évek közepére 16 százalékra nőtt és jelenleg is ezt a szintet tartja. 2030-ra az IAEA becslései szerint részaránya 13 százalékra csökken a globális energiatermelésben. [8]

Hazánk vonatkozásában a Paksi Atomerőmű adja az ország villamos energiatermelésének 39 %-át, ez 1755 MWe teljesítményt jelent, ezért üzemben tartása nélkülözhetetlen. Bezárása esetén a villamos energia ára az egekbe szökne, amely drasztikus életszínvonal csökkenéssel járna, emellett erős villamos áram importfüggőség alakulna ki Magyarország tekintetében, amely szintén negatívan befolyásolná az ország gazdasági helyzetét. Azonban figyelembe kell vennünk, hogy az erőmű blokkjainak üzemideje 30 év, amely 2012-17-ig terjedő ciklusban le fog járni. A megoldás az erőmű fejlesztésében és életciklusának meghosszabbításában rejlik, amelyet már el is kezdtek a Paksi Atomerőműben és az Országos Atomenergia Hivatalban. Továbbá tervben van a Paksi Atomerőmű további két reaktorral való bővítése. A tervek szerint 2020-ra a hazai villamos energiatermelés 60 %-át fogja megtermelni a Paksi erőmű jelenlegi 4 és tervezett 2 blokkja. [9]

Világviszonylatban a nukleáris energiatermelés egyik fontos kérdése, hogy mennyire fogja befolyásolni a nukleáris energiatermelés jövőjét a Csernobili vagy a Fukusimai hoz hasonló nukleáris balesetek? Vajon képesek lesznek a kutatómérnökök lépés tartani a természeti és a technika kihívásaival ezen a területen, hogy ne következhessenek be hasonló méretű nukleáris katasztrófák a jövőben. Úgy gondoljuk, hogy a kérdés megválaszolása igen sürgető, hiszen az emberiség energiaigénye rohamos léptékben nő és a legszerényebb prognózisok is a jelenlegi

igények megduplázódását jósolják 50 éven belül. A másik fontos kérdés a nukleáris energiatermelés melléktermékeként keletkező radioaktív hulladékok tárolási problémájának hosszú távú megoldása. Ez a kérdés az egész iparág jövőjét alapvetően befolyásolhatja és eldöntheti. A jelenlegi mélygeológiai tárolók nyújtotta tárolási lehetőséget a lakosság többsége elutasítja, és nem tartja elképzelhető alternatívának a jövőt illetően. Ezért a probléma új megoldások és megközelítések keresését követeli meg a szakemberektől.

NUKLEÁRIS VESZÉLYEHELYZETEK ÉS HATÁSAIK

Az atomerőművek üzemelése során – bonyolult rendszerről lévén szó – számos apró, vagy nagyobb rendellenesség vezethet üzemzavarhoz, súlyosabb esetben balesethez. Legsúlyosabb következménnyel a nagy primerköri csőtörés következtében fellépő hűtővíz veszteség járhat, melynek során az üzemelő, vagy a már leállított atomerőmű hűtése részben, vagy teljesen megszűnhet és a fűtőelemekben felhalmozódott nagyszámú radioaktív izotóp bomlása során termelt jelentős hőmennyiség megolvaszthatja reaktortartályban lévő hasadóanyagot tartalmazó fém rudakat (pálcákat) és felnyitja a gáz tömör csövek burkolatát. Ezt hívják részleges, vagy teljes zónaolvadásnak. A megolvadt csövek elveszítve gáztömörségüket kiengedik a reaktor tartályba, illetve annak környezetébe az illékony gáz- és gőz-halmazállapotú radioaktív hasadási termékeket, azaz a radioaktív nemesgázokat (argon, xenon, kripton stb.) és a jódizotópok gőzeit. Ezek aztán már tovább juthatnak a reaktor biztonsági tartályába, konténmentjébe és onnan a környezetbe. [10]

Az 1979. március 28-án történt Three Mile Island atomerőmű balesete volt az első komoly kereskedelmi nukleáris baleset az Amerikai Egyesült Államokban. A balesetben TMI-2 blokk sérült meg, amely 907 MW névleges villamos áram teljesítménnyel rendelkezett. A nukleáris katasztrófához egy konstrukciós és egy emberi hiba vezetett, amely következtében először a vészleállító rendszer lépett működésbe majd egy szelep meghibásodása miatt elforrt a hűtőközeg. Ezt követően a fűtőelemek hőmérséklete meghaladta az 1100 ^{0}C-t, a burkolatok felnyíltak és elkezdődött a vízcírkónium reakció. Közel tíz hosszú órába tellett mire stabilizálni tudták az erőmű állapotát a szakemberek. A baleset komoly szakmai kivizsgálás követte, amely hatalmas hatással volt az amerikai reaktorbiztonságra. [11]

A Csernobili atomkatasztrófa 1986. április 26-án következett be az ukrajnai Pripjaty és Csernobil városok melletti atomerőműben. Az atomerőmű építésénél tervezés és költségvetési problémák miatt nem épültek védőépületek ezért a baleset következtében radioaktív hulladék hullott a Szovjetunió nyugtai valamint Európa más részeire és az Amerikai Egyesült Államok keleti részéra. A baleset következtében Oroszországból és Fehéroroszországból közel 200 000 embert kellett kitelepíteni. A katasztrófa okáról két ellentmondó hivatalos állásfoglalás született. Az első, amelyet közvetlenül a baleset után tettek közzé a hatóságok az atomerőművet üzemeltető szakembereket tették felelőssé. A másik állásfoglalás szerint, amely 1991-ben jelent meg a baleset bekövetkezéséért a reaktor tervezési hibáit teszi felelőssé. Szakértői állásfoglalások szerint külön egyik állásfoglalás sem álja meg a helyét, a két hiba közösen vezetett a nukleáris katasztrófa bekövetkezéséhez. Egyrészt az üzemeltetők kikapcsolták a rektor biztonsági rendszereit, ami szigorúan tilos. Másrészt olyan mértékű tervezési hibákat titkoltak el az üzemeltetők elől, amelyek ismeretében elkerülhető lett volna a baleset bekövetkezése. A WHO (World Health Organization) 2005-ös állásfoglalása szerint a szerencsétlenség 70 éves távlatban összességében 4000 áldozatot fog követelni. [12]

A Fukusimai atomerőmű balesete 2011. március 11-én bekövetkezett tóhokui földrengés és az általa keltett szökőár előidézte Japán történelmének egyik legsúlyosabb kereskedelmi jellegű nukleáris katasztrófája, amelyet a csernobili katasztrófával egyenértékűnek 7-es kategóriába soroltak be. A földrengés bekövetkezésekor az atomerőmű 6 reaktorából a 4-es az 5-ös és a 6-os karbantartási munkálatok miatt üzemen kívül volt, az 1-es, 2-es és a 3-as pedig a földrengés

következtében azonnal leálltak, ennek következtében a villamos energiaellátása a reaktorok hűtővizét keringtető szivattyúknak megszűnt. Az energiaellátás kiesését az ilyen vészhelyzetekre telepített dízelgenerátorok beüzemelésével próbálták helyettesíteni, azonban a földrengést követő 55 percben egy 15 méteres árhullám érte el az atomerőmű 5-7 méteres árhullámra tervezett védőfalát. Az árhullám a védőfalakon áttörve megrongálta az erőmű létesítményeit, tengerszivattyúit és a dízelaggregátorok üzemanyag-ellátását és hűtőrendszerét, ezzel megszűnt és leálltak a reaktorok aktív üzemzavari hűtőrendszerei. Egyben kiesett a külön-külön is több száz fűtőelemet tároló *pihentető medencék*, valamint a külön épületben lévő *használtfűtőelem tároló* hűtése is. Az aktív hűtést csak a baleset után 9-órával a helyszínre érkezés után tudták megoldani, ennek hatására a reaktorok hűtővizének vízszintje és az aktív zónák hőmérséklete és a reaktorok nyomása kritikussá vált. Mindezen események egyenes következménye keppen bekövetkezett Japán addigi legsúlyosabb nukleáris balesete. [13]

Nukleáris veszélyhelyzetben fenyeget vagy bekövetkezik a munkahelyen és/vagy a környezetben a sugárzási szint jelentős megnövekedése, radioaktív anyagok megjelenése a nem várt helyeken, jellemzően biztonságosnak ítélt munkahelyi területeken, a lakó környezetben, valamint kiterjedten a környezetben. Az ilyenkor fellépő lehetséges károsító hatások igen kiterjedtek, jellemzően az alábbiak szerint csoportosíthatók:

- determinisztikus egészségkárosító hatás olyan egészséget károsító sugárhatás, amelynek dózisküszöb-értéke van, amely felett a hatás súlyossága a dózissal növekedik;
- sztochasztikus egészségkárosító hatás olyan egészséget károsító sugárhatások, amelyeknek küszöbdózisuk nincs, előfordulásuk valószínűsége arányos a dózissal, súlyosságuk azonban független attól;
- sugárzáshoz nem köthető egyéb egészségkárosító hatás az esetleges pánik miatt kialakuló traumatikus hatások, pszichológiai és pszicho-szomatikus hatások;
- gazdasági hatás lehet a mezőgazdasági, a turisztikai, vagy egyéb gazdasági tevékenység ellehetetlenülése;
- környezeti hatás lehet a környezet elszennyeződése, a természet károsodása. [14]

A nukleáris baleseteket, mint atombomba detonáció segítségével szeretnénk megvilágítani az emberre mért hatásait. A sugárzást alkotó részecskék behatolnak az élő testekbe, roncsolták a sejteket, a vért, megváltoztatják a csontvelő vérképző funkcióját és tönkreteszik a belső szerveket. A sugárzás okozta károsodás mértékét erősen befolyásolja, hogy az áldozat a hipocentrumtól mekkora távolságban van, és, hogy van e valamilyen tárgy, ami takarja. A robbanás követő egy percben kibocsájtott azonnali a hipocentrum 1 kilométeres körzetében a dózis általában halálos. A legtöbben, akik itt tartózkodnak, pár napon belül meghalnak. A magas sugárdózis egyik emberi szervezetre gyakorolt első hatása a hányás. A sugárbetegség kialakulása függ az ekvivalens dózis mértékétől, ami a sugárzás roncsoló hatásától és az abból az élő testet ért dózistól függ. Az ekvivalens dózis SI mértékegysége a Silvert (Sv). Az 1 Sv-nél kevesebb ekvivalens dózist befogadó emberi testben nem alakul ki különösebb betegség, de előfordulhat ingadozás a fehérvérsejtek számában, és rövid időre a férfiak sterillé válhatnak. 1–2 Sv között enyhe tünetek észlelhetőek, ekkora dózis a vérképző szöveteket károsítja.

MAGYARORSZÁG NUKLEÁRIS VESZÉLYEZTETETTSÉGE

Magyarországon kiterjedt módon valósul meg az atomenergia békés célú felhasználása, számos területén segíti elő az életfeltételek javítását. Az atomenergia békés célú felhasználása ugyanakkor jelentős veszélyeket rejt magában: nukleáris veszélyhelyzet alakulhat ki, melynek során radioaktív anyagok kerülhetnek a környezetbe, veszélyeztetve a dolgozók és a lakosság egészségét, károsítva a környezetet, és jelentős gazdasági károkat okozva.

Az atomerőművi esetleges meghibásodások káros következményei elleni védelem utolsó szintjét képviselik azok az intézkedések, amelyek nukleáris veszélyhelyzetben a dolgozók, a lakosság és a környezet védelmét szolgálják: azaz a nukleárisbaleset-elhárítás intézkedések rendszere.

Az Országos Nukleárisbaleset-elhárítási Intézkedési Terv (OBEIT) részletesen áttekinti a Magyarországot, illetve a Magyarországon élőket, tartózkodókat veszélyeztető nukleáris veszélyhelyzeteket, kezdve az ilyen veszélyhelyzetek forrásaként számításba jöhető létesítményekkel és tevékenységekkel. Az OBEIT 2.1. fejezete részletesen ismerteti a hazai nukleáris és radioaktív anyagokat alkalmazó létesítményeket, tevékenységeket, valamint az esetlegesen bekövetkező nukleáris balesetük folytán hazánkat fenyegető külföldi nukleáris létesítményeket.

A baleset-elhárítási tervezés egységesítése céljából a Nemzetközi Atomenergia Ügynökség – a kockázatok nagysága és időbeli változása alapján – a nukleáris létesítmények üzemeltetése, illetve a nukleáris és radioaktív anyagokkal végezhető tevékenységek következtében lehetséges nukleáris veszélyhelyzetek besorolására öt veszélyhelyzeti tervezési kategóriát (VTK) ajánl, amelyek általános ismertetését az alábbi fejezetek tartalmazzák. A Magyarországot veszélyeztető létesítmények és tevékenységek közé a hazai nukleáris és radioaktív anyagokat alkalmazó létesítmények, a radioaktív anyagokkal végzett tevékenységek és egyes külföldi nukleáris létesítmények tartoznak. Követve az OBEIT 2. fejezetében foglaltakat e létesítmények és tevékenységek nukleáris veszélyhelyzeti tervezési kategóriába sorolása a következő:

I. kategória: Paksi Atomerőmű

II. kategória: A Kiégett Kazetták Átmeneti Tárolója (KKÁT), Budapesti Kutatóreaktor, Izotópintézet Kft.

III. kategória: Budapesti Műszaki és Gazdaságtudományi Egyetem Oktatóreaktor, Püspökszilágyi Radioaktív Hulladék feldolgozó és Tároló Telep (RHFT), Nemzeti Radioaktív Hulladéktároló, Bátaapáti.

V. kategória: Bohunice Atomerőmű, Mohovce Atomerőmű, Krsko Atomerőmű, Dukovany Atomerőmű, Temelin Atomerőmű. [14]

A következő táblázat megadja, hogy az egyes nukleáris veszélyhelyzeti osztályok mely létesítményekben, illetve tevékenységek során bekövetkező veszélyhelyzetek esetén értelmezhetőek.

Veszélyhelyzeti osztály	**Létesítmény, tevékenység**
Általános veszélyhelyzet	Paksi Atomerőmű
Helyi veszélyhelyzet	Paksi Atomerőmű, Kiégett Kazetták Átmeneti Tárolója, Budapesti Kutatóreaktor, Izotópintézet Kft., radioaktív anyagokkal végzett tevékenységek
Létesítményi veszélyhelyzet	Paksi Atomerőmű, Kiégett Kazetták Átmeneti Tárolója, Budapesti Kutatóreaktor, Izotópintézet Kft., Budapesti Műszaki és Gazdaságtudományi Egyetem Oktatóreaktor, nagy aktivitási radioaktív anyagokat alkalmazó létesítmények,
Potenciális veszélyhelyzet	Paksi Atomerőmű, Kiégett Kazetták Átmeneti Tárolója, Budapesti Kutatóreaktor, Izotópintézet Kft., Budapesti Műszaki és Gazdaságtudományi Egyetem Oktatóreaktor, nagy aktivitási radioaktív anyagokat alkalmazó létesítmények, radioaktív anyagokkal végzett tevékenységek

1. táblázat. Veszélyhelyzeti osztályok létesítményekben, tevékenységek során [14]

A következő táblázat a károsító hatásokat, lehetséges következményeket foglalja össze a definiált veszélyhelyzeti osztályok szerint.

A legtöbb veszélyhelyzet-típus esetén a rendszabályok bevezetésére a telephelyen és telephelyen kívül kerülhet sor. Létesítmények esetében jelentős, telephelyen kívüli szennyeződést

vagy sugárterhelést eredményező veszélyhelyzet bekövetkeztekor (I. és II. veszélyhelyzeti tervezési kategóriába eső létesítmény) a tervezés szintje a létesítménytől való távolság függvényében változik. Ezen létesítményeket illetően, a tervezés a sürgős óvintézkedések esetében három veszélyhelyzeti tervezési zónára korlátozódik.

Megelőző Óvintézkedések Zónája (MÓZ) az I. tervezési kategóriába tartozó létesítmények esetében előre kijelölt terület, amelyre a sürgős óvintézkedéseket előzetesen megtervezik, és azok végrehajtását az Általános Veszélyhelyzet megállapítását követően azonnal elrendelik. Cél a súlyos determinisztikus hatások megelőzése a zónában óvintézkedések végrehajtásával a kibocsátást megelőzően vagy röviddel azt követően.

Sürgős Óvintézkedések Zónája (SÓZ) az I. vagy II. tervezési kategóriába tartozó létesítmények esetében előre kijelölt terület, amelyre a sürgős óvintézkedéseket előzetesen megtervezik. A SÓZ-ban a környezeti monitorozási adatok és a létesítmény állapotának értékelése alapján elrendelt, sürgős óvintézkedések végrehajtását azonnal megkezdik a vonatkozó jogszabályokban meghatározott dózisok elkerülése céljából. A III. és IV. veszélyhelyzeti tervezési kategóriára a MÓZ és a SÓZ kijelölése általában nem indokolt.

A MÓZ és a SÓZ nagyjából kör alakú területek a létesítmény körül, amelyek határait a beavatkozás alatt is jól felismerhető tereptárgyak (pl. utak, folyók) alapján kell kijelölni, amelyek megkönnyítik az azonosítást. Fontos megjegyezni, hogy a zónák nincsenek tekintettel a nemzeti határokra. A zónák méreteit a potenciális következmények elemzése alapján lehet meghatározni.

Veszélyhelyzeti osztály	**Létesítmény, tevékenység**	**Következmények**	**Kiterjedés**
Általános veszélyhelyzet	Paksi Atomerőmű	determinisztikus, sztochasztikus, nem-radiológiai, gazdasági, környezeti	általános, nagy kiterjedés, több 10, 100 km
Helyi veszélyhelyzet	Paksi Atomerőmű, Kiégett Kazetták Átmeneti Tárolója, Budapesti Kutatóreaktor, Izotópintézet Kft., radioaktív anyagokkal végzett tevékenységek	determinisztikus, sztochasztikus, nem-radiológiai, gazdasági, környezeti	telephely, telephelyen kívüli, néhány 100 m, néhány km
Létesítményi veszélyhelyzet	Paksi Atomerőmű, Kiégett Kazetták Átmeneti Tárolója, Budapesti Kutatóreaktor, Izotópintézet Kft., Budapesti Műszaki és Gazdaságtudományi Egyetem Oktatóreaktor, nagy aktivitási radioaktív anyagokat alkalmazó létesítmények,	determinisztikus, sztochasztikus, nem-radiológiai, gazdasági	létesítményen belül
Potenciális veszélyhelyzet	Paksi Atomerőmű, Kiégett Kazetták Átmeneti Tárolója, Budapesti Kutatóreaktor, Izotópintézet Kft., Budapesti Műszaki és Gazdaságtudományi Egyetem Oktatóreaktor, nagy aktivitási radioaktív anyagokat alkalmazó létesítmények, radioaktív anyagokkal végzett tevékenységek	nem-radiológiai, gazdasági	létesítményen belül, a tevékenység szűk körzetében

2. táblázat. Veszélyhelyzeti osztályok és a létesítmények, tevékenységek [14]

Élelmiszer-fogyasztási Korlátozások Óvintézkedési Zónája (ÉÓZ) az a terület, amelyen belül szükségessé válik a lakosság élelmiszer-fogyasztásának korlátozása, a mezőgazdasági termelők és az élelmiszer-feldolgozó ipar ellenőrzése, tevékenységük szükség szerinti, szigorú rendeleti szabályozása, illetve korlátozása. Az ÉÓZ-ban a védekezés alapvetően a helyi termelésű élelmiszerek fogyasztásának előre megtervezett korlátozását jelenti a lenyelt sugárzó anyagok sztochasztikus hatásainak csökkentése céljából. A lakosság esetleges áttelepítése, az élelmiszerkorlátozás és a mezőgazdaságban foganatosítandó védelmi rendszabályok elrendelése a

környezeti ellenőrzésen és élelmiszerminták elemzésén alapszik, a tapasztalatok szerint több száz km távolságig kell élelmiszer-korlátozással számolni. [14]

A következő táblázat összefoglalja, hogy az egyes óvintézkedési zónákban jellemzően milyen károsító hatásokra, következményekre kell számítani.

Nukleáris veszélyhelyzeti következmények	**Óvintézkedési zónák**		
	MÓZ	**SÓZ**	**ÉÓZ**
determinisztikus	x	x	-
sztochasztikus	x	x	x
nem-radiológiai	x	x	x
gazdasági	x	x	x
környezeti	x	x	x

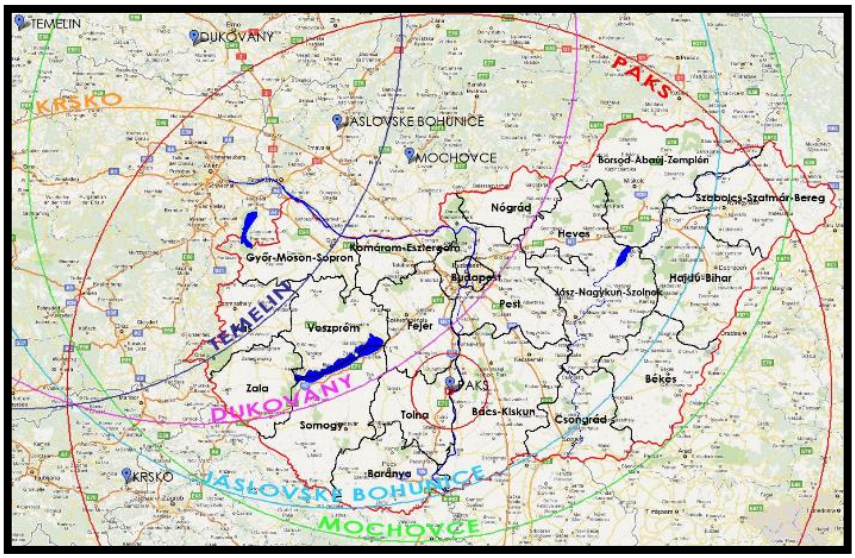
3. táblázat. Az óvintézkedési zónákban jellemző következmények [14]

A Magyarországon nukleáris veszélyhelyzetet okozható létesítmények tervezési zónáinak megnevezését és területi kiterjedését a következő táblázat mutatja be.

	MÓZ	**SÓZ**	**ÉÓZ**
I. VTK			
Paksi Atomerőmű	3 km	30 km	300 km
II. VTK			
KKÁT	-	-	3 km
Budapesti Kutatóreaktor	-	KFKI telephely	1 km
Izotópintézet Kft.	-	KFKI telephely	1 km
III. VTK			
BME Oktatóreaktor	-	-	-
RHFT	-	-	3 km
NRHT	-	-	3 km
V. VTK			
Bohunice	3 km	30 km	300 km
Mohovce	3 km	30 km	300 km
Krsko	3 km	30 km	300 km
Dukovany	3 km	30 km	300 km
Temelin	3 km	30 km	300 km

4. táblázat. Tervezési zónák megnevezése és területi kiterjedése [15]

A fenti táblázat számokkal kifejezett adatait a soron következő ábra már térképes formában is szemlélteti. Valamennyi az fenti táblázatban feltüntetett atomerőmű már hosszabb ideje működik, többségük azonos típusú VVER-440/213 reaktorblokkokkal üzemel. Valamennyi atomerőmű szigorú nemzeti hatósági felügyelet alatt áll, és biztonsági szintjük kielégíti a nemzetközi elvárásokat és követelményeket. Az előzőekben vázolt következményekkel járó nukleáris veszélyhelyzet bekövetkezésének gyakorisága az elvégzett kettesszintű Valószínűségi Biztonsági Elemzések szerint $10^{-7} \div 10^{-6}$ reaktorév^{-1} gyakoriság tartományba esik. A Rendeltben alkalmazott gyakoriság terminológia szerint az ilyen események a nagyon ritka gyakoriságtartományba tartoznak. [16]



5. ábra. Magyarország nukleáris veszélyeztetettsége [16]

AZ ORSZÁGOS NUKLEÁRISBALESETELHÁRÍTÁSI RENDSZER

Hazánkban a bekövetkezett radiológiai, illetve nukleáris események elhárításáért, az ellenük való védekezésért és esetleges bekövetkezésük esetén a következmények csökkentéséért az Országos Nukleárisbalesetelhárítási Rendszer (ONER) a felelős.

Az ONER elsődleges feladata a hazai nukleáris létesítmények, valamint radioaktív anyagokat használó tároló üzemek, üzembe helyezése, üzemeltetése során bekövetkező nukleáris veszélyhelyzetek elhárítása. A rendszer működését az országos nukleárisbaleset-elhárítási rendszerről szóló 167/2010. (V.11.) Korm. rendelet (továbbiakban: Rendelet) szabályozza. További feladatai közzé tartozik a nukleáris és radioaktív anyagok szállítása közben bekövetkezett balesetek, az ország területén kívül történt nukleáris katasztrófa helyzetek kezelése a lakosság hiteles és időbeli tájékoztatása. Az ONER felépítése a következő ábrán látható.

6. ábra. Országos Nukleárisbaleset-elhárítási Rendszer felépítése. [17]

Az ONER irányításával kapcsolatos feladatokat a kormányzati koordinációs szerv, a Katasztrófavédelmi Koordinációs Kormánybizottság (a továbbiakban: KKB) látja el, amely a Kormány katasztrófavédelemmel összefüggő döntéseinek előkészítését és a védekezéssel kapcsolatos feladatok ágazati összehangolását végző szerv.

Az atomenergia békés célokra való felhasználása során bekövetkező radiológiai, vagy nukleáris események elhárítására való felkészülésről, a bekövetkezett esemény következményeinek csökkentéséről és megszüntetéséről az Országos Nukleárisbaleset-elhárítási Rendszer (a továbbiakban: ONER) gondoskodik. Az ONER a lakosság nem tervezett sugárterhelését előidéző események megelőzésében, az ilyen esemény következményeinek csökkentésében és megszüntetésében érintett központi, ágazati, területi és helyi szintű szervek és szervezetek összessége.

Az ONER és a nukleáris veszélyhelyzet elleni védekezés tervezése, irányítása és a végrehajtásának összehangolása kormányszintű feladat. A korszerű államigazgatási struktúrának megfelelően megújításra kerültek a katasztrófavédelmi és az országos nukleárisbaleset-elhárítási rendszert szabályozó jogszabályok.

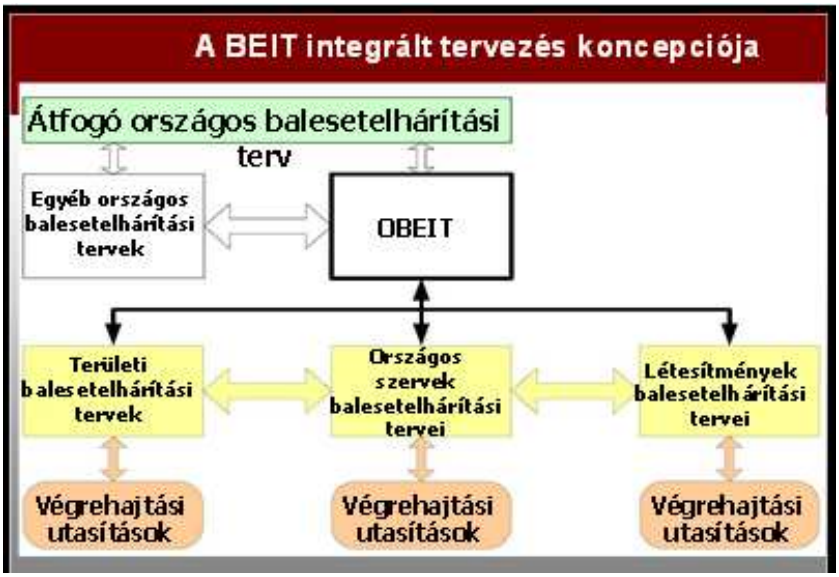
Az országos katasztrófavédelmi rendszer felépítését, a katasztrófák elleni védekezésben érintett miniszterek és állami szervek megelőzéssel, felkészüléssel és védekezéssel kapcsolatos feladatait, valamint a katasztrófavédelmi kormányzati koordinációs szerv feladatait, a Kat. tv., valamint az annak végrehajtásáról szóló 234/2011. (XI. 10.) Korm. rendelet szabályozza.

Az ONER irányításával kapcsolatos feladatokat a kormányzati koordinációs szerv, a Katasztrófavédelmi Koordinációs Kormánybizottság (KKB) látja el, amely a Kormány katasztrófavédelemmel összefüggő döntéseinek előkészítését és a védekezéssel kapcsolatos feladatok ágazati összehangolását végző szerv. Az ONER működési állapotának megváltoztatását az Országos Atomenergia Hivatal (OAH) főigazgatójának a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: BM OKF) főigazgatója útján tett kezdeményezésére a Belügyminiszter rendeli el.

A biztonságot kedvezőtlenül befolyásoló és a lakosság nem tervezett sugárterhelését előidéző esemény következtében a nukleárisbaleset-elhárítási veszélyhelyzet kihirdetésére vagy annak megszüntetésére a kormányzati koordinációs szerv elnöke tesz javaslatot a Kormány számára.

Az ONER működési rendjét a kormányzati koordinációs szerv a központi veszély-elhárítási terv részeként, az Országos Nukleárisbaleset-elhárítási Intézkedési Tervben (a továbbiakban: OBEIT) állapítja meg. Az ONER normál vagy – ettől eltérő esetben – magasabb szintű működési állapotban működik, amely lehet készenléti, veszélyhelyzeti és helyreállítási működési állapot. [14]

A kormányzati koordinációs szerv döntés-előkészítő és döntéshozó tevékenységéhez szükséges információk biztosítása érdekében Országos Sugárfigyelő, Jelző és Ellenőrző Rendszer (a továbbiakban: OSJER) működik. Az OSJER működésének összehangolását és szakmai munkájának irányítását a katasztrófák elleni védekezésért felelős miniszter végzi.



7. ábra. A BEIT integrált tervezési koncepciója. [18]

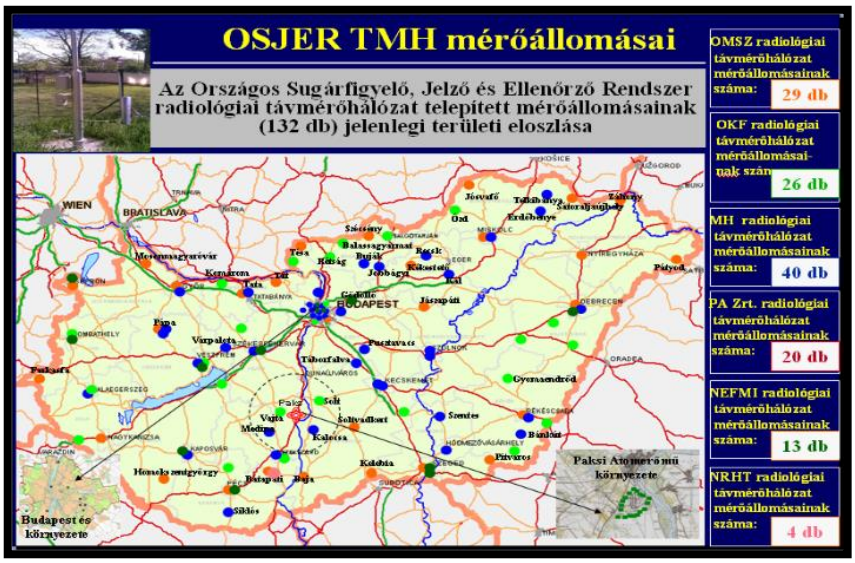
Az OSJER vezető szerve a hivatásos katasztrófavédelmi szerv központi szervének Nukleáris Baleseti Információs és Értékelő Központja (a továbbiakban: NBIÉK). A BM OKF a Rendeletben rögzítettek szerint folyamatosan tervezi, szervezi a lakosság országos sugárzási helyzettel kapcsolatos normál és rendkívüli időszaki tájékoztatását, végzi az országos sugárhelyzet-értékelését, melynek érdekében készenléti ügyeleti szolgálatot működtet. Felügyeli a területi katasztrófavédelmi igazgatóságokon működő Területi Információs Központok (TIK) munkáját, valamint háttérsugárzási adatokat biztosít a megyei sugárzási helyzetértékeléshez. Közreműködik a Magyar Honvédség Görgei Artúr Vegyivédelmi Információs Központ Atom-, Biológiai-, Vegyi Riasztási és Értesítési Rendszer (ABV RIÉR) katasztrófavédelemre háruló feladatainak végrehajtásában, továbbá részt vesz a hazai és nemzetközi nukleárisbaleset-elhárítási gyakorlatokon.

A Katasztrófavédelmi Koordinációs Kormánybizottság döntés-előkészítő és döntéshozó tevékenységéhez szükséges információk biztosítása érdekében Magyarországon Országos Sugárfigyelő, Jelző és Ellenőrző Rendszer (OSJER) működik. Az OSJER működésének összehangolását és szakmai munkájának irányítását a katasztrófák elleni védekezésért felelős miniszter végzi. Az OSJER vezető szerve a BM OKF bázisán működő Nukleáris Baleseti Információs és Értékelő Központ (NBIÉK) - más néven Nukleárisbaleset-elhárítási Osztály -, amely többek között ellátja az ország nukleárisbaleset-elhárítási korai előrejelzés központi feladatait.

Az OSJER-t három alrendszer alkotja.

A Radiológiai Távmérő Hálózat telepített automata távmérőállomásokból áll, amelyek az ország nukleárisbaleset-elhárítási korai riasztási rendszereként működnek, folyamatosan ellenőrzik az ország környezeti sugárzási dózisteljesítményét és a fontosabb lokális meteorológiai paramétereket. Jelenleg 6 ágazat 132 mérőállomásáról érkeznek gamma-dózisteljesítmény adatok a BM OKF-en működő országos radiológiai monitoring központba. [14]

A Mobil Radiológiai Laboratóriumok hálózata a sugárszennyezés felderítését, elemzését végzi veszélyhelyzetek esetén. Ennek érdekében minden évben nemzeti és nemzetközi szintű összemérési gyakorlatok kerülnek megrendezésre a technikák és a munkamódszerek tökéletesítése, valamint az állomány felkészítése érdekében. Jelenleg 6 db speciális, izotóp szelektív mérések elvégzésére is alkalmas sugárvédelmi mérő kocsi található a rendszerben, de kiemelt jelentőséggel bírnak az azonnali beavatkozásra képes, alapszintű radiológiai méréseket végző megyei katasztrófavédelmi igazgatóságok alárendeltségében - 2012. április 1-jével katasztrófavédelmi mobil labor néven - működő veszélyhelyzeti felderítő egységek (korábban veszélyhelyzeti felderítő csoportok és veszélyhelyzeti felderítő szolgálat néven működtek).



8. ábra. Az OSJER TMH mérőállomásai. [18]

A Katasztrófavédelmi Mobil Laborok (KML) biztosítják a veszélyhelyzet értékelését szolgáló kiinduló adatok gyűjtéséhez, rendszerezéséhez és feldolgozásához, valamint a mérgező vagy sugárzó anyagok helyszíni és laboratóriumi meghatározásához szükséges feltételeket, és szükség esetén közreműködnek a mentesítési feladatok koordinációjában. Jelenleg az országban 19 KML áll készenlétben, közülük egy, a fővárosban 24/72 órás szolgálatot lát el. A megyei katasztrófavédelmi igazgatóságokon a kiképzett munkatársakból álló 3 fős csoportok heti váltásos ügyeleti szolgálati rendben dolgoznak. Riasztás esetén a megyei KML munkaidőben 20, munkaidőn túl 60 percen belül, míg a fővárosi KML 2 percen belül kezdi meg vonulását a kárhelyszínre. [14]

Az OSJER harmadik alrendszere a Helyhez Kötött Laboratóriumok Hálózata, mely a beszállított minták (élelmiszer, tej, talaj, víz, stb.) radioaktivitásának mérését végzi. Ezek a mérések teremtik meg a hosszú távú óvintézkedések (legeltetési tilalom, élelmiszer és vízfogyasztás korlátozása, stb.) bevezetésének alapját. Az OSJER-ben jelenleg 7 db helyhez kötött radiológiai laboratóriumi mérő és ellenőrző hálózat található (a Vidékfejlesztési Minisztérium alárendeltségében működő két hálózat, a Nemzeti Erőforrás Minisztérium, a Magyar Tudományos Akadémia, az Országos Meteorológiai Szolgálat, a Paksi Atomerőmű Zrt. és az RHK Kft. laboratóriumai), melyekkel a BM OKF NBIÉK, mint az OSJER vezető szerve szoros együttműködést ápol.

9. ábra. A BM OKF Katasztrófavédelmi Mobil Laboratóriuma [18]

A nukleárisbaleset-elhárításban − normál és veszélyhelyzeti időszakban egyaránt − nagy jelentősége van a hiteles tájékoztatásnak, a független, folyamatos, helyi és országos szintű sugárzási helyzetértékelésnek és az egységes döntéstámogató rendszerek folyamatos készenlétben tartásának a lakosság védelmének hatékonyabb biztosítása érdekében. Ilyen nemzetközi döntéstámogató rendszer a BM OKF RODOS elnevezésű, valós idejű, online, nukleárisbaleset-elhárítási terjedésszámító és döntéstámogató rendszere is.

A határokon átnyúló következményekkel járó esetleges balesetek hatékonyabb kezelése érdekében számos ország rendelkezik együttműködési megállapodással és nemzetközi adatcsere rendszerekkel. Ilyen rendszer az *Európai Radiológiai Adatcsere Platform (EURDEP)* is. Az

Európai Unió minden tagországa számára kötelező jellegű az adatszolgáltatás ebbe a rendszerbe, de az Unión kívüli országok is csatlakozhatnak a kezdeményezéshez. Azok az országok, melyek beküldik adataikat a rendszerbe, láthatják az összes többi tagállam sugárzásmérési eredményeit, ami elősegíti a nemzetközi szintű döntéstámogatást és lakossági tájékoztatást.

Az Európai Atomenergia-közösség létrehozásáról szóló EURATOM szerződés 36. cikkelye és az EURDEP szerződés értelmében az NBIÉK ellátja a nemzetközi radiológiai monitoring adatcsere rendszer nemzeti központ feladatait**,** az ország nemzetközi értesítési kötelezettségének teljesítése érdekében radioaktív szennyezettségre jellemző adatokat biztosít. [19]

10. ábra. A BM OKF radiológiai adatcsere kapcsolatrendszere. [18]

Az ONER megfelelő működése, Nukleáris balesetelhárítási gyakorlatok alkalmával ellenőrizhető le. Ilyen gyakorlás volt az Országos Katasztrófavédelmi Főigazgatóság és az Országos Atomenergia Hivatal által közösen 2013 októberében megtartott szimuláció, amelyben az ország 7 megyéje és 28 járása volt érintett és a fukusimai atomerőmű balesettel azonos üzemzavarokat, áramellátási problémákat, hűtéskiesést és fűtőelem-olvadást szimuláltak a szakemberek. [20]

A Honvédelmi Katasztrófavédelmi rendszer (továbbiakban HKR) szorosan illeszkedik az Országos Nukleáris balesetelhárítási Rendszerhez. A HKR vezető szervei, illetve a rendszerbe kijelölt erők minden katasztrófatípus esetén rögzített feladatrendnek megfelelően működnek. Nukleáris esemény bekövetkezése esetén a HKR kijelölt erői közül az adott katasztrófatípus elhárítására leginkább igénybe vehető munkacsoportok részvétele várható. A nukleárisbaleset-elhárítási feladatok végrehajtására elsősorban vegyi-védelmi és műszaki, továbbá más szakterületi ismeretekkel rendelkező, nukleárisbaleset-elhárítási ismeretekből felkészített, egyéni védőeszközökkel felszerelt személyi állomány kerül alkalmazásra. [21]

ÖSSZEGZÉS

Összességében elmondható, hogy a nukleáris energiatermelés veszélyes üzemnek mondható, amellyel ha nem, jól bánunk akkor bizony súlyos következményekkel kell számolnunk. Éppen ezért nem elfogadható egyetlen embernek a sebesülése vagy halála sem, mely megakadályozható lenne. Az energiatermelés viszont az emberi faj létfenntartásának nélkülözhetetlen szegmense ezért szükségünk van rá, ezt mindenki elfogadja. A kérdés azonban az, milyen árat áldozunk ezért. A csernobili baleset után az atomerőműveket elkezdték világszerte leszerelni (az egyébként biztonságosakat is), míg fel nem ismerték, hogy nem szabad lemondani az atomenergiáról.

Fontos, hogy minden nemzet rendelkezzen egy olyan képességekkel rendelkező szervezettel, amely képes egy esetleges nukleáris baleset bekövetkezése esetén a megfelelő megelőzési, védekezési és kárfelszámolási feladatokat végrehajtani.

Hazánkban az Országos Katasztrófavédelmi Főigazgatóság működteti az Országos Nukleárisbalesetelhárítási Rendszert, amely elsődleges feladata a radiológiai és nukleáris balesetekkel kapcsolatos megelőzési, védekezési és helyreállítási feladatok ellátása. A Honvédelmi Katasztrófavédelmi rendszer, amely szerves részét képezi az Országos katasztrófavédelmi rendszernek szorosan kapcsolódik az ONER-hez kiegészítve és erősítve azt ezzel biztosítva Magyarország nukleáris biztonságát.

FELHASZNÁLT IRODALOM

[1] Agency of Natural Resources and Energy: A világ primer energiaigényének alakulása 1860-1990 között millió tonna kőolajra vonatkoztatva. http://rexades.blog.hu/2009/06/04/a_nuklearis_energiatermeles (letöltés: 2014. 04. 30)

[2] Rusz Tímea: Atomenergia biztonság a bővülő Európai Unióban. http://elib.kkf.hu/edip/D_9966.pdf (letöltés: 2014. 04. 30)

[3] Kecskeméti Gábor: A világ első atomerőművének „születésnapja" http://oroszvilag.hu/?t1=tortenelem&hid=862 (letöltés: 2014. 04. 30)

[4] Paksi Atomerőmű Zrt.: Két reaktor egy csarnokban, a háttérben a kiégett üzemanyagot szállító konténerek http://www.atomeromu.hu/galeria-fototar-videotar (letöltés: 2014. 04. 30)

[5] Sipos Géza: Világelső kísérleti atomerőmű épülhet Magyarországon http://www.origo.hu/idojaras/20110117-negyedik-generacios-atomeromu-gyorsreaktor-vilagelso-kiserleti-atomeromu-epulhet-magyarorszagon.html (letöltés: 2014. 05. 13)

[6] Dr. Csom Gyula: Sipos: Nemzetközi összefoglalás a 21. század atomenergetikájáért. http://www.reak.bme.hu/fileadmin/user_upload/felhasznalok/csom/nemzetkozi_osszefogas_a_21_szazad_atomenergetikajaert.pdf (letöltés: 2014. 05. 13)

[7] Mészáros Tamás: Atomenergia: a múlt vagy a jövő technológiája? http://kitekinto.hu/europa/2011/04/28/atomenergia_a_mult_vagy_a_jov_technologiaja_i.&lap=3 (letöltés: 2014. 05. 13)

[8] MTI: 2030-ig megduplázódhat a nukleáris energiatermelés a világon http://www.stop.hu/articles/article.php?id=216620 (letöltés: 2014. 05. 13)

[9] Csom Gyula: Nemzetközi összefogás a 21. század atomenergiájáért. http://www.reak.bme.hu/fileadmin/user_upload/felhasznalok/csom/nemzetkozi_osszefogas_a_21_szazad_atomenergetikajaert.pdf (letöltés: 2014. 05. 13)

[10] Pátzay György; Kossa György; Grósz Zoltán: Atomerőművek biztonsága és az atomerő művi balesetekből, üzemzavarokból levonható következtetések. http://www.vedelem.hu/letoltes/tanulmany/tan477.pdf (letöltés: 2014. 05. 13)

[11] MVM Paksi Atomerőmű Zrt. : Balesetek. http://www.atomeromu.hu/balesetek (letöltés: 2014. 05. 15)

[12] Rausch Péter: A nukleáris energiatermelés helyzete és szerepe a jelenkori társadalomban. http://rexades.web.elte.hu/letoltes/rpszakdolgozat.pdf (letöltés: 2014. 05. 15)

[13] Prof. Dr. Aszódi Atilla, Boros Ildikó, Yamaji Bogdán: A fukusimai atomerőmű balesetének lefolyása, következményei, tapasztalatai és európai vonatkozásai. http://www.reak.bme.hu/fileadmin/user_upload/felhasznalok/aszodi/letoltes/Japan/Aszodi_ObudaiEgyetem_20111004.pdf (letöltés: 2014. 05. 16)

[14] Bognár Balázs, Kátai-Urbán Lajos, Kossa György, Kozma Sándor, Szakál Béla, Vass Gyula: Kátai-Urbán Lajos (szerk.) IPARBIZTONSÁGTAN I.: Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához. Budapest: Nemzeti Közszolgálati és Tankönyvkiadó, 2013. 564 p. (ISBN:978-615-5344-12-1)

[15] Kátai-Urbán Irina; Vass Gyula: Veszélyes tevékenységek osztályozása és áttekintő értékelése Magyarországon. Bolyai Szemle XXIII. évfolyam 2014. 3. szám pp. 70-87.

[16] Nemzeti Katasztrófa Kockázat Értékelés, Magyarország. BM OKF Budapest, 2011.

[17] Dr. Vincze Árpád: A Nukleárisbaleset-elhárítás alapjai. http://www.zmne.hu/tanszekek/vegyi/personal/NukleBalesetElharitas.pdf (letöltés: 2014. 05. 13)

[18] Taskó-Szilágyi Eszter: A nukleáris baleset-elhárítás országos rendszere. Előadás NKE Katasztrófavédelmi Intézet. 2014.

[19] Szakál Béla, Kátai-Urbán Lajos, Vass Gyula: Veszélyes anyagok és ipari katasztrófák III. (egyetemi jegyzet), Budapest: Szent István Egyetem Ybl Miklós Főiskolai Kar, 2008. 116 p. ISBN: 978-963-2691-15-2

[20] BM OKF: Eredményesen zárult az országos nukleárisbaleset-elhárítási gyakorlat. http://www.katasztrofavedelem.hu/index2.php?pageid=press_sajto_olvas&kid=747 (letöltés: 2014. 05. 25)

[21] Dr. Nagy Károly, Dr. Halász László: Katasztrófavédelem. http://hhk.uni-nke.hu/uploads/media_items/nagy-halasz-katasztrofavedelem.original.pdf (letöltés: 2014. 05. 25)

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Balog Károly
balog.karoly07@gmail.com

DIGITÁLIS PMR RENDSZEREK ÖSSZEHASONLÍTÁSA I.

Absztrakt

Cikkemben a hagyományos analóg rendszereket fokozatosan leváltó elterjedtebb FDMA[1] típusú digitális PMR[2] szabványok, rendszerező, összehasonlító elemzésének eredményeit foglalom össze. Ismertetem a feldolgozott szabványokból, egyéb technikai leírásokból megismerhető, általános, és azoktól eltérő egyedi megoldásokat, eljárásokat, melyekből következtetéseket vonok le a felderítésük és azonosításuk lehetséges ismérveire, technikai paramétereik megállapításán keresztül. Az ismérvek megállapításának célja az alacsony szintű analóg és digitális beszédtípusú PMR adások felderítésére, azonosítására a beszédinformáció kinyerésére univerzálisan alkalmazható eszköz paramétereinek, a vételi képességek tulajdonságainak kidolgozása.

This article summarizes the results of the comparative analysis of the more common FDMA type digital PMR systems, which gradually replace the presented analog systems. I describe the commonly used and unique solutions and procedures from the processed standards, technical descriptions and from which conclusion are set out in the radio detection and identification of possible criteria, through technical parameters. The goal of develop parameters is the low-level analog and digital, voice type PMR transmission detection, identification, speech information extraction for the determination of parameters of the radio reception capabilities, in the universally applicable device.

Kulcsszavak: *PMR (Professional/Private Mobile Radio), DMR (Digital Mobile Radio), dPMR (Digital PMR), LLVI (Low Level Voice Intercept), COMINT (Communications Intelligence) ~ professzionális / magán mobil rádió, digitális mobil rádió, digitális professzionális mobil rádió, alacsonyszintű beszédtípusú kommunikációs jelek felderítése, kommunikációs felderítés*

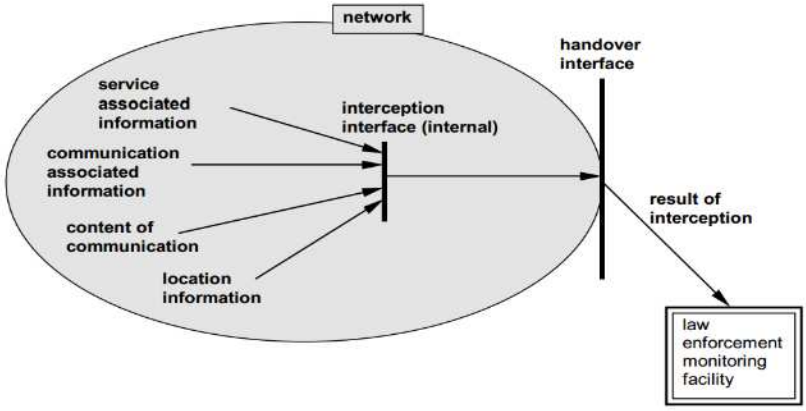
[1] FDMA: Frequency Division Multiple Access – frekvenciaosztásos többszörös hozzáférési (rádiócsatorna megosztási) eljárás
[2] PMR: Professional / Private Mobile Radio - professzionális / magán mobil rádió: A felhasználók által saját maguknak nyújtott zártkörű rádióalkalmazások gyűjtőneve

BEVEZETÉS

A két cikkből álló sorozat első részében, a hagyományos, analóg PMR rendszereket fokozatosan leváltó – frekvenciaengedélyhez kötött és nem kötött formában egyaránt alkalmazható – világviszonylatban elterjedtebb digitális PMR szabványok közül, az FDMA típusú keskenysávú szabványok rendszerező, összehasonlító elemzésének eredményeit foglalom össze. Ismertetem a feldolgozott szabványokból, specifikációkból, egyéb technikai leírásokból megismerhető általános, és azoktól eltérő egyedi megoldásokat, eljárásokat, melyekből következtetéseket vonok le a felderítésük és azonosításuk lehetséges ismérveire, technikai paramétereik megállapításán keresztül. Az ismérvek megállapításának célja az alacsony szintű analóg és digitális beszédtípusú PMR adások jeleinek felderítésére, azonosítására a beszédinformáció kinyerésére univerzálisan alkalmazható eszköz paramétereinek, vételi képességeinek tulajdonságainak kidolgozása. Ez főleg a nemzetbiztonsági, de a katonai felderítés számára is jelentőséggel bír, mivel ezek a rendszerek és az egyedi készülékek képesek kikerülni a hagyományos távközlési infrastruktúrákat, így ebben az esetben felderítésük, ellenőrzésük kizárólag rádiós úton a kommunikációs felderítés eszközrendszerével lehetséges. A cikk tervezett II. részében a TDMA[3] típusú szabványok vizsgálatát fogom a fenti módszerek segítségével elvégezni, így az I. és II. rész együttesen fog áttekintést nyújtani a digitális PMR szabványokról.

A KOMMUNIKÁCIÓS ELLENŐRZÉS ÉS A TÖRVÉNYES ELLENŐRZÉS KAPCSOLATA

Az un. törvényes ellenőrzésnek (LI)[4] a távközlési rendszerekkel szemben támasztott általános technikai követelményeit európai szinten az ETSI[5] szabványok tartalmazzák. Az ETSI 1991 óta vezető szerepet tölt be az LI szabványosításában. Ezek egyes országokra vonatkozó konkrét szabályait pedig általában a nemzeti távközlési /hírközlési/ törvényekben és egyéb ország specifikus jogszabályokban rögzítik. A törvényes ellenőrzésnek egyre nagyobb szerepe van a nemzetbiztonságban, a terrorizmus elleni harcban, és a súlyos bűncselekmények kivizsgálásában, megelőzésében egyaránt [1], azonban nem mindenható eszköz a távközlés ellenőrzésében. Az LI szabványos egyszerűsített technikai megvalósítását vázolja az 1. ábra.



1. ábra A törvényes ellenőrzés általános technikai kivitelezése [2]

Az LI koncepciójából következik, hogy olyan rendszerek és egyedi eszközök ellenőrzése nem lehetséges ebben a formában, amelyeket nem szolgáltatásként vesznek igénybe (nem

[3] TDMA: Time Division Multiple Access – időosztásos többszörös hozzáférési (rádiócsatorna megosztási) technika
[4] LI: Lawful Interception – törvényes ellenőrzés (A távközlési rendszerek törvényes lehallgatása)
[5] ETSI: European Telecommunications Standards Institute – európai távközlési szabványosítási intézet

regisztráltak a hírközlés jogi engedélyezési rendszerében), nem kapcsolódnak semmilyen egyéb hálózathoz és más kommunikációs rendszerhez, hanem azokat maguknak nyújtják a felhasználók (bűnözők, terroristák) egy zárt csoport részére. Ez fokozottan érvényes az illegálisan alkalmazott és az engedélyhez nem kötött rádiókészülékekre, melyek más távközlési infrastruktúrákhoz egyáltalán nem csatlakoznak, így az LI tudatos elkerülésének eszközei. Az 1. ábrán jelölt internal interception interface (belső lehallgatási felület) szerepét ekkor egy külső lehallgatási felület, a rádiócsatorna veszi át, azaz kommunikációs felderítésről (COMINT[6]) beszélhetünk.

Természetesen kommunikációs felderítést szolgáltatásként nyújtott rendszerek esetében is lehet alkalmazni (pl. GSM, vagy trönkölt PMR rendszerek pl. TETRA esetében, annak ellenére, hogy ezekre egyértelmű LI szabványok kerültek kidolgozásra), azonban az általam vizsgált rádiószabványok esetében a szabványszintektől és kategóriáktól függően – az un. direkt kommunikációt alkalmazó PMR hálózatok esetén – ez az egyetlen és kizárólagos módja az ellenőrzésnek. Azonban az un. diszpécser típusú (átjátszóállomást alkalmazó) PMR rendszereknél elviekben mindkét módszer (LI, COMINT) alkalmazható, de ezekre nem létezik kidolgozott LI szabvány, így a COMINT egyelőre itt is fontos szerepet játszik. A trönkölt (civil) PMR rendszerekre szintén nincs konkrét LI szabvány, azonban ezekre vélhetőleg a TETRA-ra kidolgozott szabványok adoptálhatóak amellett, hogy a COMINT ezeknél szintén lehetséges. A digitális infokommunikációs technológiák aszimmetrikus alkalmazása nem csak műveleti, de technikai szempontból is jelentős kihívást jelent a COMINT tevékenységére.[2] Az új típusú digitális rádiók nem csak kommunikációra, de pl. RCIED[7] eszközök távvezérlésére is használhatók, így az EW[8] számára is kihívást jelenthetnek [2]. Összességében vizsgálatuk időszerű, szükségszerű és indokolt.

A COMINT által megszerezhető információk

A Comint tevékenysége sokkal kevésbé szabályozott technikai értelemben, mint az LI, azonban a szükséges és kinyerhető információk köre véleményem szerint gyakorlatilag ugyan az, mint az LI esetében. Azonban van egy jelentős különbség közöttük, mégpedig az, hogy az LI szabványok előírják a szolgáltatók részére az átadási felületen[9] (1. ábrán) a közlésinformációk szerviz vagy titkosító kódolástól mentes biztosítását, azaz a „nyers kommunikációtartalmat”, vagy annak kinyeréséhez szükséges kulcsokat [3]. A COMINT esetében azonban ezt a rendszernek kell megfejtenie, dekódolnia. A digitális átvitel alkalmazása különösen nagy kihívás elé állítja a kommunikációs felderítést, ezért fontos az újonnan megjelenő technológiák kutatása, megismerése, információ és műveleti tartalmuk maximális kinyerése érdekében. Így a digitális PMR rendszerekből elviekben a következők nyerhetőek ki, ha az átvitt bitfolyam titkosítás nélkül a rendelkezésünkre áll:

- A szolgáltatáshoz társított információk (service associated information), amelyekből az alkalmazott rádiószabványra és szolgáltatásaira lehet következtetni, a technikai paraméterek vizsgálata által, pl., konkrétan melyik digitális szabvány, milyen szintű rendszerben alkalmazva, milyen általános és egyedi szolgáltatásokkal társítva.
- A kommunikációhoz társított információk (communication associated information), amelyek metaadatok (kísérő adatok), a rádiókészülékek által használt egyedi azonosítók, a rádiókészülékek rendszeren belüli egyedi címei, a címzett(ek) és feladó relációjára, valamint a hívócsoportra vonatkozó adatok. A kommunikáció tartalmát és kódolását jelző adatok. Az időbeli adatok: a kommunikáció kezdetének és végének

[6] Communication Intelligence – rádiófelderítés (a SIGINT részterülete)
[7] Rádió-távirányítású improvizált robbanóeszközök - Radio Controlled Improvised Explosive Devices
[8] EW: Electronic Warfare – Elektronikai Hadviselés
[9] handover interface

időpontja. A készülékek státuszában, működésmódjában, a szolgáltatásban vagy annak paramétereiben beállt változások (pl. a hálózat hozzáféréséhez), valamint egyéb egyedi információk.

– A kommunikáció tartalma (content of communication) amely beszéd vagy adatátvitel tartalmú lehet, ezen belül is különféle beszéd és adatkódolású formákban.
– A rádiókészülékek helyzetinformációi (location information), amelyek a kisugárzás helyszínére vonatkoznak és amelyik lehet mért adat pl. több iránymérés eredményeként előálló, de lehet közölt adat is, amennyiben a rádiókészülék beépített GPS vevője (vagy egyéb helymeghatározó rendszere) a rádiócsatornán ez társított vagy egyedi információként közli.

A COMINT számára jó hír, hogy míg korábban az analóg rendszereknél a társított információk köre meglehetősen szűk volt (különféle szelektív hívók, amelyek gyakran csak egy hívócsoportot azonosítanak), addig a digitális PMR-ek esetében ezek új értelmezést nyerhetnek, a készülékek, hívócsoportok, a kommunikációtartalom és a szolgáltatások egzaktabb azonosítása által. Így ezek kinyerése több műveleti értéket hordozhat magában.

A DIGITÁLIS PMR SZABVÁNYOK

A digitális PMR szabványkategóriának két nagy csoportja létezik, melyeket alapvetően a csatorna hozzáférési technika alapján lehet elkülöníteni, és amely egyben a csatorna sávszélességet is meghatározza. Így a gyakorlatban TDMA alapú szélessávú (12,5-25 kHz), valamint FDMA alapú keskenysávú (6,25-12,5 kHz) technológia csoportokat különböztetnek meg a szabványokban és a szakirodalmakban egyaránt (1. táblázat).

FDMA alapú	TDMA alapú
dPMR[10], TS 102-490, TS 102-658 (EU)	DMR[11] (EU) /2 időréses/
NXDN (USA)	
DCR[12], ARIB[13] standard T-98 (Japán)	
ARIB standard T-102 (Japán)	
P25[14] (1 fázis TIA-102) (USA)	P25 (2. fázis) (USA) /2 időréses/
Tetrapol[15] (Francia)	TETRA[16] (EU) /4 időréses/
D-Star[17] (Japán amatőr)	PDT[18] (Kínai) /2 időréses/

1. táblázat. A jelenlegi elterjedtebb digitális PMR rádiószabványok (saját kutatás alapján)

[10] dPMR: Digital Professional Mobile Radio – Amely a hagyományos 12,5 kHz-es analóg csatornát két 6,25 kHz-sávszélességű digitális rádiócsatornával váltja ki.
[11] DMR: Digital Mobile Radio – Amely a hagyományos 12,5 kHz-es analóg csatornát, 12,5 kHz-sávszélességű két időréses TDMA (időosztásos) digitális rádiócsatornával váltja ki.
[12] DCR: Digital Convenience Radio – az európai dPMR alapján készült Japán digitális rádiószabvány
[13] ARIB: Association of Radio Industries and Business – Japán Üzleti és Ipari Rádió Társaság, a DCR kidolgozója
[14] P25: Project 25 – az APCO (Association of Public Safety Communications Officials International) kezdeményezésére a TIA (Telecommunications Industry Association) által kidolgozott nyílt rádiószabvány, melyet a TETRA-hoz hasonló célokkal hoztak létre amerikában, de Kanadában és Ausztráliában is használt.
[15] Tetrapol: A tetrától eltérő francia trönkölt szabvány
[16] TETRA: Terrestrial Trunked Radio – európai trönkölt rádiószabvány
[17] D-Star – Digital Smart Technologies for Amateur Radio, a Japán rádióamatőr szövetség (JARL) szabványa
[18] PDT: Professional Digital Trunking – 2 időréses DMR-hez hasonló trönkölt rendszer

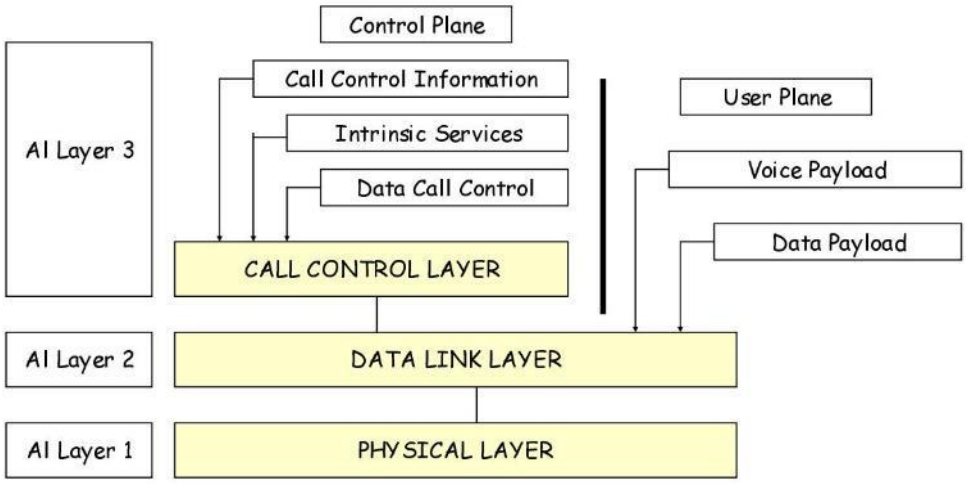
Az FDMA alapú digitális PMR szabványok

Ebben a cikkben a táblázat baloldali oszlopával az FDMA típusú szabványokkal kívánok foglalkozni. Összességében elmondható, hogy az FDMA technológiájú dPMR-hez hasonló szabványok hardver platformjai közelebb állnak a hagyományos FM rádiók adás-vétel technológiájához, így a TDMA-hoz képest kisebb komplexitású és olcsóbb rádiótechnológiát képviselnek [4]. Ez abból a szempontból is érdekes, hogy az eszközök legális és illegális elterjedését is jobban elősegíti az „olcsóságuk". A kiindulási európai digitális szabványosítási tervek csak a 2 időréses TDMA technológián alapultak volna, mivel a 6,25 kHz-es FDMA-t nem tartották megfelelően kivitelezhetőnek. Ennek ellenére az Icom és Kenwood cégek bebizonyították, hogy a 6,25 kHz FDMA egy praktikus választás, és közös megállapodás keretében fejlesztették ki a technológiát. Ezt az új digitális 6,25 kHz FDMA ötletet vette fel az ETSI, és fejlődött ki belőle az európai dPMR szabvány, amely nyílt, nem védett EU-szabvány. TS 102 490 [5] számon tették közzé az engedélymentes, és TS 102 658 [6] számon az engedély köteles FDMA protokoll specifikációját. Jelenleg a keskenysávú szabványkategóriának több más országbeli pl. japán: ARIB standard T-98 [7], T-102, valamint amerikai: NXDN TS-1 [8], TS-2 implementációja is létezik, amelyek nagyrészt az európai dPMR szabványtól „csak" a moduláció paramétereiben, valamint a keretszervezés és a logikai csatornák felépítésében térnek el [5][8][9], de emiatt nem teljesen kompatibilisek.

Ezektől jelentősebb eltérést mutat a trönkölt P25, és Tetrapol. A japán D-Star pedig egy rádióamatőr szabvány. Ezek mindegyike egymástól különböző egyedi megoldást takar a dPMR-től eltérő modulációval és keretszervezéssel. Ezek globális jelentősége jóval csekélyebb mint a dPMR-é, így ez utóbbi szabványcsalád változatait tekintem át részletesebben. A vizsgálat során csak a jelek vételéhez szükséges mozzanatokat vizsgálom, mivel a felderítés szempontjából csak erre van szükség a COMINT feladatok végrehajtásához.

A dPMR szabványok általános protokoll felépítése

A dPMR szabványcsalád protokoll felépítése az egyes szabványokban hasonló, ahol 3 szintű rétegben, rétegenként eltérő funkciókat valósítanak meg, az alábbi, 2. ábrának megfelelően. A protokoll felépítés eltér az OSI 7 rétegű modelltől, amennyiben itt csak 3 réteget használnak.



2. ábra A dPMR protokoll felépítése [6]

A rádiócsatornán (Air Interface) a fizikai rétegen (Physical Layer), az adatkapcsolati rétegen (Data Link Layer) és a hívásvezérlő rétegen (Call Control Layer) keresztül megvalósított rádiófunkciók a következők:

A *fizikai rétegen keresztül* valósul meg: az RF jel vétele, a 4FSK demoduláció, a bit-, és szimbólum helyreállítás, a frekvencia és szimbólum szinkronizáció.

Az *adatkapcsolati rétegben* kerülnek végrehajtásra a következők: a csatorna dekódolása hibajavítása: de-scrambling, bitsorrend-visszarendezés[19] (az adásnál történt bitszétkenés inverz folyamataként) de-FEC[20], és de-CRC[21]); a szuperkeretek és keretek szinkronizálása visszaállítása, burst és paraméter visszaállítás; a kapcsolat (forrás és cél) címének megállapítása (a hívásvezérlő rétegen keresztül); felületet biztosít a beszédalkalmazások (beszéd adatok) számára a fizikai réteg irányába; adathordozó szolgáltatásokat biztosít, a jelzésrendszer és/vagy felhasználói adatok cseréjére a hívásvezérlő réteggel és végül a dPMR esetében automatikus sajátazonosító, (Own-ID) és csoportazonosító (Group-ID) érzékelést, míg az NXDN esetében automatikus RAN (Radio Access Number) érzékelést biztosít.

A *hívásvezérlő rétegben* (Call Control Layer) történik a jelzésátvitel a végpontok között: az egyéni vagy csoporthívások, kezelése, a cél címzése, a hívásvezérlés (hívások létrehozása, fenntartása, lezárása), valamint a belső szolgáltatások támogatása: pl. késői hívásbelépés[22], hívásátirányítás stb. kezelése.

A dPMR alapú digitális PMR szabványok alapsávi jelfeldolgozása

A fenti protokollnak megfelelően létre lehet hozni egy valódi jelfeldolgozó struktúrát. A keskenysávú dPMR adásmódok vételi mechanizmusa teljesen hasonló, azonban a 4FSK demodulátor frekvenciaeltolás paramétereik különböznek egymástól, valamint a keretszervezésben és a logikai csatornák típusában és felépítésében is vannak eltérések. A következő 2. táblázat a 4FSK moduláció paraméterek eltéréseit foglalja össze. [4],[5],[8],[9]

		4 FSK frekvencia eltérés [Hz]-ben				
Dibit	Szimbólum	dPMR	NXDN		ARIB T-98	ARIB T-102
		4800 bps	4800 bps	9600bps	4800bps	4800 bps
01	+3	+ 1050	+ 1050	+ 2400	+945	+990
00	+1	+ 350	+ 350	+800	+315	+330
10	-1	- 350	- 350	-800	-315	-330
11	-3	- 1050	- 1050	-2400	-945	-990

2. táblázat. A dPMR szabványok 4 FSK frekvencia-eltérések összehasonlítása

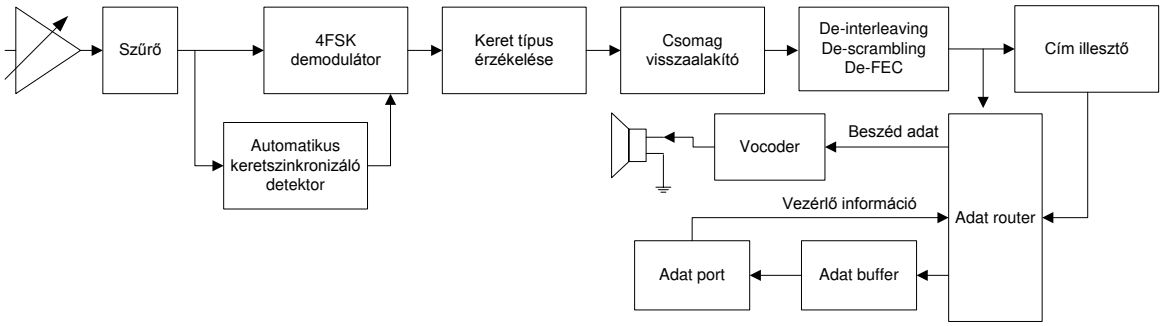
Ennek ellenére a vétel folyamata – mely a felderítés szempontjából leginkább érdekel bennünket – egymástól jól elkülöníthető részfeladatok sorozatára bontható fel. A dPMR típusú szabványok digitális vételéhez a 3. ábrán látható univerzális felépítésű rádióvevő alkalmazható [10], amelyik csak az alapsávi jelfeldolgozás folyamatát mutatja be, az RF vevőrészek ismertetése nélkül.

[19] de-interleaving – a bitszétkenés inverz folyamata, ahol helyreállítjuk a bitek eredeti sorrendjét (ennek az a célja, hogy az átvitel során fellépő csoportos hibák, a visszarendezés után ne egymás mellé essenek, így a csoportos hibákat különálló bithibákká alakítjuk, aminek a korrigálása sokkal egyszerűbb és hatékonyabb)

[20] Forward Error Correction – hibakorlátozó kódolás inverz művelete a hiba ellenőrzési és javítási eljárása

[21] Cyclic Redundancy Check – hibadetektáló kódolás inverz folyamata, a CRC ellenőrzése

[22] Late entry call: /a dPMR szolgáltatása/ amikor egy már kisugárzott adást nem az elejétől veszünk, hanem közben lépünk be a kommunikáció vételébe.



3. ábra A dPMR vevő általános logikai felépítése [10]

Ha különféle szabványok vételére akarjuk alkalmazni ezt az elrendezést, akkor a 4FSK demodulátor utáni részek (az egyes különálló blokkok) feldolgozási paramétereit kell megváltoztatni az egyes eltérő szabványoknak megfelelően. Erre kézenfekvő megoldást a szoftverrádió (SDR) technológia jelenti, azonban az alkalmazott hardvertől függően ennek kivitelezése a gyakorlatban többféle módon történhet: hagyományos mikroprocesszorral, DSP[23], FPGA[24], FirmAsic[25] technológia alkalmazásával, amit jelen cikk keretei között nem vizsgálok.

A vételi folyamat eredményeként az RF vevő analóg limiter/diszkriminátor kimenetéről az információt hordozó analóg jel egy állítható szintű erősítőn keresztül egy szűrőre kerül. A szűrő emelt-koszinuszos karakterisztikájú, amelyiket gyakran használják a digitális modulációk jelfeldolgozásában, mivel minimalizálni lehet vele a szimbólumok közötti áthallást (ISI - Intersimbol Interference).

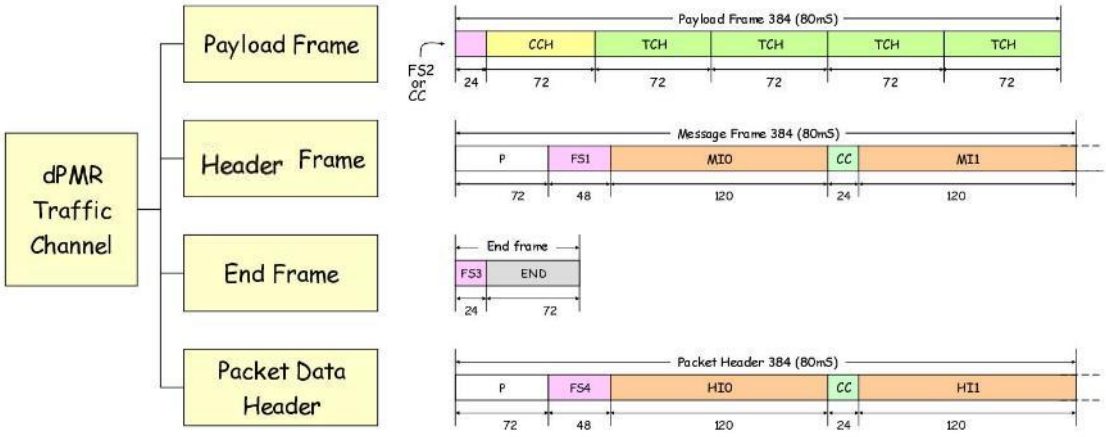
Keretszinkronizálás érzékelése és a demodulálás

A jel a szűrőről az automatikus keretszinkronizáló detektor (AFSD - Automated Frame Sync Detector) blokk bemenetére kerül, amelyik kinyeri, elvégzi a szimbólum és keret-szinkronizációt. Amint az AFSD elvégezte a keret-szinkronizációt, kinyerte az időzítési adatokat, átadja a demodulátornak az időzítési és szimbólum szint információkat, amelyik ez alapján elkezdi kinyerni az ezt követő adat biteket, azaz demodulálja a jelet. A forgalmazás végét előre lehet jelezni a vett frekvencia kontrollcsatornájának folyamatos figyelésével, mely az egyes szabványok esetében más és más lehet (lásd később). Valamint detektálni lehet a kapcsolat bontása speciális keret együttesének vételével (ha nem az előző módszerrel valósul meg). Így a kommunikáció végén újra lehet indítani a keret-szinkronizáció keresését.

A dPMR keretszervezése, logikai csatornái, címzési módjai

Ahhoz, hogy a további áramkörök működését érteni lehessen szükséges megvizsgálni a rendszerben alkalmazott keretszervezési elveket. A dPMR szabványban annak ellenére, hogy FDMA szabványról van szó, a digitális átvitel miatt az információközlés a rádiócsatornán egy előre definiált bitstruktúra és időzítés szerint történik. Ennek megfelelően a GSM és egyéb digitális rendszerekhez hasonlóan az átvitel un. keretekbe (frame) és szuperkeretekbe (superframe) szervezve bonyolódik. A dPMR rendszerben alapvetően négyféle keretformátum alkalmazott az átvitel során. Ezek un. logikai csatornákból épülnek fel (különböző színek szimbolizálják), ezáltal különíthető el az egyes keretek felépítése és tartalma, ami a következő 4. ábrán látható:

[23] DSP: Digital Signal Prosessor
[24] FPGA: Field Programmable Gate Array
[25] FirmAsic: un. Function Image-ek betöltésével konfigurálható a vevő képessége és működésmódja

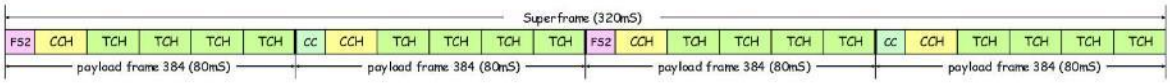


4. ábra A dPMR keretek felépítése [6]

Az egyes keretek a következők: 1. üzenet keret (Payload Frame), 2. bevezető keret (Header Frame), 3. Vége keret (End Frame), 4. Adat csomag fejléc (Packet Data Header). Minden keret hossza 80 ms, ami 384 bit átvitelét teszi lehetővé, ettől egyedül a 3. sz. vége keret tér el, amely mindössze csak 96 bit és a kommunikáció végének jelzésére szolgál.

Az átvinni kívánt közlésinformációt az 1. sz. üzenet keretek sorozataival visszük át, amelyben a 4 db 72 bites blokk (TCH - Traffic Channel) hordozza a hasznos közlemény információt. Ezt a szintén 72 bites vezérlő csatorna (CCH-Control Channel) valamint a 24 bites keret-szinkronizációt biztosító FS2 (Frame Syncronisation) rész vagy az un. csatorna kód (CC-Channel Code, /korábban szín kódnak-Colour Code nevezték /) vezeti be.

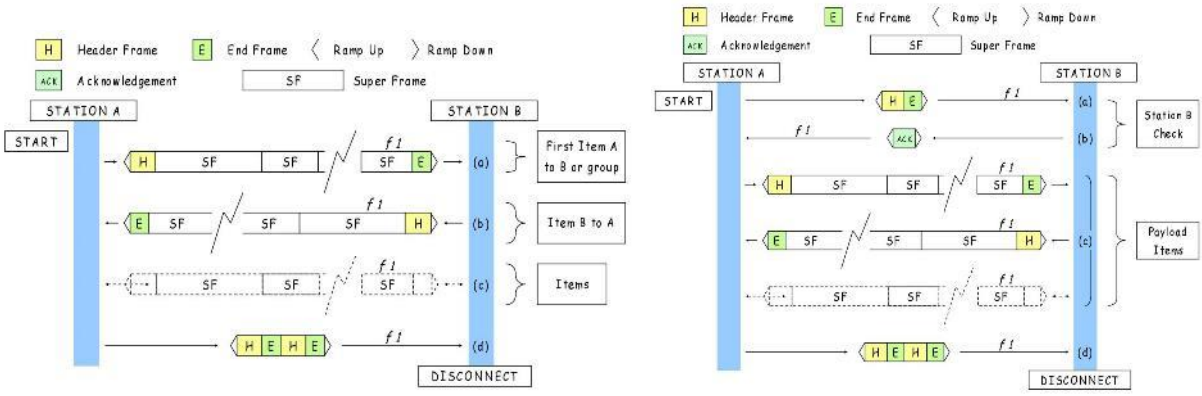
A közlemény (audio vagy adat) hosszától függően üzenet keretek sorozatából szuper kereteket (SF- Superframe) hoznak létre, amelynek a felépítése a következő: A 4 db üzenet keretet tartalmazó összesen 320 ms hosszúságú 1536 bites jelsorozatban, minden páros keret csatorna kóddal (CC), illetve minden páratlan keret FS2 típusú keretszinkronizáló kóddal kezdődik. A dPMR esetében ez a legnagyobb hosszúságú szabályozott bitstruktúra, amelyből a közlésinformáció hosszának megfelelő számú db-ot visznek át egymás után a rádiócsatornán.



5. ábra A dPMR szuperkeretek felépítése [6]

A kommunikáció felépítése, azaz a keretek és szuperkeretek egymásutánisága, sorrendje az un. keretszervezés, egyrészt a dPMR szabvány szintjétől (mode 1. 2. vagy 3.) másrészt a kommunikáció tartalmától (beszéd, adat) is függ. A 6. ábrán tipikus keretszervezések láthatóak a mode1. szabványú közvetlen (peer-to-peer) beszédátvitel során. A TS 102 490 kétféle működési módot definiál a dPMR rádiók részére. A bal oldali ábra az un. ISF[26] gyárilag felprogramozott módú (out of the box) kommunikáció felépítését mutatja, míg a jobboldali ábra az un. CSF[27] menedzselt módú kommunikáció menetét ábrázolja. Az utóbbi felépítése a kapcsolatfelvétel módjában tér el a gyári állapotútól. A 6. ábra jobb oldalán látható, hogy a kommunikáció kérést, ami egy bevezető és vége keret együttese (Header+End frame), egy nyugtázó (ACK) üzenettel jelzi vissza a megszólított készülék, ami egy speciális tartalmú bevezető keret (Header Frame). Így gyakorlatilag egy kézfogás (handshake) jön létre a készülékek között.

[26] ISF: Initial Services and Facilities - Kezdeti szolgáltatások és eszközök (a gyárilag beállított állapot)
[27] CSF: Configured Services and Facilities - Konfigurált szolgáltatások és eszközök (a gyári állapottól eltérő utólag felprogramozott állapot)



6. ábra A dPMR közvetlen kommunikáció felépítése [6]

Az ISF és CSF működési módnak megfelelő kétféle címzési eljárást is definiál a TS 102 490 szabvány. Az egyik a 24 bites bináris, a másik a 7-digites BCD[28] módú címzési eljárás. Az ISF módban kizárólag a bináris címzés használatos, de CSF módban mindkét eljárás megengedett. Az alkalmazott címzési eljárás megállapítása felhasználható bizonyos műveleti adatok megállapítására. Például a BCD módú címzés egyértelműen bizonyítja, hogy a készüléket átprogramozták. Az un. csatorna kód (CC), melyet kódolatlanul visznek át a rádiócsatornán – egyértelműen az alkalmazott frekvenciához rendelt bináris kód – szintén összefüggésben van a címzési eljárással. Ugyan annak a frekvenciának (16 db engedélyhez nem kötött frekvencia) más a CC kódja ISF („A" módú címzés) és CSF („B" módú címzés) üzemmódú készüléknél. Ez szintén lehetővé teszi a beállított működési mód, továbbá az alkalmazott frekvencia beazonosítását is. 31 db további bináris CC kódot tart fenn a szabvány, 31 további felhasználó által programozható frekvencia azonosítására (CSF módú készüléknél). [5]

A dPMR kerettípus érzékelése, címillesztés és a vétel folyamata

Egy dPMR hívás mindig egy un. bevezető kerettel (header frame) kezdődik, amelyik azonos felépítésű 2. vagy 4. sz. keret lehet, amelyek abban különböznek, hogy FS1 vagy FS4 típusú keretszinkronizáló kódot tartalmaznak. A bevezető keret mindig egy 72 bites bevezető bitsorozattal (Preamble) kezdődik, amelyet a 48 bites keretszinkronizáló csomag (FS) követ. A preamble bitek funkciója, az, hogy segítsék megtalálni a 3. ábrán látható „automatikus keretszinkronizáló detektor" (AFSD) blokknak, az FS1 vagy FS4 bitek elejét. A közleményeket ezután szuperkeretekbe szervezett üzenet keretekben viszik át, amelyekben minden 2 keret FS2 típusú keretszinkront tartalmaz. Az AFSD blokk, folyamatosan érzékeli az FS kódok típusát, így egyértelműen eldönthető, hogy mi „zajlik" éppen a rádiócsatornán, illetve hogy a keretszervezés hol tart az időzítés folyamatában Az üzenet keretek szuperkereten belüli számát, azaz a keretsorszámot a CCH tartalmazza (lásd a 3. táblázat FN mezőjét). Az FS1 vagy FS4 detektálása éppen egy beszéd vagy adat közlemény elejét, az FS2 pedig egy már folyamatban lévő kommunikáció közepét (late entry call) jelzi. Amint a keretszinkronizálást elértük, a 4FSK demodulátor bekapcsol, és az utána lévő blokkok veszik át a szerepet, az AFSD kikapcsolásra kerül. A demodulátor utáni blokkok elkezdik helyreállítani az eredeti üzenet bitstruktúráját. A feladat ez után az, hogy eldöntsük, nekünk szól-e az üzenet vagy sem. Azaz a címzés ellenőrzése, amit a 3. ábra szerinti címillesztő blokk végez el.

Ennek érdekében FS1/FS4 vétele esetén értelmezésre kerül, a bevezető keret MI0 és MI1 (illetve adatfejléc esetén: HI0 és HI1) információtartalma, melyet a 3. táblázat bal oldala szemléltet. Először ennek „F" (kommunikációforma) mezője kerül értelmezésre, amely megmondja, hogy egyéni vagy csoporthívásról van szó. Csoporthívás (All Call) esetén, a vett

[28] BCD: Binary Coded Decimal - binárisan kódolt decimális számformátum. Ennek az alfanumerikus kijelzővel rendelkező rádiók készülékről történő kézi címbevitelkor van jelentősége

jel feldolgozásra kerül. Direkt (peer-to-peer) hívás esetén a hívott ID mező (Called ID - a hívott állomás azonosítója) összevetésre kerül a készülékünk saját ID azonosítójával (Own ID - ami nem egyezik meg az ID2 mező értékével, mert az a hívó fél saját azonosítóját jelenti). Ezek egyezése esetén az üzenet nekünk szól, és feldolgozásra kerül, ha nincs egyezés eldobjuk az üzenetet.

Az ID-k kialakítása a következő elvet követi. ISF módban egyszerűsített címzést alkalmaznak (azaz nincs külön egyedi és csoportcímzés, csak közös azonosító): a 24 bites címrészt 2 részre bontjuk, az első 16 bit fix 1-eseket tartalmaz, az utána következő 8 bit, az un. Common ID (közös azonosító), amely az analóg rendszerek CTCSS[29]/DCS[30] szelektív hívókódjának felel meg. Itt a beállítható értékek 1-254-ig az egyedi rendszerkódot jelentik, a 255-ös érték az un. All Call (mindenki hívása), azaz a 255-ös ID-jű üzenet a beállított saját ID-től függetlenül mindig dekódolásra kerül.

CSF módban a rádiók egyedi címmel rendelkeznek, melyek nem azonosítanak csoport kódot, hiszen ilyenkor egy ismert csoport részeként vesznek részt a kommunikációban. A csoporthívást a rendszerben lévő rádiók részhalmazát jelentő egyedi címek definiálásával oldják meg ekkor.

FS2 vétele esetén (késői belépéskor) az üzenet keretek CCH vezérlő csatornájában szintén megtalálható az „F” mező értéke, valamint a hívott készülék ID kódja (3. táblázat jobb oldala). Ezek ismeretében eldönthető, hogy nekünk szól-e az üzenet vagy sem. Ha nem akkor az AFSD folyamata újra indul, ha igen akkor megkezdődik a helyreállított bitsorozat további feldolgozása. A további feldolgozás menetének eldöntésében is 3. táblázat mezőire támaszkodhatunk.

A következő táblázatok az MI0-MI1, HI0-HI1, valamint a CCH logikai csatorna mezőinek értelmezését, és hasznos bitjeinek számát mutatják.[5]

MI0 MI1 HI0 HI1 72 bit + kódolás	HT	fejléc típus	4
	ID0+1	hívott ID	24
	ID2+3	saját ID	24
	M	kommunikációs mód	3
	V	verzió	2
	F	kommunikációforma	2
	RES	fenntartott	2
	CI	hívás információ	11

CCH 41 bit + kódolás	FN	keret száma (1,2,3,4)	2
	FN1: ID0 FN2: ID1 FN3: ID2 FN4: ID3	hívott ID (felső 12 bit) hívott ID (alsó 12 bit) Saját ID (felső 12 bit) Saját ID (alsó 12 bit)	12
	M	kommunikációs mód	3
	V	verzió	2
	F	kommunikációforma	2
	RES	fenntartott	2
	SLD	lassú adat	18

3. táblázat A dPMR bevezető keretek MI-HI mezői és CCH csatorna bitjeinek értelmezése

Az „M” (kommunikációs mód) mezőből kiderül, hogy milyen típusú információt viszünk át az üzenet keretek TCH blokkjaiban a rádiócsatornán: csak beszéd, beszéd+lassú adat[31], csak adat FEC-nélkül /T1/, csak adat FEC-el /T2/, csomagkapcsolt adat ARQ eljárással /T3/[32], beszéd és csatolt adat. Hanghívás esetén az adatokat átadjuk a beszédszintetizátornak (Vocoder). A „V” (version - változat) mezőből megtudhatjuk, hogy az üzenet Ambe+2 (TS 102 490 szerinti), RALCWI (olcsó, licensz nélküli), vagy Chinese DRA (nyelvspecifikus) beszédkódolással, esetleg valamilyen gyártó specifikus kódolással készült. [6],[10] Az egyes beszédkódolók árban jelentősen eltérhetnek, valamint nyelvi specifikumaik is vannak. A „V” mező értékéből szintén lehet műveleti adatokat megállapítani, pl. távol-keletről behozott készülékre következtetni, még abban az esetben is, ha nem rendelkezünk a szükséges beszédkódolóval.

Különálló adathívás (T1, T2, T3), illetve valamilyen társított adat átvitele esetén a visszaállított adatfolyam 3. ábra szerinti adatportra (adatbuszra) kerül kiírása, az adatbufferen

[29] CTCSS: Continuous Tone Coded Squelch System – folyamatos alacsony frekvenciával kódolt zajzár
[30] DCS: Digital Coded Squelch – digitálisan kódolt zajzár
[31] a CCH vezérlőcsatorna SLD –Slow Data mezőjében visszük át
[32] csak CSF működési módban lehetséges

keresztül. A CCH vezérlőcsatorna SLD (Slow Data) mezőjében lassú adatként átvihetünk státusz üzeneteket, előre megírt üzeneteket, szabad szöveges üzeneteket, rádió által generált adatokat, rövid fájlokat, felhasználó által előre definiált adatokat, melyek több keretben is átvihetőek.

Csak a bevezető keretekben meglévő CI (Call Information) mező további változó tartalmú kiegészítő adatokat tartalmaz a bevezető keret típusáról, a nyugtázó keret minőségéről (ACK /elfogadás/, NACK /adat hiba, kérés újraküldés vagy kérés megtagadás tényéről), valamint az SLD mező tartalmáról. Így megtudható hogy T1/T2/T3 adatot viszünk át, illetve T3-nál a keretméretet (80-160-240-320 ms illetve 288-672-1056-1440 bit /kódolás nélküli/) és a keretszám (max. 8 keretben) is.

A HT (fejléc típusa - Header Type) mezőből megtudhatjuk, hogy a fejlécet mire használjuk, azaz, hogy milyen információ következik utána.

A hasznos információtartalom átvitelét követően, a feldolgozás folyamata a kommunikáció befejezése (disconnection request) speciális keretcsomag 4 db egymást követő bevezető és vége keret (lásd 6. ábrán) érzékelésével leáll, és az AFSD folyamata újraindul.

Az NXDN egyedi megoldásai

Az amerikai NXDN protokollt 2005-ben mutatta be az Icom és a Kenwood (jelenleg JVC-Kenwood) cég és 2006-ban jelentek meg az első eszközök. 2012-ben a szabványt nyilvánossá tették. Hasonlóan a dPMR-hez 384 bites (80 ms) kereteket alkalmaznak, melyből 3 féle definiált a szabványban. 1. hangkommunikációs keret, 2. adatkommunikációs keret, és 3. adatkommunikációs burst keret. A dPMR-től eltérő nevű logikai csatornákat használnak, de funkciójukat tekintve hasonlóak. A hangkommunikáció átvitelére a következő keretformátumokat alkalmazzák.

bits:	>24	20	16	60	144		144	
	P	SW	LI	SACCH	FACCH1		FACCH1	
		SW	LI	SACCH	TCH1	TCH2	TCH3	TCH4
		SW	LI	SACCH	TCH1	TCH2	TCH3	TCH4
		SW	LI	SACCH	TCH1	TCH2	TCH3	TCH4
		SW	LI	SACCH	TCH1	TCH2	TCH3	TCH4
	Repeat until PTT released....							
		SW	LI	SACCH	FACCH1		FACCH1	

7. ábra Az NXDN beszédátvitel keretek felépítése [12]

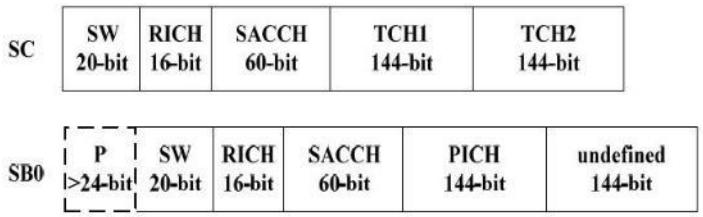
Az első (start) üzenetkeretben (ami a dPMR bevezető keretének felel meg) az SW-t egy P (Preamble) bevezető rész előzi meg, amelyik jobb keret-szinkronizációt biztosít. Ezután egy 20 bites SW (Synchronization Word) keretszinkronizáló blokk következik, amit egy 16 bites összeköttetés információs csatorna (LICH - Link Information Channel) követ. Az LICH definiálja a keretformátumot és az üzenet típusát (ami TCH és FACCH lehet). Ezután egy 60 bites SACCH (Slow Associated Control Channel - lassú társított vezérlőcsatorna) következik, ami a dPMR CCH vezérlő csatornájához hasonló funkciójú és az üzenet keretekben is megtalálható. Az első (start) keretben ezután két darab 144 bites FACCH1 (Fast Associated Control Channel - gyors társított vezérlőcsatorna) következik, ami a dPMR MI-HI információs csatornáihoz hasonló funkciókat tölt be (lásd 3. táblázat).

A bevezető keret után egy 4 keretből álló szuperkeret következik. Ennek kereteiben visszük át a beszédinformációkat ahol az FACCH1 helyén 4x72 bites TCH (Traffic/Payload Data – üzenet blokkokat) viszünk át. Ha több szuperkeret szükséges az átvitelhez azok az átvitel végéig ismétlődnek, majd a bevezető keret formátumának megfelelő, de más kommunikációtartalmú (vége keret) jelzi a kapcsolat végét, ahogyan ez a 7. ábrán látható. A címzéshez használt 6 bites RAN (Radio Access Number – rádió hozzáférési szám) értéke az SACCH/FACCH1 csatornák

„SU” mezőjében definiált, amelyet a saját–RAN (Own–RAN) –al összehasonlítva eldönthetjük, hogy nekünk szól-e az üzenet. Az egyéni és csoporthívás (All Call) egyaránt értelmezett, mely utóbbinál a RAN értéke zéró. A fentieknek megfelelően az NXDN jelek vételéből hasonló információtartalom nyerhető ki, mint a dPMR esetében. A vétel folyamata a 3. ábrának megfelelő sorrendű elrendezéssel realizálható.

A DCR egyedi megoldásai

A japán ARIB standard T-98 szabványleírás 2008-as az eredeti szabvány, 2012. decemberi a legújabb verziója, amit a dPMR szabvány alapján fejlesztettek ki. A DCR rendszerben, eltérően a dPMR-től csak 2 féle kerettípus létezik. Az egyik az SB0 (Synchronous Burst 0) típusú, ami a kommunikáció kezdetét jelzi, a másik az SC (Service Channel) típusú, ami magát a hasznos információt viszi át. A keretfelépítés a következő 8. ábrán látható.



8. ábra A DCR T-98 keretek felépítése [9]

A keretek 80 ms hosszúak, és 4 db keret alkot egy szuperkeretet, hasonlóan a dPMR-hez. A logikai csatornák nevei eltérőek. Az RICH (Radio Information Channel – rádió információs csatorna) felel a logikai csatornák és a kommunikációs háttér azonosításáért. A hasznos tartalma 7 bit. A 36 bites hasznos tartalmú SACCH (Slow Associated Control Channel - lassú társított vezérlőcsatorna) a dPMR CCH vezérlő csatornájához hasonló funkciójú logikai csatorna. Az SB0 tartalmaz ezeken felül egy 144 bites PICH (Parameter Information Channel - paraméter információs csatorna) nevű blokkot, ami a dPMR MI-HI információs csatornáihoz hasonló funkciókat tölt be (lásd 3. táblázat), valamint egy 144 bites padding részt (itt nem ismétlik meg kétszer a PICH tartalmát úgy, mint az MI0-MI1 esetében a dPMR-nél). A PICH tartalmaz egy 36 bites CSM (Call Sign - hívójel) mezőt. Ez a rádiók egyedi 9 digites sorozatszámát tartalmazza BCD kódolásban, amit minden SB0 keretben kisugároznak, azonban a címazonosításhoz nem használnak fel [11]. Az SC keret RICH csatorna kommunikációs mód (Communication Mode) mezője definiálja a 2x144 bites TCH (Traffic Channel - forgalmi csatorna) blokkok tartalmát, amelyben beszédinformációt, kódolatlan adatot, vagy FEC kódolt adatot visznek át a rádiócsatornán. Nem lehetséges azonban a dPMR-hez hasonló beszéd és adat vegyes átvitele jelenleg.

Minden DCR hívás, egy SB0 kerettel kezdődik, és négy darab SC kerettel folytatódik, melyek egy szuperkeretet alkotnak. Az SB0 elején lévő (P-Preamble) rész az utána következő 20 bites szinkronizáló szóval (SW - Synchronization Word) együtt alkotja a dPMR-nél FS1-nek nevezett keretszinkron logikai csatornát. A kommunikáció kezdetét az AFSD a P utolsó 18 bitje + az SW 20 bitje együtteseként próbálja megtalálni a beérkező bithalmazban. Természetesen itt is van lehetőség a kommunikáció közbeni szinkronizálásra, (late entry - késői belépés) esetén. Ekkor egyből egy SC kerettel kezdődik a vett jel, azaz csak a 20 bites SW-ből lehet megállapítani a keretszinkront, amit ekkor FS2 ként definiálhatunk. Ekkor legalább 2 sikeres FS2 detektálás engedélyezi a demodulátor aktiválását, a keretszinkron elérése után, hasonlóan a dPMR-hez.

A keretszinkron elérése után el kell dönteni, hogy nekünk szól-e az üzenet. A DCR rendszer is támogatja mind az egyéni, mind a csoport címzés alkalmazását, melynek dekódolását az SACCH csatorna 9 bites felhasználói kód (User Code) valamint információ típus (Information Type) mezőivel oldanak meg, hasonlóan a dPMR „called ID” és „F” mezőjéhez. Itt vagy a User

Code és Own ID egyezés vagy All Call detektálása esetén történik meg a további feldolgozás engedélyezése, a TCH-k tartalmának megfelelően.

Az információtartalom átvitele után a kommunikáció végét az SACCH csatorna Information Type nevű mezőjében jelzik, egy hívás vége (Call End) kódtartalmú üzenettel. Ezután a keretszinkronizáció folyamata újraindul.

A fentieknek megfelelően a DCR jelek vételéből hasonló információtartalom nyerhető ki, mint a dPMR esetében. A vétel folyamata a 3. ábrának megfelelő sorrendű elrendezéssel realizálható.

ARIB standard T-102 szabványleírás megoldásaiban nagymértékben hasonlít a T-98-hoz, azonban itt 3 kerettípus létezik (hang, adat, burst adat) a keretszervezése pedig nagymértékben az NXDN-hez, mivel ugyan azok a cégek dolgozták ki. A logikai csatornák nevei ugyan azok, és hasonló a vevőrealizáció is. A kinyerhető információkra a fentebb leírtak igazak.

A KOMMUNIKÁCIÓS ELLENŐRZÉSSEL KINYERHETŐ INFORMÁCIÓK

A rádiók egyedi modulációs paramétereiből kézi, vagy automatikus jelelemzés segítségével megállapíthatók a 2. táblázatban összefoglalt 4FSK frekvencia-eltérések [13], melyből más egyéb paraméterek azonosítása után következtetni lehet az adás szabványára. A rádiók egyedi címzési módjával kapcsolatban többféle következtetés is levonható. Egyrészt a csatorna kódból CC, valamint az ISF és CSF módú címzésből következtetni lehet a rendszer működési módjára, közvetve arra, hogy felprogramozták- e a készüléket, vagy gyári állapotban van. Az egyedi rádiócímek csoport és rendszerazonosító kódok megállapításából pedig egyértelműen azonosítani lehet a kommunikációban résztvevő feleket.

A cikkben leírt CC és ID illetve (a többi szabványnál az ennek megfelelő adatok pl. DCR-nél: User Code) azonosítása, azaz a címegyezés vizsgálata egy normál rendszerben alkalmazott eljárás. Egy erre a célra alkalmazott COMINT vevőben nem csak a nekünk szóló, hanem a CC-től és ID-től (kódoktól és azonosítóktól) függetlenül bármely üzeneteket szeretnénk venni, (rögzíteni), amellett hogy a CC az Own ID valamint a Called ID (az ezeknek megfelelő más szabványú adatok) felhasználhatók a vett/rögzített üzenetek azonosítására, egymáshoz rendelésére, időbélyeggel történő ellátás esetén pedig az időrendiség megállapítására is.

Ez jóval több műveleti információt hordoz magában, mint az analóg rádiók vételéből származó adatok. A 3. táblázat tartalmát kiértékelve további információkhoz juthatunk a kommunikáció formája, módja, tartalma valamint az alkalmazott beszédkódolás tekintetében, még akkor is, ha nem tudjuk visszaállítani az eredeti hangüzenetet vagy adattartalmat. Az átvitt információtartalom kódolását jelen cikk keretei közt nem vizsgáltam, csak azt tekintettem át, hogy elméletben milyen adatok ismeretét teszi lehetővé a rendszerek vizsgálata, jeleinek vétele. A kódolt adatokból az információ visszanyerése adatfeldolgozó eljárásokkal dekódolással lehetséges, amely további vizsgálatokat igényel. Mivel azonban nyílt szabványokról van szó, ezért az összes kódolási folyamat ismert és publikus folyamattal és paraméterekkel rendelkezik, ami elviekben nem jelenthet akadályt, kivéve, ha kiegészítő titkosítást is alkalmaznak az átvitelben.

ÖSSZEGZÉS

Bemutattam, hogy a törvényes ellenőrzés nem alkalmazható az általam vizsgált PMR rendszerek nagy részének esetében, kivéve akkor, ha azok valamilyen hálózati infrastruktúrához kapcsolódnak, vagy egyéb távközlési rendszerek irányába is biztosítanak kommunikációt. Az engedély nélkül üzemeltethető, illetve az illegálisan alkalmazott eszközökre rendszerekre ez hatványozottan érvényes, így ezek esetében az egyedüli módszer az ellenőrzés kivitelezésére a kommunikációs felderítés. A cikkben, azok működésmódjának bemutatásán keresztül összefoglaltam a COMINT által a dPMR típusú rendszerekből

kinyerhető technikai és műveleti információkat, melyek jóval pontosabb azonosítást tesznek lehetővé az analóg rendszerekhez képest, mind a kommunikáció módja, tartalma, mind a résztvevő felek, illetve az alkalmazott rádiókészülékek azonosító és technikai adatai tekintetében. Mivel e témában még nem jelent meg magyar nyelvű szakirodalom, így mindenképpen hiánypótló a jelen cikk, mely a téma bevezető publikációjával [14] együtt jó alapot képez a kérdéskör további vizsgálatához, kutatásához. A téma aktualitását is mutatja, hogy a TS 102 490 szabvány legújabb verziója V.1.8.1 2014. júniusban jelent meg.

Felhasznált irodalom

[1] Rupert Thorogood, Charles Brookson: Lawful Interception, Telektronikk - Privacy in Telecommunications, Volume 103 No. 2. 2007., ISSN 0085-7130, Telenor 2007 http://www.telenor.com/wp-content/uploads/2012/05/T07_2.pdf (2014. 05. 05.)

[2] Haig Zsolt, Kovács László, Ványa László: Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata, FELDERÍTŐ SZEMLE 10. évf.: (1-2.sz.) pp. 183-209. http://www.kfh.hu/hu/letoltes/fsz/2011-1-2.pdf (2013. 04. 23.)

[3] ETSI TS 101 331 V1.4.1 (2014-02) , Technical Specifications, Lawful Interception (LI) Requirements of Law Enforcement Agencies http://www.etsi.org/deliver/etsi_ts/101300_101399/101331/01.04.01_60/ts_101331v010401p.pdf, (2014. 05. 10.)

[4] CML Microcircuits (White Paper): NXDN High Integration SDR Approch (2014. 04.08.) http://www.cmlmicro.com/products/CMX7131_CMX7141_Digital_PMR_Processors/ (2014. 05. 10.)

[5] ETSI Standard TS 102 490 V1.7.1 (2013-02): Electromagnetic compatibility and Radio spectrum Matters (ERM); Peer-to-Peer Digital Private Mobile Radio using FDMA with a channel spacing of 6,25 kHz with e.r.p. of up to 500 mW. ETSI 2013. 02. http://www.etsi.org/deliver/etsi_ts/102400_102499/102490/01.07.01_60/ts_102490v010701p.pdf, (2014. 05. 20.)

[6] ETSI Standard TS 102 658 V1.2.1 (2009-09): Digital Private Mobile Radio (dPMR) using FDMA with a channel spacing of 6,25 kHz. ETSI 2009.

[7] Digital Convenience Radio Equipment for Simplified Service, ARIB STD-T98 1.3 http://www.arib.or.jp/english/html/overview/doc/1-STD-T98v1_3.pdf (2014. 05. 25.)

[8] NXDN Technical Specifications TS 1-A Version 1.3, NXDN forum, 2011. November http://radioscanner.pl/wiki/images/f/f7/NXDN-TS-1-A_v0103.pdf (2014. 03.25.)

[9] Yufeng Li, Jun Yang, Qingyang Guan: Research on Channel Codec of DCR System Based on CMX7141, Communications and Network, 2013, 5, p. 286-291 http://www.scirp.org/journal/PaperDownload.aspx?paperID=39378 (2014. 05. 20)

[10] CMX8341 Digital PMR (dPMR) Baseband Pocessor Datasheet, CML Microcircuits, 2011. june http://www.alcom.nl/binarydata.aspx?type=doc/CML_CMX8341FI.pdf (2013. 10. 08.)

[11] CMX7131/CMX7141 Digital PMR Processor DCR Operation, Datasheet, CML Microcircuits, 2013. April http://www.cmlmicro.com/products/CMX7131_CMX7141_Digital_PMR_Processors/#ARIB STD-T98 (2013. 12. 06.)

[12] CMX7131/CMX7141 Digital PMR Processor NXDN Operation, Datasheet, CML Microcircuits, 2014. April http://www.cmlmicro.com/products/CMX7131_CMX7141_Digital_PMR_Processors (2014. 05. 06.)

[13] Dipl.-Ing. Roland Proesch: Signal Analysis for Radio Monitoring, Edition 2013, Books on Demand GmbH, Norderstedt, Germany, ISBN 9783732242566

[14] Balog Károly: A PMR rádiózás kialakulása, fejlődése, jelentősége napjaink hírközlésében, Társadalom és Honvédelem, 2013. XVII. évf. 3.-4. szám, pp. 97-115.

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Berecz Antónia
berecz@gdf.hu

AZ ÁLLAMI ÉS ÖNKORMÁNYZATI SZERVEKNÉL DOLGOZÓK JOGSZABÁLYOKBAN MEGHATÁROZOTT KÉPZÉSEINEK KÖLTSÉGEI BLENDED LEARNINGGEL

Absztrakt

A biztonsági összekötő személyek képzését a Katasztrófavédelmi Oktatási Központ végzi, az első képzés 2014 második felében indul, az elektronikus információbiztonsági képzések pedig a Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézetének honlapján 2014 elejétől vannak meghirdetve a jelentkezők számára a „Továbbképzések/Elektronikus információbiztonsági képzések" menüpontban. A képzéseket a tudásátadás biztonságának fokozása, a költséghatékonyság és a tanítási-tanulási élmény miatt is blended learning formájában javaslom megvalósítani. A jelenléti órákat és az önálló tanulási munkát online keretrendszerek támogató lehetőségeit kihasználva úgy kell megtervezni és lebonyolítani, hogy azok a képző intézmény, a munkavállaló és a munkaadó szervezet számára a leginkább megfelelők legyenek a költségek és a tudásátadás biztonságának szempontjából is.

The training of security liaison officers is conducted by the Disaster Management Training Centre. The first course will be launched in the second half of 2014. The courses in electronic information security have been advertised on the website of the Institute of Executive Training and Continuing Education (IETC) of the National University of Public Service in the menu item 'Further training' since the beginning of 2014. Because of cost-effectiveness and the security of the teaching/learning experience and of the transfer of knowledge I propose to conduct the training in the form of blended learning. Presence (classroom) lessons and self-access work (exploiting facilities provided by the online learning management systems as assistance) should be designed and carried out in a way that is the most favourable both in terms of costs and the security of transfer of knowledge.

Kulcsszavak: *elektronikus információs rendszer, biztonság, képzés, blended learning, ILIAS ~ electronic security systems, security, training, blended learning, ILIAS*

BEVEZETÉS

A nemzetközi tudományos irodalomban és a gazdaságban megfigyelhető, hogy a leginkább fontos gazdasági növekedési faktor az emberi tőke, az ebbe fektetett beruházások közvetlenül növelik a termelékenységet. A munkaerő piaci értékét egyre inkább a mentális képességek adják, amit az is mutat, hogy az új állások döntő részére magasan képzett munkavállalókat várnak.

Azért, hogy a társadalmak versenyképesek legyenek, és működésük zavartalan legyen, számos infrastruktúrát szükséges biztosítani. Az infrastruktúrák fizikai építményeket, rendszereket, eszközöket és azokat működtető, megfelelő szaktudással rendelkező embereket foglalnak magukban. Az infokommunikációs társadalmak infrastruktúrái és az azok közötti kapcsolatokban lényeges szerepet töltenek be az informatikai rendszerek és a kommunikációs hálózatok, amelyek technológiája sok átfedést tartalmaz, és amelyek üzemeltetéséhez, használatához képzett munkaerő, illetve felhasználó szükséges. A mai tudástársadalmak hatékony irányításához, az ügyintézéshez, a védelemhez elengedhetetlen az állami és az önkormányzati szervek információs rendszereinek biztonságos üzemeltetése.

A létfontosságú rendszereknél és létesítményeknél a képzett hatósági személyek és biztonsági összekötők, valamint az állami és önkormányzati szerveknél az informatikai feladatokat végző munkavállalók szervezett és tervszerű, államilag szabályozott képzésével az infrastruktúrák biztonságos működtetése magasabb szinten valósulhat meg. A képzések kidolgozásába bevont intézmények együttműködésének eredményeként a kutatások eredményesebbek lehetnek, a tananyagok folyamatosan frissülhetnek. Az országban szétszórtan dolgozók egységes, naprakész tananyagokból tanulhatnak, és egységes vizsgáztatási rendszerben adhatnak számot tudásukról. Munkájukon, illetve az általuk működtetett infrastruktúrákon keresztül az ország teljes lakosságára hatással lesz megemelt szintű képzettségükkel végzett tevékenységük.

JOGSZABÁLYOK ÁLTAL MEGHATÁROZOTT KÉPZÉSEK A LÉTFONTOSSÁGÚ RENDSZEREK ÉS LÉTESÍTMÉNYEK, ILLETVE AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁG TERÜLETÉN

Jogi szabályozások a vizsgált területeken

A Nemzeti Biztonsági Felügyelet honlapján összegyűjtve megtalálhatók az adatvédelemre és az elektronikus információbiztonságra vonatkozó nemzeti és nemzetközi jogszabályok [1]. Ebben a fejezetben közülük nem mindet emelem ki, de több más dokumentumot is bevonok a vizsgálatba. A fejezet elején lényeges fogalmakat határozok meg: kritikus (újabb, megfelelőbb fordításban létfontosságú) infrastruktúra, létfontosságú információs rendszer és létesítmény, információbiztonság, minősített adat; majd a jogi szabályozásokkal adok képet a létfontosságú rendszerek és létesítmények, illetve az elektronikus információbiztonság képzések jogszabályok által meghatározott hátteréről.

Az infrastruktúrák sok szempontból lehetnek kritikusak, de kritikussá minősítésükhöz elég az is, ha csak egy kritérium szerint azok (a kritikussá minősítés szempontjait lásd *65/2013. (III. 8.) Korm. rendelet A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról* [2].) Kritikus a törvény szóhasználatával élve a létfontosságú rendszerelem, ha „a benne meghatározott ágazatok – energia, közlekedés, agrárgazdaság, egészségügy, pénzügy, ipar, infokommunikációs technológiák, víz, jogrend-kormányzat, közbiztonság-védelem – valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.” [3:1. § f)]

A létfontosságú információs rendszerek és létesítmények a törvény megfogalmazásában „a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek.” [2:1§ 3.]

A létfontosságú rendszerelemekkel kapcsolatban különösen fontos adataink védelme, főként, ha az információbiztonság az információs és kommunikációs rendszerek, illetve az azokban kezelt adatok védelmére vonatkozik. A NATO szerint az információbiztonság (INFOrmation SECurity, INFOSEC) „a biztonsági rendszabályok alkalmazása a kommunikációs, információs és más elektronikus rendszerekben a feldolgozott, tárolt vagy továbbított információ bizalmasságának, sértetlenségének vagy rendelkezésre állásának véletlen vagy szándékos elvesztése ellen, és e rendszerek sértetlenségének vagy rendelkezésre állásának elvesztése ellen”. [4]

Az információbiztonságba beleértjük az információ minden megjelenési formájának (például elektronikus, papíralapú), az információs szolgáltatásoknak és az ezeket biztosító információs rendszereknek (akár szóbeli kommunikáció) a védelmét. Az információbiztonság jelen van a szervezetek minden területén, ezen kívül a feltételeinek megfelelő kialakítása és működtetése túl is mutat az információ biztonságos kezelésén. Beletartozik a szervezet minden erőforrásának, az embereknek, az eszközöknek, az információs rendszereknek és más vagyontárgyaknak a szabályozása, viselkedése, használata, ellenőrzése. Ezért irányítása a felső vezetés felelőssége. [5:13]

A *2009. évi CLV. törvény a minősített adat védelméről* (Mavtv.), a minősített adat létrejöttének és kezelésének alapvető rendelkezéseit, valamint a minősítési eljárás és a nemzeti minősített adat felülvizsgálatának rendjét tartalmazza. Meghatározza a minősített adat védelmének általános szabályait, a nemzeti iparbiztonság rendszerének főbb elemeit. Ezeken kívül rendelkezik még a minősített adat védelmét ellátó szervekről és személyekről. A törvény megteremteti a minősített adatok védelmének egységes jogszabály- és intézményrendszerét, és biztosítja a jogharmonizációt. Egységes követelményeket ad a nemzeti és a külföldi minősített adatok védelmére. [6]

A nemzetközi és hazai szabályozások a létfontosságú infrastruktúrák, illetve az információbiztonság területén alig egy évtizedre nyúlnak vissza, ezért az Európai Unió sem tud támaszkodni az egyes tagállamok kialakult gyakorlataira. Az Európai Unió a kritikus infrastruktúrák, illetve a kritikus információs infrastruktúrák szabályozásával először a 2004. június 18–19-i brüsszeli Európai Tanácson foglalkozott, ahol a tagállamok állam- és kormányfői átfogó stratégia készítését kérték az Európai Unió Bizottságtól és Tanácsától a létfontosságú infrastruktúrák védelmére.

A 2004-es madridi, majd a 2005-ös londoni terrortámadások után az Európai Bizottság 2005 novemberében adta ki az úgynevezett Zöld Könyvet. Ezután rendszeressé és fokozottá vált az EU kritikus infrastruktúrákat érintő irányelveinek és cselekvési terveinek kiadása, amelyek közül a fontosabbakat Haig–Kovács foglalta össze. [7:204] Közülük az egyik első *Az Európai Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről*. Az ennek való megfelelést szolgálja a *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről*. [3:16. §] Ide kapcsolódik még többek között, hogy az ország új nemzetbiztonsági stratégiáját 2012 márciusában határozatban fogadta el a kormány. A stratégiában szó van arról, hogy a kormányzat kiemelten kezeli a mindennapi élet fenntartásához szükséges kritikus infrastruktúrák hatékony védelmét. [8]

A *Digitális megújulás cselekvési terv 2010–2014*, amelynek alcíme *Az infokommunikációs ágazat cselekvési terve a társadalom és a gazdaság megújulásáért*, Magyarország középtávú

infokommunikációs cselekvési terve. Figyelembe véve az EU célkitűzéseit, infokommunikációs programjait, az európai digitális menetrendet, a cselekvési terv négy intézkedési főirány mentén elemzi a jelenlegi helyzetet, és fogalmazza meg a teendőket. A kritikus információs infrastruktúra-védelemmel kapcsolatban két területen ad intézkedési tervet és hozzájuk kapcsolódó akciókat: *i:2.11 IT-szakember át- és továbbképzési program* és *i:4.20 Összkormányzati szinten a kritikus információs infrastruktúrák védelme területén a tudatosságnövelés és az oktatás, továbbképzés*. A dokumentumnak *Az akciók megvalósításának ütemezése* fejezetében áttekinthetők a feladatok. Minden évre, így 2014-re is vannak feladatai az előbb említett két programhoz [9:104-111].

A *Digitális megújulás cselekvési terv 2010–2014* c. dokumentumban megjelöltekhez illeszkedik a *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről*, valamint a *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról*. Ezek adják dolgozatom témájának alapját, ezért az alábbiakban röviden áttekintem őket.

A 2012. évi CLXVI. törvényt az Országgyűlés „az élet és az anyagi javak védelmének, az alapvető szolgáltatások biztosítása folyamatosságának érdekében” alkotta. Ebben szabályozza a nemzeti és az európai (nemzetközi szóhasználattal) kritikus infrastruktúrák védelmét. A törvény rendelkezik az európai és a magyar kritikus rendszerek kijelöléséről, a kijelölés visszavonásáról, a nyilvántartás rendjéről, az üzemeltetői biztonsági tervek bevezetésének szükségességéről és az ellenőrzés rendjéről. A kormányzat ezután a törvény felhatalmazása alapján a *65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról* rendeletben készítette elő az azonosítási, kijelölési eljárás konkrét szabályait, az ágazati és horizontális (ágazattól független) kritériumok meghatározását és az ágazati üzemeltetői biztonsági terv formai, tartalmi követelményeinek meghatározását.

Most térjünk át a számunkra lényeges másik törvényre, de előbb annak egyik előzményére. *1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról* meghatározza a kormány kibertérre vonatkozó értékrendjét, jövőképét és céljait. [10] Megadja a hátteret a kibertér igényeihez és az ezáltal generált feladatokhoz alkalmazkodni képes kormányzati képességeket biztosító kormányzati struktúra kiépítésének is. A stratégia gyakorlati megvalósulását biztosítja a *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról*. Utóbbi megadja az intézményrendszert a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon és a létfontosságú információs rendszerek és rendszerelemek biztonsága alapfeltételeinek kialakításához. A törvény meghatározza, hogy hatálya mely szervekre, illetve hivatalokra terjed ki. [11:2. § (1)] Ezen felül ezt a törvényt kell alkalmazni a megadott szerveknél vagy azok számára adatkezelést végzőknél is, és a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozóinál, továbbá a létfontosságú rendszerelemek elektronikus információs rendszereinek védelmére. [11:2. § (2)] A törvény megadja, hogy mely szervek és szervezetek által kezelt, „a nemzeti adatvagyon részét képező adatok Magyarország területén üzemeltetett elektronikus információs rendszerekben, valamint diplomáciai információs célokra használt zárt célú elektronikus információs rendszerben kezelhetőek”. [11: 3. § (1)]

A szervezeteknek az általuk üzemeltetett rendszereket egyenként be kell sorolniuk biztonsági osztályba a bizalmasság, sértetlenség és rendelkezésre állás szempontjából. A szervezet biztonsági szintje az elektronikus információs rendszereinek legmagasabb biztonsági osztályával egyező besorolású, de van egy minimálisan előírt biztonsági szintje. [11:9. §] A törvény előírja a szervezeteknek az elektronikus információs rendszereik védelmét biztosító kötelezettségeit. [11:6. fejezet]

Jogszabályok által meghatározott képzések a vizsgált területeken

Biztonsági összekötők képzése

A 65/2013. (III. 8.) Korm. Rendelet az 5. pontjában adja meg a biztonsági összekötő személy képesítési követelményeit és foglalkoztatásának feltételeit. E szerint az adott ágazatnak megfelelő szakirányú végzettséggel kell rendelkeznie, valamint rendelkeznie kell

„a) védelmi igazgatási vagy rendészeti igazgatási szakon szerzett felsőfokú végzettséggel,
b) tűzvédelmi, iparbiztonsági, polgári védelmi szakmai irányú rendészeti szervezői szakképesítéssel vagy ezzel egyenértékű végzettséggel,
c) iparbiztonsági szaktanfolyami végzettséggel,
d) iparbiztonsági szakon szerzett felsőfokú végzettséggel, vagy
e) a katasztrófavédelem hivatásos szerveinél legalább 5 év iparbiztonsági szakterületen szerzett gyakorlattal."

Mentesül az a)–c) pontban előírt követelmények alól az a felsőfokú végzettségű személy, akiről rendvédelmi szerv igazolja, hogy a rendvédelmi szerv alaptevékenységébe tartozó feladatok ellátása körében legalább öt évig foglalkoztatták. [8]

A biztonsági összekötő személyek képzését a Katasztrófavédelmi Oktatási Központ (KOK) végzi saját és külső helyszínen. Az első képzés várhatóan 2014. augusztus második felében indul, majd az igények szerint folyamatosan. A képzés részletes leírása, illetve a jelentkezési lehetőség a KOK webes portálján található meg. [12]

A képzés két modult tartalmaz, amelyeket a végzettség megszerzéséhez teljesíteni kell: az általános katasztrófavédelmi és veszélyes ipari védelmi ügyintéző valamint a szakmai modult. A képzés levelező munkaformában történik. Az általános és a szakmai modul is 2x3 napos, 48–48 tanórás. A modulok elméleti és gyakorlati tanórákat tartalmaznak. A résztvevők jelenléti és egyéni tanulással készülnek, blended learning formában.

A legalább középszintű katasztrófavédelmi, polgári védelmi vagy tűzvédelmi képesítéssel rendelkező hallgató mentesül az általános modul tanóráinak látogatása és a (nagyjából) fele tandíj kifizetése alól. A képzés költségeiben benne van a munkaidőben történő jelenléti oktatás, a KOK tárhelyéről letölthető jegyzetek ára és az első vizsga. Vizsga a modulok teljesítése után tehető, amelynek sikere esetén a KOK bizonyítványt állít ki. [12]

A KOK-nál tehát elméleti és gyakorlati tanórákkal biztosított a biztonsági összekötők képzése. Jelenléti és egyéni tanulást is alkalmaznak, a blended learning kifejezés megjelenik a honlapon. Sajnos arról nem tájékoztatnak, hogy a weboldalukra belépve a hallgatók tanulását hogyan támogatják, például tutorokkal és mentorokkal.

Az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek képzése

A 2013. évi L. törvény szerint a szervezet vezetőjének kell gondoskodnia az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról. A törvény *IV. Oktatás-képzés és a kutatás-fejlesztés* fejezete a Nemzeti Közszolgálati Egyetem (NKE) körébe utalja a képzési tevékenységet, amely az alábbiakat foglalja magában:

- „gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,"
- „kidolgozza és a közigazgatás-fejlesztésért felelős miniszter elé terjeszti a vezetők, az elektronikus információs rendszer biztonságáért felelős személyek képzési, továbbképzési követelményeit, oktatási programját,"
- kidolgozza és a közigazgatás-fejlesztésért felelős miniszter elé terjeszti az elektronikus információs rendszer biztonságáért felelős személy képzettségi követelményeit,

- „gondoskodik a vezetők, az elektronikus információs rendszer biztonságáért felelős személyek és az általuk irányított szervezeti egységek munkatársai képzéséről és éves továbbképzéséről,”
- „közreműködik az információbiztonsági, kibervédelmi, létfontosságú információs rendszer védelmi gyakorlatokon.”

Ez után megszületett a *26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról*. A rendelet szerint az NKE kell, hogy meghatározza és tegye közzé honlapján az oktatások formáit (tantermi és e-learning) és azok arányát, tananyagát, a vizsga követelményrendszerét. Az NKE gondoskodik a szükséges oktatókról, a vizsgáztatás helyszíneiről és az elméleti oktatás segédanyagairól, a gyakorlati oktatás szükséges eszközeiről.

A rendelet meghatározza a képzési formák szükséges bemeneti, kimeneti és jelentkezési követelményeit, időtartalmát és az elméleti/gyakorlati részek arányát, tárgyköreit. Meghatározza továbbá azt is, hogy mi minősül szakmai gyakorlatnak, ki mentesül az oktatási forma alól.

Három képzési formát ad meg, amelyek 2014 elejétől vannak meghirdetve: [13]

1. Elektronikus információbiztonsági vezető képesítést nyújtó akkreditált szakirányú továbbképzés: iskolarendszerű, a 2011. évi CCIV. felsőoktatási törvényben meghatározottak szerint folyik a biztonságért felelős személy számára.

A felelős személynek a feladatellátáshoz szükséges felsőfokú végzettséget és szakképzettséget a 2013. július 1-jei hatálybalépést követő öt éven belül kell teljesítenie. Nem kell ezt a képzettséget megszereznie annak, aki a külön jogszabályban meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal rendelkezik.

Erre a zárt képzésre az állami és az önkormányzati szerveknél foglalkoztatott, információs rendszerekért felelős személyek munkáltatói delegálás alapján jelentkezhetnek. A felvétel feltétele felsőfokú végzettség és angol nyelvből legalább alapfokú komplex nyelvvizsga.

A nemzetközi oktatási környezetben elfogadott akkreditált képzések közül az Information Systems Audit and Control Association (ISACA) nemzetközi szervezet Certified Information Security Manager (CISM) képzését vették alapul e továbbképzési szak kidolgozásakor.

A képzés programtípusa e-tananyag és jelenléti képzés, vagyis blended learning. Óraszáma 2 félév (320 óra), amely 80% elméleti és 20% gyakorlati részből áll. Tanulmányi pontértéke 48. A képzés költségtérítéses. A 26/2013. (X. 21.) KIM rendelet felsorolja, hogy mi minősül szakmai gyakorlatnak. A képzésben szakdolgozatot kell készíteni, valamint a kurzust vizsga zárja.

2. Továbbképzés: iskolarendszeren kívüli képzés, igény esetén indul
    a) az elektronikus információs rendszerek védelméért felelős vezető számára,
    b) az elektronikus információs rendszerek biztonságával összefüggő feladatok ellátásában részt vevő személy számára.
3. Éves továbbképzés: iskolarendszeren kívüli képzés, igény esetén indul
    c) az elektronikus információs rendszerek biztonságáért felelős személy számára,
    d) az elektronikus információs rendszerek védelméért felelős vezető számára,
    e) az elektronikus információs rendszerek biztonságával összefüggő feladatok ellátásában részt vevő személy számára.

Az alábbi táblázatban a nem iskolarendszerű továbbképzés, illetve éves továbbképzés tulajdonságait gyűjtöttem össze. Mindegyikre igaz, ezért nincs a táblázatba foglalva, hogy

- e-learning formájúak, a kötelező szakirodalom e-learning tananyag,
- a részvételre vonatkozó elvárás az e-learning tananyag teljes megtekintése,
- a képzés végi vizsgán feleletválasztós kérdéseket kap a hallgató, amelyeknek minimum 50%-át kell helyesen megválaszolni a sikeres teljesítéshez.

A táblázat fejlécében

- vezető: az elektronikus információs rendszerek védelméért felelős vezető,
- feladatok ellátásában részt vevő: az elektronikus információs rendszerek biztonságával összefüggő feladatok ellátásában részt vevő személy,
- felelős személy: az elektronikus információs rendszerek biztonságáért felelős személy.

A vezető továbbképzése és éves továbbképzése, valamint a feladatok ellátásában részt vevő éves képzése esetén bár a témakörök megegyeznek, de azonos irányú az eltérés az óraszámban és pontértékben. A feladatok ellátásában részt vevő továbbképzése és a felelős személy éves továbbképzése esetén a témakörök szintén megegyeznek, de ott nincs eltérés az óraszámban és pontértékben.

Hosszabb képzések esetén mindenképpen blended learning formát javaslok, viszont ezekben az esetekben is e-learning van megadva. Sajnos a honlapon nem hangsúlyozzák ki, hogy milyen tanulástámogatást nyújtanak az önálló munkához – például tanulási ütemterv, útmutató, aktív tutorálás és mentorálás a *12/2013. (III. 14.) KIM utasítás a közszolgálati tisztviselők továbbképzésének minőségirányítási szabályzatáról* szerint.

A *Közszolgálati továbbképzési programkatalógus 2014* a szakmai továbbképzési programok között tartalmazza az e-biztonsági képzéseket. [14:157-161] Ezek a képzések díjkötelesek, a továbbképzési normatíva nem tartalmazza.

	vezető		**feladatok ellátásában részvevő**		**felelős személy**
	továbbképzés	éves továbbképzés	továbbképzés	éves továbbképzés	éves továbbképzés
óraszám	8		50	25	50
pontérték/ kts. ezer Ft	8		32	16	32
részvétel előfeltétele	nincs	továbbképzés	nincs	továbbképzés	akkreditált szakirányú továbbképzési szak
témakörök	- információbiztonsági technológiai ismeretek - informatikai biztonságpolitikai, stratégiai és szabályozási ismeretek - jogi, közigazgatási, vezetéselméleti és szervezeti ismeretek		- kockázatértékelés és biztonsági események kezelése (incidenskezelés)		- kockázatértékelés és biztonsági események kezelése (incidenskezelés)
vizsgán kérdés (db)	20		50	25	50
sikeres teljesítés esetén	bizonyítvány	tanúsítvány	bizonyítvány	tanúsítvány	tanúsítvány

1. táblázat. Az elektronikus információs rendszerek továbbképzések és éves továbbképzések adatainak összefoglalása

KÉPZÉSI PROGRAMOK TÍPUSAINAK BEMUTATÁSA

A képzési programok típusainak áttekintése

A hagyományos képzések esetén a tanár a fő információforrás. A tudást személyes jelenlétet igénylő előadásokon és gyakorlatokon adja át. A tanulásra készített könyvekben is ott van a tanár: kiemeli a lényeget, rendszerez, vagy például ellenőrzésre, továbbgondolkodásra késztető kérdéseket és feladatokat ad fel. A távoktatásban, amely „a tanítási/tanulási idő és hely szempontjából rugalmas képzési forma, mely biztosítja a naprakész tudást, akár földrajzilag is szétszórtan élő célcsoport számára" [15] ezért az önálló feldolgozásra szánt könyvekben és munkafüzetekben „megjelenő" tanárra különösen nagy súlyt helyeznek.

Az elektronikus médiumok használatával a tanár, illetve a tananyag egyre inkább irányító, facilitáló szerepet tölt be. Legtágabb értelemben az e-learning körébe soroljuk mindazokat a tanítási-tanulási megoldásokat, amelyek valamilyen elektronikus eszközt használnak – legyen az CD-n megjelenő, programozott oktatást megvalósító tananyag, vagy csak egy részterület ismereteit gyakoroltató vagy számon kérő elektronikus teszt.

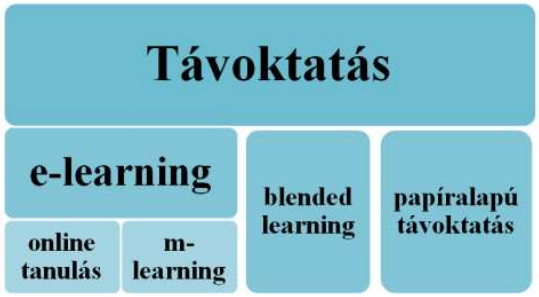
Az e-learning egy általános definíciója szerint "elektronikus hálózaton megvalósított tanítás-tanulás, amelyben az oktatási tartalmak az interneten, intraneten, extraneten keresztül érhetőek el, különböző infokommunikációs (IKT) eszközök segítségével." [16:74] Másként megfogalmazva az e-learning „olyan távoktatás, amely elektronikus úton valósul meg." [16:62] "A távoktatás számos elemzés szerint nem csak a közoktatás és egyéb felsőfokú, illetőleg a posztgraduális képzésekben nyújthat költséghatékony megoldást az oktatásszervezés területén, hanem a közigazgatási szektorban is, méghozzá a közszolgálati alkalmazásban állók rendszeres továbbképzésében." [16:62]

Tiszta e-learning alapú oktatás, illetve online tanulás ritkán valósul meg. Ehhez a tanítás-tanulás minden elemét elektronikusan kell megvalósítani a képzésre jelentkezéstől az (akár) egyéni igényeknek megfelelő multimédiás tananyagokig és a számonkérésig. A tiszta e-learnig ezen kívül magas tanulói motivációt és önálló tanulási készségeket feltételez. Napjainkra az „olvasott web"-ről, a Web 1.0-ról fokozatosan az „írott-olvasott web", a Web 2.0 irányába haladunk a tanítás-tanulás során is. A hallgatók akár egymással együtt dolgozva is új tartalmakat készítenek – amely szintén részét képezi a magas színvonalú e-learningnek.

A mobil tanulás (m-learning) az e-learning része. Az NKE Vezető és Továbbképző Intézetében (VTKI) is súlyt helyeznek az egyre inkább terjedőben levő mobil tanulási eszközök, technológiák használatára a tanításban-tanulásban. Ezekkel bármely hallgató bárhol, bármikor (3B elmélet) elérheti az online képzések webes tanulási terét, valamint a költséghatékonyságot is emelheti. [16]

A vegyes/ kevert oktatás vagy blended learning „olyan oktatási technológia, amely a képzéshez változatos tanulási környezeti elemek (módszerek és eszközök), hagyományos és virtuális tantermi tanulási formák, személyes és távolsági konzultáció biztosításával, nyomtatott- és elektronikus tananyagok segítségével hi-tech infokommunikációs eszközök révén a tananyagot kooperatívan, változatos módszerekkel, egyénre szabott formában teszi hozzáférhetővé, biztosítja a tanulók előrehaladási ütemének ellenőrzését, értékelését." [17]

A fentiekben meghatározott oktatási formákat tekinti át az alábbi ábra, amelyen „a mobiltanulás távoktatáson belül sokak által elfogadottan van ábrázolva, az e-learningen belül helyezkedik el az online tanulás mellett." [18]



2. ábra. Az m-learning helye a távoktatáson belül [18]

A 12/2013. (III. 14.) KIM utasítás a közszolgálati tisztviselők továbbképzésének minőségirányítási szabályzatáról három fő formáját határozza meg a képzéseknek: hagyományos (jelenléti) képzés, e-learning és vegyes (blended learning) képzés. [15]

Az *On-line képzési stratégiák és nemzetközi jó gyakorlatai a közszolgálati továbbképzések terén* tanulmányban [16] a blended learning és a vegyes képzés kifejezés egyszer-egyszer fordul csak elő, a kevert oktatás egyszer sem, viszont az m-learninggel örvendetes módon két alfejezetben is foglalkoznak. A tanulmány javaslata szerint Magyarországon sikeresen alkalmazható az online közszolgálati továbbképzés az „angol minta alapján a jogalkotók, joghasználók szakmai tudásának frissítésére, illetve az ágazatban újonnan elhelyezkedett alkalmazottak számára…" [16:7–8] Ez is azt mutatja, hogy az általam vizsgált területeken a teljesen e-learninges képzés nem megfelelő. A létfontosságú rendszerek üzemeltetésében közreműködő hatósági személyek és biztonsági összekötők képzése a KOK-ban blended learning képzésben [12], viszont az állami és önkormányzati szervek elektronikus információbiztonsági képzései e-learning képzésben vannak meghirdetve, kivéve az iskolarendszerű elektronikus információbiztonsági vezető képesítést nyújtó akkreditált szakirányú továbbképzést az NKE-n, amelyet blended learningben kínálnak [14: 183].

A *Közszolgálati továbbképzési programkatalógus 2014* a VTKI-ben folyó közszolgálati tisztviselői továbbképzéseket is alapvetően három oktatás-módszertani típusba sorolja: jelenléti képzés, e-tananyag, valamint a két oktatási módszert ötvöző továbbképzés (bár a blended learning vagy kevert tanulás kifejezést nem használják ebben a dokumentumban sem). „A jelenléti és e-learning módszereket ötvöző képzéseink nagy előnye, hogy a tanulás során nem kell lemondani a személyes kapcsolatok, az azonnali reagálások és visszacsatolások, az elsajátított ismeretek közvetlen ellenőrzése adta előnyökről, úgy, hogy mindezt közben a kényelmi funkciókat is biztosító korszerű e-learning modulok támogatják és egészítik ki, így téve még hatékonyabbá és élményszerűbbé a tanulást." [14]

A programkatalógusban sok továbbképzési program típusa e-tananyag vagy e-tananyag és jelenléti képzés. Utóbbi „keretében azonos elsajátítandó tudásanyaggal, de magasabb óraszámmal, magasabb pontértékkel és eltérő oktatási módszerrel találkoznak a tisztviselők". A vizsga különbözőségét nem említik. A magasabb óraszámban tanulók magasabb (tantermi, oktatói stb.) költséggel, magasabb kreditszámot szerezhetnek. [14] Az oktatói segítséggel és változatos módszerekkel való tanulás magasabb szintű megértést, készségeket fog eredményezni. Véleményem szerint ehhez más, a pusztán e-learninges képzéstípustól eltérő vizsgára van szükség, amely nem csak online tesztet tartalmaz, hanem olyan típusú feladatokat is, amelyekre a jelenléti képzést létrehozták.

A *12/2013. (III. 14.) KIM utasítás a közszolgálati tisztviselők továbbképzésének minőségirányítási szabályzatáról* az eddig definiált tanulási formákon, illetve tanulási formákon és tananyagtípusokon kívül még továbbiakat is definiál. A távoktatás forma után az e-learning 1.0, más megnevezéssel alapszintű stúdium következzen most a sorban, amely „az IKT-kal segített tanulás, „magába foglalja az oktatási rendszerek és módszerek átalakítását (adaptálását) az IKT alkalmazásokhoz". Ez után az e-learning következik, amely technológiailag és formailag is a számítógépes hálózatokhoz kötődik. Egységes

keretrendszerbe foglalva teszi hozzáférhetővé a tananyagot és a tanulói forrásokat, valamint a tutor-tanuló kommunikációt és az interaktív számítógépes oktatószoftvert. Az e-Learning 2.0, más megnevezéssel emelt szintű stúdium már használja a mobil kommunikációs eszközöket és az egymásba kapcsolódó hálózatokat. „Gyakorlatában tolódik a web 2.0 alkalmazások tudatos integrálása felé, és cselekvési elvnek a szabad tudásmegosztást teszi." Végül zárja a sort a „szimulációs-szerepjátékos stúdium: a közigazgatásban előforduló, munkavégzéssel, ügyintézéssel kapcsolatos szituációkat, élethelyzeteket szimuláló, szakmai tudást és készségeket fejlesztő tanulási forma illetve tananyag". [15]

A blended learning oktatás sikerének okai és lehetőségei

A blended learninget (vagyis a tantermi és az interneten keresztüli, tervszerűen „kevert" tanítást-tanulást) Ágoston–Budai szerint az teszi sikeressé, hogy elfogadható a tradicionális és a távoktatási intézmények számára is a megfelelő testre szabással, vagyis a módszerek és az eszközök kiválasztásával. Ez a tanítás-tanulás evolúciósan alakítható ki és fejleszthető, radikális változások nélkül. [19]

Amellett, hogy a blended learning jól használható a közoktatásban és a felsőfokú oktatásban, hatékonyan képes támogatni a törvényekben, egy-egy munkakör betöltéséhez előírt képzéseket, továbbképzéseket is, valamint az átképzéseket, szakirányú továbbképzéseket. A biztonság és az informatika területén továbbtanuló szakemberek esetében különösen lényeges az élethosszig tartó tanulás (LLL), illetve az élethelyzethez igazított tanulás [20], így itt a blended learning kifejezetten hatékony.

Fontos, hogy a tudásátadás megfelelő biztonsági szintjét érjük el a blended learning képzési formában is. Varga–Pálosi kimutatták, hogy a tudásátadás ugyanakkora biztonsági szintje érhető el bizonyos mértékű IKT használatával, mint 100%-ban osztálytermi oktatással, de progresszíven alacsonyabb költségek mellett. [21]

Az alacsonyabb költségek egyik oka a blended learning alkalmazása esetén, hogy az oktatásban több hallgatónak van lehetősége részt venni, mint a hagyományos tantermi képzésben, mert például a kreditek teljesítéséhez szükséges óraszám nagy részét a képzőintézményen kívül, saját időbeosztás szerint teljesítik. A magasabb hallgatói létszám egyben növeli az intézmény jövedelmezőségét is, amely ösztönzően hat az intézmény oktatási minőségének fejlesztésére. Ez újra a hallgatói létszám növekedését okozza, ami ismét pozitívan hat az oktatás minőségére. [21]

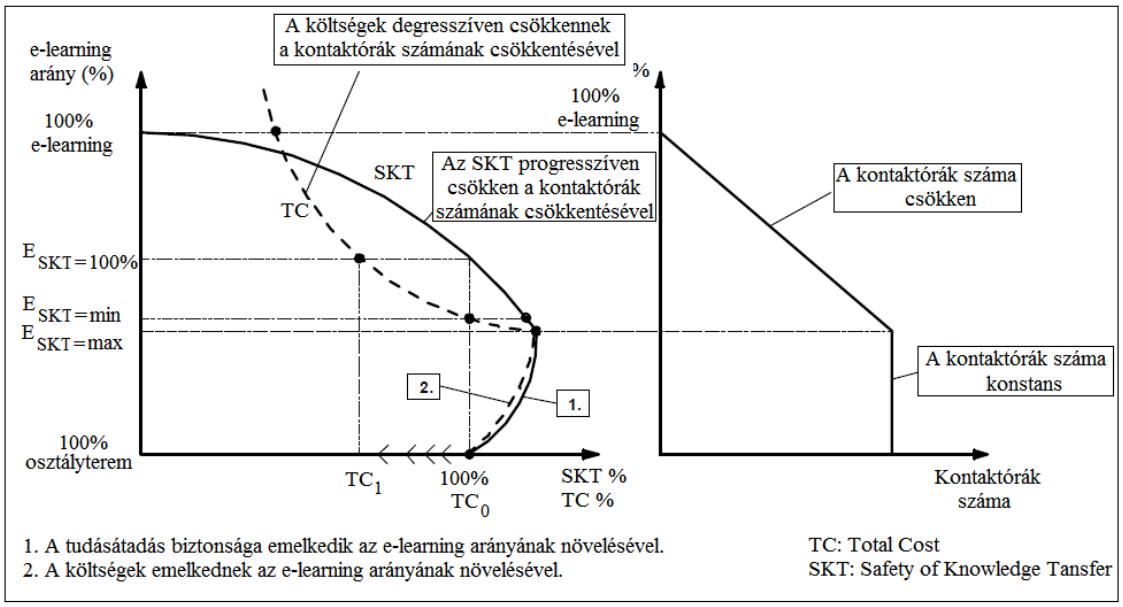
A blended learning bevezetésekor költséges fejlesztések szükségesek (emberi és tárgyi infrastruktúra, tananyag-fejlesztés terén), hogy elérjük, majd aztán kihasználjuk a gazdasági előnyöket. Varga–Pálosi kutatásai szerint ebben az esetben az IKT alkalmazások növekedése az oktatási folyamatban automatikusan maga után vonja a tudásátadás biztonságának csökkenését.

Az alábbi ábrán az oktatásban az e-learning elemek közötti arányt, a teljes költséget és a tudásátadás biztonságát (safety of knowledge transfer, SKT) vizsgálja Varga–Pálosi. Az ábra azt mutatja, hogy ha az osztálytermi órák száma állandó, akkor az IKT alkalmazások erősítése növeli a tudásátadás-biztonság mutatóját, és a költségek fokozatosan csökkennek. Az IKT alkalmazás egy bizonyos szintjén (ESKT=max) lehetséges csökkenteni a kontaktórák számát, ami szintén a költségek fokozatos csökkentéséhez vezet, de progresszíven csökken a tudásátadás biztonsága.

Ha az oktatási intézmény azért épít be a kurzusaiba IKT-elemeket, mert elkerülhetetlen az IKT használata, csak akkor eredményez költséget és SKT-t, ha a kezdeti fázisban jelentkezik, amikor a kontaktórák számának csökkentése nem lehetséges. Később az IKT alkalmazás ESKT=max szintje a kontaktórák csökkenésével az eredeti költségszinten (Emin) vezet jobb SKT-hez. A költségstruktúra vissza fogja tartani az intézményeket, hogy további IKT-

eszközökbe ruházzanak be, amíg az arány nem haladja meg az Emin-t. Az IKT-arány meghatározása mindig intézményfüggő, ez az ő döntésük eredménye.

Elégséges az IKT-t ESKT=max szinten alkalmazni. Viszont az e-oktatás makroelőnyei miatt az IKT-arány emelése javasolt, mert a munkaerő képzettségének fejlődése az emberi alapú gazdasági növekedés előfeltétele. Ehhez szükséges a jelenlegi oktatási rendszer kerete is. Az IKT-arány további növelése után egy adott szint fölött (ESKT=100%) az SKT visszaesik a kezdeti szintre, de alacsonyabb költségen integrálható a makroelőnyökbe. [21]



1. ábra. Kapcsolat az oktatás e-learning elemeinek aránya és a teljes költség, valamint a tudásátadás biztonsága között [21]

Varga–Pálosi kutatásai szerint ekkor az IKT-alkalmazások növekedése az oktatási folyamatban automatikusan maga után vonja a tudásátadás biztonságának csökkenését. Ennek az az oka, hogy a rendszerek tanulásra kényszerítő ereje csökken a folyamatos tanár-hallgató találkozások hiánya miatt. Viszont a hallgatóknak ugyanazt a tudásszintet kell elérniük a képzés során, hogy diplomájuk/oklevelük ugyanolyan piaci értékű legyen.

Varga–Pálosi kutatásai a nemzetközi tudományos irodalomban azt mutatják, és személyes tapasztalatom is az, hogy nincs különbség a hallgatói jegyek, teljesítmények között a különböző tanulási munkaformában (nappali, levelező, távoktatás) tanulók között. Viszont a távoktatásban tanulóknál nagyobb az esélye a tanulmányok idő előtti feladásának. Gyakoribb a folyamatos tanulásnak, aztán a hallgatói viszonynak a szüneteltetése, amelyek szintén a tanulmányok feladásához vezetnek.

Az önálló tanulás gyakorlatának hiánya miatti lemorzsolódás csökken, ha a hallgatóknak már korábbi tanulmányaik alatt részük volt önálló tanulásban. Ezt a gyakorlatot megszerezhetik általános és középiskolában is, ahol egyre több IKT-elemet alkalmaznak. Ma már azonban a gyerekek többségének lehetősége van otthon is számítógép- és internethasználatra. Az érettségi után hosszabb szervezett képzésben részt nem vevők tanulási kompetenciái viszont az életkor előrehaladtával egyre alacsonyabbak. A diplomás továbbtanulók döntő többsége nagy önálló tanulási tapasztalattal, kialakult tanulási stílussal és hatékony tanulási stratégiával rendelkezik. A hallgatóknál iskolai végzettség tekintetében „Általában nem csak, és nem elsősorban a kognitív képességeik tekintetében mutatkoznak különbségek, inkább a tanulási és vizsgarutin, a tanulási stílus terén” [15]. Mindemellett véleményem szerint az egyes tantárgyak/ modulok és a teljes képzés során szükséges a hallgatók monitorozása, odafigyelés a tanulmányi előrehaladásukra, hogy biztosítsuk a folyamatos tanulást és a képzés végén a kimeneti követelményeknek való lehető legjobb megfelelést.

Blended learning képzések az NKE két szervezeti egységében

Ebben a részben az NKE két szervezeti egységében folyó képzéseket tekintem át. A Vezető- és Továbbképzési Intézet (VTKI) és Katonai Vizsgaközpont (KVK) is az élethelyzethez igazított tanulást [20] igyekszik támogatni, és képzésein, továbbképzésein több oktatási formát is nyújt (honlapjukon megnevezettek: jelenléti oktatás, távoktatás, e-learning, blended learning). Véleményem szerint minden képzésnél és továbbképzésnél a blended learningre kellene törekedni, és a képzésben résztvevők (oktatók, hallgatók, referensek/mentorok stb.) számára online elérhetővé tenni minden lehetséges, az őket érintő képzéssel kapcsolatos tananyagelemet, oktatáshoz kapcsolódó objektumot.

Az elektronikus tananyagok szolgáltatását és a vizsgáztatást ILIAS e-learning keretrendszer használatával oldja meg a VTKI és a KVK. A VTKI szervezeti egységei, illetve képzései számára működő ILIAS a Továbbképzési és Vizsgaportál, amely a https://tvp.uni-nke.hu/portal/ címen érhető el. A KVK képzései számára működő ILIAS a http://kvk.uni-nke.hu/ilias címen érhető el.

„A VTKI munkája a modern, elkötelezett közszolgálati állomány folyamatos, szisztematikus fejlesztését, végső soron a jó kormányzást, ezen keresztül hazánk versenyképességét is szolgálja. A VTKI feladatai ellátásához együttműködik az Egyetem karaival és intézeteivel, a felsőoktatási társintézményekkel és a közigazgatási szervezetekkel, kiemelten a Közigazgatási és Igazságügyi Hivatallal, valamint a kormányhivatalokkal kialakított kooperációs hálózatokban.

Az Egyetem stratégiai célja, hogy többoldalú együttműködés keretében bekapcsolja a kimagasló szakmai műhelyekkel rendelkező hazai felsőoktatási intézményeket, ahol módot ad és keretet teremt a magyar felsőoktatás információbiztonsági oktatási és kutatási lehetőségeinek közös áttekintésére, szakmai együttműködésre az e-közszolgálat, a technológiai modernizáció, sőt a magyar információs társadalommal kapcsolatos képzések, továbbképzések koordinálásában is.” [22]

Az Egyetem, azon belül a VTKI feladata és felelőssége:

- Közigazgatási vizsgák: Az Egyetem a 2012/2013-as tanévben kezdte meg a tervezett közigazgatási továbbképzési rendszer igényeinek megfelelő fejlesztéseket. Az NKE VTKI a továbbképzési rendszerrel kapcsolatban a szakmai-módszertani és minőségirányítási központ is. Sok ezer hallgatót képzenek a sok száz kurzusukon, majd vizsgákat szerveznek számukra.
- Továbbképzés: a 26/2013. (X. 21.) KIM rendelet az NKE feladatai közé sorolta az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzését és továbbképzését, amelyek honlapján meg vannak hirdetve jelentkezésre.
- Szakirányú továbbképzések: „A szakirányú továbbképzési szakok célja, hogy a hallgatók bizonyos szűkebb közszolgálati területeken széles horizontú, multidiszciplináris, elmélyült ismereteket szerezzenek.” Több ezer fős a hallgatói létszám itt is. Feladatkijelölés alapján közreműködik egyes ÁROP (Államreform Operatív Programok) projektek szakmai és szervezési feladataiban. A meglévő szakirányú továbbképzési szakok egy része nyitott képzésként került meghirdetésre, vagyis az egyes szakok KKK-jában (önkormányzati szaktanácsadó szakirányú továbbképzési szak képzési és kimeneti követelményei) meghatározott előképzettség birtokában bárki részt vehet azokon, nem szükséges hozzá közszolgálati jogviszony. A VTKI szervezeti egységei közül a legszorosabban kapcsolódik a felsőoktatási képzési rendszerhez.
- ÁROP (Államreform Operatív Programok) projektek: Ezekben többek között elektronikus képzési és távoktatási anyagok készítése folyik. Ezek közül témánk

szempontjából az egyik legizgalmasabb a 2013.01.01–2014.05.31. közötti ÁROP-2.2.19, amely célja az e-tananyagfejlesztés állandó szakmai és intézményi bázisának kiépítése. A közszolgálati tisztviselői kar képzési igényeit akarja kielégíteni a hagyományostól eltérő e-learning, blended learning és szimulációs módszerű továbbképzési formákban. Ennek keretében került kidolgozásra az *On-line képzési stratégiák és nemzetközi jó gyakorlatok a közszolgálati továbbképzések terén* tanulmány is [16].

- Módszertani és Minőségirányítási Központ: „A továbbképzési programok minősítésével, nyilvántartásával, a közszolgálati programok fejlesztésével, az oktatók, tutorok, szakértők, trénerek és egyéb közreműködők felkészítésével, nyilvántartásával, valamint a minősített továbbképzések teljes körű minőségbiztosításával… foglalkozik."

A *VTKI továbbképzései* menüpontban tájékoztatást kapunk a 2013. évi L. törvény és a 2013. 26/2013. (X. 21.) KIM rendelet által az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról, a jelentkezés módjáról.

A KVK-nak „a Magyar Honvédség egész állományára kiterjedő feladata a teljesítményértékeléshez szükséges éves fizikai felmérések, az önkéntes jelentkezésen alapuló minősítő (katonai elméleti, szakmai elméleti) vizsgák előkészítése, a vizsgáztatás végrehajtása, felügyelete, illetve a szakmai előmeneteli rangsor összeállítása. További feladata a meghatározott (magasabb) szintű, illetve a külszolgálatok parancsnoki, vezetői beosztás betöltésére tervezettek kiválasztásának támogatása." Tevékenységei közé tartozik többek között a vizsgarendszer kialakítása, egyéni felkészülést lehetővé tevő oktatócsomagok kidolgozásának tervezése és koordinálása, távoktatási rendszer kialakításának és működtetésének koordinálása. [23]

A BLENDED LEARNING KURZUSOK FELADATAI ÉS KÖLTSÉGEI AZ OKTATÁSI INTÉZMÉNYEKBEN

Közszolgálati tisztviselők továbbképzésének minőségirányítási szabályzata

A 273/2012. (IX. 28.) Korm. rendelet nyomán született a *12/2013. (III. 14.) KIM utasítás a közszolgálati tisztviselők továbbképzésének minőségirányítási szabályzatáról.* Az utasítás szerint az NKE VTKI-nek „a közszolgálati tisztviselők továbbképzési rendszerében az egyik fő feladata, hogy kidolgozza és működtesse a továbbképzés minőségirányítási rendszerét, ezért a továbbképzéssel szembeni összes minőségügyi követelményt dokumentált minőségirányítási folyamatleírásban határozta meg." Az Eljárásgyűjtemény tartalma lefedi a közszolgálati továbbképzésekkel kapcsolatos folyamatokat a továbbképzési programok nyilvántartásba vételi eljárásától (I. ME-TK-01) a képzések tervezésén-fejlesztésén-megvalósításán, az oktatási módszerek, oktatási és segédanyagok kialakításán, infrastruktúrán és oktatási környezeten, értékelésen keresztül az önértékelésig és az éves működés értékeléséig (XXII. ME-TK-22). [15]

Ez az eljárásgyűjtemény véleményem szerint a 2012. évi CLXVI. és a 2013. évi L. törvényben megjelölt szakmai képzésekhez is alkalmazható, de mivel a biztonsági összekötő személy képzését a KOK, az elektronikus információbiztonság területén igényelt képzéseket pedig csak az NKE végzi, ezért a külső akkreditált intézménnyel kapcsolatos eljárásokra nincs szükség.

Bár az elektronikus információbiztonság képzéseinél csak e-learning tananyagot kapnak a hallgatók, de már a képzésekre beiratkozásnál is nyújt tájékoztatást a VTKI honlapján „a képzés lebonyolításának körülményeiről, a képzések során alkalmazott módszerekről és elvárásokról". A továbbképzések során alkalmazott oktatási és segédanyagok magukban foglalnak tanulási

ütemtervet és útmutatót. A hallgató tanulását segítik továbbá utasítások, javaslatok, tanulást segítő tananyagelemek, támogató tutori munka. Az online keretrendszer használatát helpdesk szolgálat, illetve kurzusadminisztrátor támogatja. A hallgatóknak lehetőségük van kapcsolatot tartani fórumokon, de az oktatók által választható akár onlie közösségi portál is nevelési, oktatási környezetként. [15]

Mindezek mellett hasznosnak tartanék a rövidebb kurzusok esetén egy kezdő, áttekintő előadást a követelményekről, a keretrendszer használatáról, a szakanyagról, a tanulástámogató egyéb lehetőségekről. A hosszabb kurzusok esetén még további előadásokra is szükség lehet. Ezeket kis csoportokban internetes videokonferencián is le lehet bonyolítani, akár ingyenes szoftverekkel is. A blended és e-learningben alkalmazható tanulástámogató módszerekről későbbi fejezetekben részletesebben is szólok.

A képzések megvalósítását szolgáló költségek

Sajnos az NKE önköltségszámítási szabályzatához nem fértem hozzá, mert nem nyilvános. Ezért nem tudom számba venni a vizsgált kurzusok közvetett és közvetlen költségeit, valamint az állandó és változó költségeket, illetve a költségviselőket. A 2012. évi CLXVI. és a 2013. évi L. törvényben foglalt képzések költségei mégis áttekinthetők a *12/2013. (III. 14.) KIM utasítás a közszolgálati tisztviselők továbbképzésének minőségirányítási szabályzatáról* alapján. Függelékében a továbbképzési programok minősítésével, a képzésfejlesztéssel, a képzések megvalósításával és ellenőrzésével kapcsolatos tevékenységekre, szolgáltatásokra, termékekre és költségtérítésekre vannak számba véve, valamint forintban megadva az egységköltségek – jelenleg a 2014. évre. Az egységköltség „a továbbképzési normatívából teljesíthető egy tanulmányi pont költsége, amelyet a KTK (Közigazgatási Továbbképzési Kollégium) határoz meg tárgyévre vonatkozóan a közszolgálati és vezetőképzések fejlesztésének, működtetésének, valamint a rendszer kapcsolódó költségeinek figyelembevételével.” Ezért a függelék nem terjed ki például a minőségbiztosítási ellenőrzésekkel kapcsolatos költségekre, az oktatók pályáztatásával, nyilvántartásával kapcsolatos költségekre, a tananyagverziók nyilvántartásának és archiválásának költségeire.

Amint fentebb írtam, a biztonsági összekötők képzését a KOK, az elektronikus információs rendszer biztonsági képzéseket az NKE végzi, ezért nincs szükségük a 12/2013. (III. 14.) KIM utasításban szabályozott, a más képző intézményeknél elkészített képzési programok minősítésére és helyszíni ellenőrzésekre (a *Függelékben* az *I. Programminősítési díjak* és a *II. Helyszíni ellenőrzés díja* pontok).

A *III. Képzésfejlesztés díja* pontban a tananyagfejlesztés és -előállítás költségei kerültek felsorolásra a 12/2013. KIM utasításban. Logikusan és helyesen két díjcsoport van, mivel a tananyagkészítés elválik: 1) szakanyag elkészítése egy dokumentumban/fájlban (szerzői díj) és 2) a tananyagfejlesztés, amely lefedi a teljes dokumentum tartalomfejlesztési és előállítási díját. Utóbbi díjait 45 perces tanórára vetítve, módszertani és technológia műveletekkel együtt adja meg az utasítás.

A *IV. Képzésszervezés, lebonyolítás, oktatás* pontban vannak a humánerőforrás-díjak: oktató, konzulens, tréner; oktatók felkészítője; konferenciaelőadó; tutor; vizsgabiztos, vizsgabizottsági tag; vizsgaelnök; oktatásszervező; konferenciaszervező; helpdesk (segítségnyújtási) operátor; technikai munkatárs. A tevékenységek ellátásához szükséges dologi kiadások beleértendők a díjakba. A tutor díja tartalmazza a képzésre felkészülést, a képzés helyszínére utazást és a képzés idejére eső költségeket. A 12/2013. KIM utasítás feljebb a függelékben találhatónál több oktatói szerepet (és többször) definiál: tanár, oktató, tutor, facilitátor, konzulens, tréner, coach.

Az e-learningben, illetve a blended learning önálló, online keretrendszerrel támogatott szakaszaiban különösen fontos a hallgató támogatása. Ekkor a tutor „a képzési terv alapján felkészül és a megadott módon (szinkron-aszinkron) tutori támogatást nyújt egyénileg vagy

csoportosan meghatározott időtartamban, és ügyeleti idővel a kifejlesztett elektronikus tananyagra és tutori specifikációra támaszkodva. A tutor egyszerre, egy időben egy képzésben több résztvevőt támogat, segít, felkészít. Online elérhető, rendelkezésre áll." A tutor munkáján belül többek között „a képzésbe bejelentkezés után a résztvevőkkel felveszi a kapcsolatot, fórumot nyit"; tanulásmódszertani tanácsokat ad; „feldolgozza, értékeli a résztvevők tevékenységét, az általuk készített anyagokat ellenőrzi, előrehaladásukat támogatja, méri fejlődésüket".

A (függelékben nem szereplő) facilitátor és az oktatásszervező feladatai meghatározásából az következik, hogy csak a jelenléti oktatáshoz, illetve vizsgához kapcsolódnak feladataik. A (függelékben nem szereplő) képzési referens feladata a jelenléti oktatás és a vizsga adminisztrálása, részvétel az elégedettség mérésében és a panaszkezelésben. Véleményem szerint a képzési referens munkájára minden munkaformában (nappali, e-learning, blended learning) tanuló képzési csoport esetében szükség van. Feladatkörét kibővíteném, és a mentori feladatokat is ő látná el. Ennek oka, hogy például minden jelenléti oktatási alkalommal ott kell lennie a szükséges adminisztráció (jelenléti ívek aláíratása, képzési napló aláíratása az oktatóval stb.) elvégzése miatt. A kurzusok során több tantárgyat is tanulhatnak a hallgatók, amelyekhez más-más előadótanár(ok), gyakorlatvezető(k), tutor(ok) tartoznak. Ezért a teljes hallgatói csoport követelményeit és benne az egyes oktatókat-hallgatókat ismerő személyre is szükség van a mentor személyében. Ennek a szereplőnek a feladatai tehát nem egyeznek meg a tanulmányi hivatali oktatásszervezőével. Ha szükséges, akkor bizonyos kérdések esetén tanulmányozza a tanulmányi és vizsgaszabályzat, illetve tanulmányi szerződés vonatkozó pontjait, és egyeztet a megfelelő hivatallal, majd tájékoztatja a hallgatókat problémás kérdésekben. Meghatározott pontokon a mentor is nyomon követheti a hallgatók előrehaladását (például az e-learning keretrendszerben feladatleadás határidejére hívhatja fel a figyelmet). Sok szempontból a közoktatás osztályfőnökére emlékeztet.

Az *V. Terembérlet* díja pontban van számba véve az oktatási helyszíntípusok díja, az oktatástechnikai eszközök bérlése és a tananyaghoz való hozzáférés költsége. A terembérlet díjat sok teremtípusra és azon belül felszereltségre adja meg az utasítás. Ezzel véleményem szerint megfelelően lefedi az oktatás színhelyeit, és minden képzés esetében kiválasztható a módszertanilag és költség szempontjából is megfelelő terem.

A tananyaghoz való hozzáférés költsége három médiumtípusra van meghatározva: papíralapúra, optikai lemezre és elektronikus tananyagra. Az elektronikus tananyagok hozzáférési költsége csak a távoktatásos formájú képzésekre szorítkozik, pedig szerintem minden képzési formában van létjogosultsága az e-tananyag szolgáltatásának, nappali, tiszta e-learning és blended learning képzés esetén is.

A keretrendszer üzemeltetési, karbantartási és hardver-, szoftverszolgáltatás bérbevételi (hostolási) költségeinek maximális díja egységnyi (45 perces) tananyagra vetítve van meghatározva, de nincs felsorolva, hogy mi minden tartozik ide.

A keretrendszer kiépítésére sem térnek ki, amely egyszeri nagy beruházás. Itt költség a szerverek és a szerverszoba, a számítógépes hálózat, az internetelérés kiépítése, vezeték nélküli hálózat kiépítése. Ezek után folyamatos költség az üzemeltetés, majd esetenként jelentkezik a fejlesztés. Operációs rendszer és alkalmazói szoftverek, beleértve az e-learning keretrendszert is, választható az ingyenes, nyílt forráskódúak közül is. Ezek mellett szükség van rendszergazdákra, akik munkaidőn túl ügyeletet adnak, hiszen egy folyamatosan képzéseket futtató intézményben az online keretrendszernek is folyamatosan (az év minden napján 24 órában) üzemelnie kell.

A rendszeradminisztrátor szerepű munkatárs külön szakterületet művel, feladatai és jogosultságai nem egyeznek meg a rendszergazdáéval. A rendszeradminisztrátor feladata, hogy beállítsa az e-learning keretrendszer tulajdonságait, kialakítsa szerkezetét (létrehozza a tantárgyi és más információkat tartalmazó mappákat, kurzusokat stb.). Ő veszi fel a

keretrendszerben a szerepeket (például oktató, tutor, referens, tananyag-szerkesztő, tantárgy/kurzus hallgatója), és ad hozzájuk jogosultságokat (például objektumok létrehozására, szerkesztésére, olvasására). Ezután felügyeli a felhasználói fiókokat (létrehozásukat a felhasználók egyéni regisztrációjával, külső azonosítással például a hallgatói tanulmányi rendszerből, vagy ő maga vesz fel felhasználókat). Végül szabályozza a jogok kiosztását a felhasználói fiókokhoz. Tehát a rendszeradminisztrátor munkaidejével is kell számolni, amely a bevezetés időszakában a legmagasabb, majd kiugró időszakok vannak új képzések indításakor és régi képzések frissítésekor; de munkájára folyamatosan szükség van.

A sikeres kurzusok költségei megfelelő kurzusszervezéssel és aktív tutorálással, mentorálással tovább csökkenthetők – erről lesz szó a következő alfejezetben.

A folyamatos tanulástámogatás eszközei blended learning esetén

A folyamatos tanulástámogatásnak kiemelt szerepe van a blended learning oktatási forma esetén. A jó színvonalon oktató intézményekbe több hallgató iratkozik be, azokat többen végzik el, ezáltal pozitív hatást gyakorolnak az intézmény blended learning oktatási formájának fejlesztésére, amint ezt már „A blended learning oktatás sikerének okai és lehetőségei" fejezetben írtam.

A lemorzsolódások elkerülése miatt és a jó vizsgateljesítményhez a kimeneti kritériumoknak kell megfelelni. Ehhez a kurzus kezdetén ismerniük kell a hallgatóknak a tananyag tematikáját, a követelményeket, hogy beszerzendő a tananyag, vagy szolgáltatják nekik. A 26/2013. (X. 21.) KIM rendelet is ezzel cseng egybe, amikor azt mondja, hogy az NKE hivatalos honlapján közzéteszi az elektronikus információs rendszer biztonságáért felelős személyek képzéseinek formáit (tantermi és e-learning) és ezek arányát, a vizsga követelményrendszerét és tananyagát.

A tananyagot ütemezni kell a felnőtt tanulók számára is, teljesítendő egységeket kell megadni (például a tanulási ütemtervben), azok végén pedig megadott időpontokra valamilyen ellenőrzést (például tesztet, dolgozatot, gyakorlati feladatot, illetve azok dokumentálását) kell kitűzni. Az *On-line képzési stratégiák és nemzetközi jó gyakorlatok a közszolgálati továbbképzések terén* tanulmányban is szó van ezekről az elemekről [16: 50-51], és a 12/2013. (III. 14.) KIM utasítás is külön foglalkozik az ellenőrzések helyével a továbbképzések folyamatában [15: XIII. ME-TK-13-1]. Irányelv lehet, hogy adjunk lehetőséget a kurzus befejezése előtt próbavizsgára, amelyen ahhoz hasonlóan mérjük a tárgyi tudást, illetve a tananyag gyakorlatbeli elsajátítását, ahogyan azt a vizsgán is tesszük majd. A hallgatóknak a tutorok egyedi visszajelzések adhatnak, így biztosítva őket, hogy követik előrehaladásukat – a tanítás-tanulás személyekhez köthető, személyre szabható.

Nem javaslom a folyamatos tanulást azzal motiválni, hogy nem érhető el egy tananyagrész, ha lejárt az arra ajánlott tanulási idő. Viszont ha a tanulási egység végi ellenőrző feladat nem mutatja a megfelelő elsajátítást, hasznos, ha a tanulónak először újra „végig kell menni" a tanulási egységen, és sikeresen teljesítenie kell az ellenőrző feladatot.

A hallgatók teljes körű és ideje korán végzett informálása csökkenti a tutorok és a mentorok munkáját (így a költségeket is), mivel a szervezésről, követelményekről nem kell a kurzusok alatt folyamatosan kommunikálniuk a hallgatókkal, megválaszolniuk az ezekkel kapcsolatos e-maileket, fórumhozzászólásokat.

A 12/2013. (III. 14.) KIM utasítás nem szól arról, hogy a jelenléti képzések tananyaga, oktatási eszközei elérhetők-e az e-learning keretrendszerből. Véleményem szerint a képzés során használt minden tananyagnak és segédletnek fenn kell lennie a keretrendszerben megfelelő logika szerint elrendezve. (Természetesen a gyakorlatok során használt tárgyi prezentációs eszközökről csak fénykép vagy a használatukról videó tehető fel.) Így a jelenléti képzésről hazatérve a hallgató újra elő tudja venni azokat, ismételhet, elmerülhet azokban, és a jelenléti képzés alatt nem fog idegeskedni a jegyzetelési tempója miatt, hanem koncentrálhat a

tanári magyarázatokra. Utóbbi megoldására az utasítás azt ajánlja, hogy a prezentáció diasorait nyomtatott formában osszák ki papíron az előadás előtt a hallgatóságnak.

Az előadások lehetnek előre videóra rögzítettek – ebben az esetben a hallgató bármikor megtekintheti azokat. Egy másik lehetőség, amely jobban biztosítja, hogy legalább egyszer, a javasolt ütemezés szerint végignézzék a videót, ha csak előre, órarendben meghirdetett időben érhető el az előadás. Bár a tanár csak virtuálisan van jelen, előre ismertetett szabályok szerint alkalmat lehet biztosítani az interaktív részvételre. Például kisebb feladatok oldhatók meg, azok automatikusan kiértékelhetők, a megoldást és a típushibákat az oktató értékelheti. Ezen kívül jól beváltak a szavazások, vélemény nyilvánítása egy-egy kérdésben.

Egy tutor valós időben egyszerre csak néhány hallgatóval tud érdemben foglalkozni interneten keresztül. A hallgatók száma kevesebb lehet még a gyakorlati órákon megszokottnál is. Ennek oka a kommunikációs közeg, illetve a használt alkalmazások, eszközök. Ha lényeges, hogy mi történik például az épp tanult program felületén, jó, ha a tanár képernyőképe át van adva minden hallgatónak, és a tanár egyszerűen át tudja venni bármelyik hallgató képernyőjét. A hallgatók is megkaphatják egymás képernyőképét, így biztosítható az együtt dolgozás is, de ez is különbözik a géptermi, egymás mellett történő tanulástól.

Az e-konzultációk a gyakorlati virtuális óráknál könnyebben kezelhetők, de itt is csak kis csoportban lehetséges mindenki aktív részvételének biztosítása. A hang- és videokonferencia-rendszerekbe egy időben belépők előre elküldhetik tutoruknak szakmai kérdéseiket, és a tutor is készülhet az előző konzultáció óta felmerült kérdések és problémák megválaszolására. A mentorok fogadóórái, az általuk tartott megbeszélések szintén kivitelezhetők ilyen módon.

A tantermi és virtuális órák között a hallgatók adminisztratív vagy szakmai kérdésekben aszinkron kommunikációs lehetőségeket is használhatnak. Ha csak őket érintő a kérdésük, akkor feltehetik e-mailben (erre az e-keretrendszerek biztosítanak belső levelezést) vagy a tantárgy internetes fórumának megfelelő témájában (amit igény esetén ők is létrehozhatnak).

Az e-learninges elemek, mint minden más elem a tanítás során, tervezetten kell, hogy felhasználásra kerüljön, szerves része kell hogy legyen a tanításnak. Minden hallgatói csoport esetén arra a bizonyos hallgatói közösségre kell alkalmazni az e-learninges elemeket. A kurzusban vannak állandó elemek (tematika, tanulási útmutató, tananyagok, kiegészítő anyagok stb.), és kellenek olyan elemek, amelyek az adott csoport számára vannak létrehozva, például tantárgyi fórum adminisztrációs és vagy szakmai kérdésekre, témákra bontva; wikipédia egy-egy terület vagy kérdés önálló/közös feldolgozásához; gyakorlatok önálló vagy projektmunkákhoz félév közben vagy vizsgán; hallgatói portfóliók.

Az e-learning keretrendszerek számos lehetőséget biztosítanak a hallgató előrehaladásának nyomon követésére. Például SCORM (Megosztható Tartalom Objektum Hivatkozási Modell) tananyag esetén listázható, hogy ki mennyi időt töltött a tananyagban (természetesen ennek egy része nem aktív tanulás volt, hiszen közben mással is foglalkozhatott), hány lapmegtekintése volt (vagyis hányszor lépett új lapra), mely lapokat tekintette meg (pontosabban melyekre kattintott). Ha ellenőrző kérdések is be vannak építve, akkor azokat milyen eredménnyel oldotta meg stb.

A mentoroknak nagy szerepe lehet abban, hogyan érzik magukat a hallgatók a kurzus közben, és hogy milyen sikerrel teljesítik a vizsgákat. Ők látják át a teljes képzést, ismernek minden oktatót és hallgatót, ezen kívül az oktatási intézmény és a képzés felépítését, szabályozóit. Ezért nagy segítségére lehetnek a hallgatóknak a többi szereplő közötti híd megteremtésében, valamint a tanulási előrehaladás követésében. Az *On-line képzési stratégiák és nemzetközi jó gyakorlatok a közszolgálati továbbképzések terén* tanulmányban [16 a diákoknak a tananyag- és felhasználói felület használatában való támogatására és a tanárokra háruló kommunikációs feladatok ellátására segítők alkalmazását javasolják. A tanulmányban egy helyen fordul elő a mentor szó [16:55], más helyeken a megnevezés online moderátor, tanársegéd, alacsonyabb bérigényű munkatárs.

A megfelelő jelenléti és internetes tanítás-tanulás aránya és az aktív internetes tutorálás, mentorálás főként a hosszabb, több féléves képzéseknél fontos, amikor a lemorzsolódásnak nagyobb valószínűsége van a kezdeti, beiratkozási utáni lelkesedés lecsengésével.

Hasznos a hallgatók számára, ha közösség alakulhat ki a kurzus során. A személyes találkozások között ez megoldható levelezőcsoporttal, fórummal az e-learning keretrendszerekben. A hallgatók egymást segíthetik: érzelmileg bátoríthatják, adminisztrációs kérdésekben informálhatják egymást, saját jegyzeteiket megoszthatják. Ezekhez az e-learning keretrendszerek számos objektumtípust biztosítanak (a csoportokban a tagok megoszthatják elérhetőségeiket, munkahelyük megnevezését, egyéb adataikat), de hosszabb képzéseken készíthetők portfóliók is saját szakmai anyagokkal, amelyekre olvasási és véleményezési jogosultsága lehet a többi csoporttagnak.

A 12/2013. (III. 14.) KIM utasítás foglalkozik a tanulási környezettel is, amelyek részét képezik a tanulást segítő vagy esetenként akadályozó személyek is: tanulócsoport, fórumozó társak, család, munkatársak. Ezek egy részére nem tud hatással lenni a tutor és a mentor, viszont „Egy oktató által jól működtetett csoportban a nagy tapasztalattal rendelkező csoporttagok egyrészt felkelthetik mások érdeklődését a téma iránt, azaz erősíthetik a motivációt, másrészt tapasztalataik megosztásával részt vehetnek a kevésbé tapasztaltak képzésében.” A hallgatók közti jó kommunikáció amellett, hogy aktív, bevonódó, elmélyültebb tanulást eredményez, hozzájárul ismét a költségcsökkenéshez, hiszen munkaidőt takarít meg a tutoroknak.

Az *On-line képzési stratégiák és nemzetközi jó gyakorlatok a közszolgálati továbbképzések terén* c. tanulmány összefoglalja az Egyesült Királyság Királyi Ügyészség esettanulmányában olvasható hasznos negatív és pozitív példákat, többek között az önálló tanulásszervezés és önértékelés folyamatát segítő mentori és tutori visszajelzéseket; a folyamatos tanulás fenntartását támogató kommunikációt. A keretrendszer megismertetésére és a hallgatók önálló tanulásra való rávezetésére, ezzel a tanári munka és költségek csökkentésére több módszertani javaslatot is adnak. A hallgatók feljebbvalóit is bevonják, részletes tájékoztatást nyújtanak nekik is a képzés személyre szabott, negyedévente frissülő célkitűzéseiről. [24]

Néhány kiemelt szempont a tananyagkészítéssel kapcsolatban

A tananyagkészítés, illetve tananyagbeszerzés minden képzés, így a blended learning bevezetésekor nagy költségekkel jár. A 12/2013. (III. 14.) KIM utasítása hat fázisra bontva, teljességre törekedve adja meg a tananyag-készítésben és aktualizálásban résztvevő szereplőket a hozzájuk tartozó tevékenységekkel és javasolt ráfordítási idejükkel.

Sajnos nem derül ki, hogy az e-learning keretrendszerben kell-e és milyen formában szerepelnie a papíralapú és a CD/DVD-kiadványok anyagainak. Az utasítás nem tér ki arra sem, hogy csak a hosszabb ideig érvényes ismereteket érdemes papír alapon publikálni. Az *On-line képzési stratégiák és nemzetközi jó gyakorlatok a közszolgálati továbbképzések terén* tanulmány célul tűzi ki a papíralapú tananyagok mielőbbi átalakítását e-learningessé. [16]

Véleményem szerint az e-learninges anyagoknak a tanulást kell támogatniuk, amelyben nem annyira a multimédiás elemek aránya, illetve a használt e-learning platform kihasználása lényeges, hanem az önálló tanulásra előkészítettség, illetve az ergonómia. Ha nincsenek szinte korlátlan források vagy idő a multimédiás, e-tananyagok elkészítésére, a megfelelő megoldás első lépésben a szakmai anyagok akadálymentesített PDF és PPT fájlként feltöltése – ezekben például könnyen válthatunk a tartalomjegyzékből a fejezetekre, külső forrásokra –. Vannak esetek, amikor idegen nyelvű tananyagok vásárolhatók, amelyeket esetleg le sem kell fordítani, figyelembe véve a hallgatók nyelvismeretét. Ellenkező esetben megjelenik költségként a szaknyelvi fordítás és lektorálás, korrektori munka, valamint a szerkesztés-tördelés. Multimédiás anyagoknál ehhez még hozzájön például a képek, animációk és videofájlok feliratainak elkészítése.

A későbbiekben, figyelembe véve az oktatási intézményben felgyülemlő tapasztalatokat, a tananyagok fokozatosan és folyamatosan fejleszthetők tovább, egyre több e-learninges elemmel bővülhetnek. Ha már működő oktatási intézményben vezetünk be blended learninget vagy e-learninget, akkor az alkalmazott módszereknek, eszközöknek illeszkednie kell a tanári kar addigi módszertanához, az intézményi know howhoz. Fontos, hogy már induláskor legyenek a teljes szervezetre érvényes, közösen elfogadott/ elfogadható irányelvek/ megvalósítandó elemek, módszerek, kurzussablonok. Vagyis ahogyan a tanulmány is javasolja, lényeges, hogy az e-learning tervezését, a tananyagfejlesztést az intézmények egyéni igényeit szem előtt tartva végezzük, vonjuk be az intézmények vezetőit és a rendszer felhasználóit is. [16]

A kész e-learninges tananyag publikálásának is vannak költségei, amelyek többségére 12/2013. (III. 14.) KIM utasítás kitér. Például a tananyag CD-n/DVD-n kiadásakor a megvásárolt optikai lemezekre az előkészített, mappákba rendezett fájlokat nem egyszerűen ki kell írni. Ezek a lemezek a használhatóságot segítendő esetleg automatikusan elindítják menüjüket, amelyből kiválaszthatók a tantárgyak/ tananyagok. Jó, ha a lemezek borítója nyomtatható, és azon megjelenik a képzést szervező intézmény logója, neve, a képzés neve, kiadás éve, a szakanyag szerzőjének és szerkesztőjének neve, kiadója és további grafika.

A webes publikálású tananyagok javítása, továbbfejlesztése esetén a lektorálás és a kiadás költsége csökken, mert csak a megfelelő fájlt vagy fájlokat kell módosítani, illetve az újakat be kell szúrni, majd a kész tananyagot mesterpéldányként archiválni. Nagyobb módosítások esetén viszont minden érintett szereplőt be kell vonni, a szakanyagkészítőtől a lektorokig. Ezek után az e-learning keretrendszerben a képzés online felületén le kell cserélni a régi tananyagot vagy tananyagelemet, segédletet a frissre. Ezt a lecserélést véleményem szerint egy ember kell végezze, és a folyamatosan foglalkoztatott oktatókat, tutorokat az ő munkájához igazodva kell értesíteni a frissítésről; az értesítést végezheti akár ő is.

Az *On-line képzési stratégiák és nemzetközi jó gyakorlatok a közszolgálati továbbképzések terén* tanulmány az online továbbképzési tartalomtípusoknak Gill szerinti csoportosítását alkalmazza. [25] [26] A tartalomtípusok segítségével felállítható a használandó keretrendszer, és ennek nyomán a képzések várható költségei mikroökönómiai szempontból is elemezhetők. Majd a tanulmány az online továbbképzési rendszerek céljainak meghatározásához Porter három stratégiai építőelemét ajánlja, amelyekhez tartalomtípusokat javasol. Ezek alapján hatékonyan meghatározható, hogy egy-egy képzőintézmény egy-egy képzéséhez milyen típusú tananyagot készítsen. Az alábbi táblázatban ezt foglaltam össze; fenn a Porteri stratégiák, lenn a Gilli főtartalomtípusok főbb jellemzői olvashatók.

Költségcsökkentési stratégia	Fókusz stratégia	Megkülönböztetés stratégia
• Az intézményen belül felszabaduló erőforrások más célokra felhasználhatók. • A tudás idővel viszonylag kevés területen változik, ezért a fejlesztéséhez és bevezetéséhez szükséges költségek több költségvetési időszakra oszthatók meg. • Az online tananyag átadása nem kíván meg jelenléti részvételt, a hallgató nem esik ki a munkából. • Országos feladatokat ellátó intézményeknek, országra kiterjedő képzéseknél javasolható.	• A továbbképzés a szervező intézmény tudásbázisára épül. • A közszféra szűkebb körében alkalmazható, amikor a specifikus tudás kihasználása a cél. • Regionális, járási, városi feladatokat ellátó kisebb közintézményeknek javasolható.	• A továbbképzésekből származó pénz jelentősebb e-learning rendszerek kidolgozására fordítható. • Valamely szakmai szempontból referenciapontnak számító közintézményeknek javasolható. • Regionális, járási, városi feladatokat ellátó kisebb közintézményeknek javasolható.

Előkészített tartalom	Támogatói tartalom	Fejlődő tartalom	Részvételi tartalom
• Újrafelhasználható. • Az oktatás alatt kevés időbefektetést igényel az oktatóktól.	• Az újrahasznosításból eredő előnyök nem jelentősek. • Viszonylag kevés időbefektetést kíván az oktatóktól.	• Újrahasznosítható. • Nagy oktatói időbefektetést igényel, különösen a továbbképzések kezdeti fázisaiban.	• Kevés újrahasznosítási lehetőség. • Folyamatosan változó tananyag a diákok kommunikációjának eredményeként. • Igen nagy online oktatói időbefektetés, kissé csökkenthető moderátorokkal.

3. táblázat. A Porteri stratégiák és a Gilli főtartalomtípusok főbb jellemzőinek összefoglalása

A megkülönböztetett fő tartalomtípusoknak két-két „altartalom-típusa" is van: 1) tantermi oktatás és továbbképzés helyettesítésére kidolgozott, valamint 2) tantermi oktatásban nem modellezhető technológiai sajátosságokat kihasználó megoldásokkal létrehozott.

Az e-learning keretrendszereket és a tananyagokat az akadálymentesség (a WCAG 2.0 irányelveinek megfelelőség) szem ellőtt tartásával kell kialakítani. Ezáltal lehetővé kell tenni, hogy az IKT-szempontból fogyatékosok és esetleges hátrányban levők ne legyenek kirekesztve a tanulásból. Az akadálymentes fejlesztéssel a költségek már rövidtávon csökkennek (csak egy változatot készítünk mindenből), azokkal hatékonyabban és magasabb elégedettségi szinten tanul mindenki, illetve minél többen vehetnek részt a továbbképzéseken, annál alacsonyabbak lesznek a képző intézmény költségei. [16] Az ergonomikus felületű keretrendszer és tananyagok gyorsabban megtanulhatók, könnyebben megjegyezhetők, a felhasználó hatékonyabban használja, kevesebb hibát vét használata során, és a vétett hibákat gyorsabban küszöböli ki – végső soron pedig elégedettebb.

A tananyagokat a széles körben elfogadott szabványrendszereknek megfelelően érdemes készíteni (például SCORM). Ezekkel biztosítható a keretrendszerek közötti átjárhatóság, valamint hogy a hallgatók legszélesebb köre használhassa változatos platformú számítógépein.

A HALLGATÓ ÉS A MUNKAVÁLLALÓ KÖLTSÉGEI

Pálosi–Varga a tanulást befektetésként értelmezi, amelyre az általános pénzügyi szabályok érvényesek. 2008-ban diszkontált értéken a felsőfokú végzettségűek 62 éves, nyugdíjas korukig 19%-kal többet kerestek. A magyarországi felsőoktatási átlagos, hagyományos, nem rendszeres kurzusok és a Gábor Dénes Főiskola kevert távoktatási kurzusainak gazdasági hatékonyságát összehasonlítva arra az eredményre jutottak, hogy a hallgatóknak több mint negyedével

kevesebbe került a képzés az utóbbi intézményben. Ugyanez az összehasonlító elemzés a nappali tagozattal szemben még nagyobb megtakarítást mutatott. Hangsúlyozták, hogy ez a jelentős gazdasági előny a tanuláshoz szükséges idő újraelosztását jelenti. A kontaktórák csökkenése az egyéni, otthoni tanulási idő radikális növekedését okozza. [27]

Nézzük most külön-külön a felmerülő költségeket, amelyeket a hallgatók azért fektetnek be, mert azt remélik, hogy megtérül a jövőben, amikor munkájukat hatékonyabban végzik majd, termelékenyebbek lesznek, vagy a jövőben egy megcélzott munkakört láthatnak el. Így magasabb fizetést, magasabb pozíciót érhetnek el, valamint kevésbé fogja fenyegetni őket a munkanélküliség. A munkáltatók reményei/elvárásai hasonlóak a hallgatókéhoz: képzettebb, hatékonyabb munkavállalót remélnek a képzések végére.

Először is, a hallgatók befektetik idejüket. További költség a kurzusdíj. Ha nem a lakóhely közvetlen közelében van a képzőintézmény, akkor az utazási díjak és idejük, sőt a kurzus szervezéséből és a lakhely távolságából adódóan szállás díja is felmerülhet. A papíralapú tananyag megvásárlása vagy internetes keretrendszerben az elektronikus tananyag használata ismét költségként jelentkezik, ha a tandíj azt nem foglalja magában.

Mindezeket a költségeket a munkáltató részben vagy teljesen átvállalhatja munkaidő-kedvezménnyel, képzési díj kifizetésével vagy normatív támogatásból finanszírozással, utazási és szállásköltség térítésével. Ha a munkáltató átvállalja a képzés költségét, szerződésben ki szokta kötni, hogy sikertelen vizsga esetén a hallgató saját költségén köteles ismétlővizsgát tenni, és a tanfolyam költségét kifizetni.

A munkáltató és a munkavállaló részéről is költség (elmaradt haszon) a munkaidő kiesése. Ezzel kell számolni a kontaktórák és vizsgák, valamint az utazás idejére. Ez a költség blended learning esetén alacsonyabb, mint csak tantermi/jelenléti képzésnél. Ha délutánonként vannak ezek az alkalmak, akkor csak fél munkanap esik ki. Ha hétvégére esnek, akkor nem terhelik a munkaidőt, de munkaidő-kedvezményt kaphat a tanuló munkavállaló.

A munka mellett (pontosabban munka utáni, szabadidő terhére történő) tanulásnak még akkor is nagyobb valószínűsége van, ha a munkatársak és a felettesek elismerik a továbbképzések/átképzések szükségességét és a tanulásba fektetett munkát. A dolgozó a munkakörében meghatározott tevékenységeket akár szinte teljes intenzitással kell, hogy ellássa a képzés alatt is. Ha munkahelyváltásra készül, akkor nem is tudatja a munkahelyi környezetével, hogy képzésben vesz részt.

Felnőtt embernél számolni kell azzal, hogy ha a képzés idejére mentesül is a munkavégzés alól, a tanulásbeli teljesítés miatti stressz hatással lesz mindennapi életére a családban és a munkahelyen.

Az otthoni tanuláshoz tiszta e-learning és blended learning esetén szükség van számítógépre, operációs rendszerre és legalább irodai szoftverekre (utóbbiak az ingyenes és nyílt forráskódúak közül is választhatók), valamint internet-kapcsolatra és internet-előfizetésre vagy mobil internetes kapcsolatra. Ezek szintén költségekként jelentkeznek, és nem valószínű, hogy a munkahely átvállalja. Előfordul, hogy a dolgozó munkahelyi munkaállomásán nem futtathatók bizonyos, a tanuláshoz hasznos alkalmazások (például szimulációk, a képzésben résztvevőkkel kapcsolattartáshoz azonnali üzenetküldő alkalmazások).

ÖSSZEGZÉS

A képzéseket a tudásátadás biztonságának fokozása, a költséghatékonyság és a tanítási-tanulási élmény miatt is blended learning formájában javaslom megvalósítani. A blended, vagyis tervszerűen „keverve” összeválogatott tanítási-tanulási módszerek és eszközök esetén a hallgatók tanulásra motiválásának, illetve előrehaladásuk ellenőrzése mellett bármelyikük, bárhol, bármikor elérheti a jelenléti órákon kívül is a képző intézmény által stratégiailag

megfelelően kifejlesztett tananyagokat, valamint kapcsolatot tud teremteni tanáraival, hallgatótársaival és az adminisztrációt lebonyolítókkal.

A képző intézmény az IKT-támogatást úgy kell, hogy alkalmazza, hogy az ne menjen a tudásátadás biztonságának rovására, valamint ki kell használnia az általa választott képzési stratégiából adódó lehetőségeket és előnyöket. A hallgatókat már a képzésről való tájékoztatás idején megfelelően kell informálni elérendő céljaikról, a rájuk váró feladatokról és az igénybe vehető lehetőségekről. A képzés elektronikus infrastruktúráját biztosító e-learning/online keretrendszer funkcióival a tanulás elején meg kell ismertetni a hallgatókat, ami által magabiztosak, önállóak lesznek, ezáltal csökkentik a jelenléti oktatókra és e-learning rendszerbeli tutorokra és a támogató mentorokra háruló kommunikációt, vagyis költségeket.

A tanítási-tanulási élmény a munka mellett és nappali, levelező, távoktatási munkaforma mellett is megfelelően magas szintű lesz, ha a résztvevők a megfelelő szakmai tartalmú, a választott és mindenki számára ismert módszerekkel és eszközökkel dolgozhatnak. Az online keretrendszerek és a tananyagok felülete ergonomikus és akadálymentes kell legyen, hogy az esetleg fogyatékossággal élő (például siket, csökkentlátó, akár ideiglenesen kézsérült, kisképernyős mobil készülékes) felhasználók is jól használhassák.

A jogszabályok és a Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézetének (VTKI) valamint Katonai Vizsgaközpontnak (KVK) a nyilvános internetes oldalait tanulmányozva úgy gondolom, hogy

- a VTKI-ben és a KVK-ban a blended learning terén folyó több éves munka nyomán felgyülemlett tapasztalatok alapján egyetemi szinten általánosan használandó elveket, módszereket és eljárásokat kellene kialakítani azokon a képzésekkel kapcsolatos területeken, ahol csak lehetséges/indokolt;
- a VTKI-ben a 26/2013. (X. 21.) KIM rendeletben meghatározott, az elektronikus információs rendszerek biztonságához kapcsolódó képzésekre a 12/2013. (III. 14.) KIM utasítás alkalmazható, eltekintve a továbbképzési programok nyilvántartásba vételétől és minősítésétől, valamint az éves tervezés folyamatától;
- a 2012. évi CLXVI. a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről törvényben meghatározott, a KOK-ban folyó képzésekhez szintén minden bizonnyal alkalmazható a 12/2013. (III. 14.) KIM utasítása, eltekintve a továbbképzési programok nyilvántartásba vételétől és minősítésétől, valamint az éves tervezés folyamatától;
- a hallgatók folyamatos tanulástámogatását és a vizsgára megfelelő felkészültséggel érkezésüket minden (rövidebb, hosszabb, iskolarendszerű és azon kívüli) képzés esetén támogatni szükséges, amely e-learning keretrendszer segítségével (például a VTKI-ben az ILIAS-szal) hatékonyan tehető meg; az alkalmazandó tanulási forma a blended learning;
- hosszabb iskolarendszeren kívüli képzéseknél pusztán e-learninges képzést nem javaslok, mert nem biztosított a tudásátadás megfelelő színvonala;
- azt javaslom, hogy az iskolarendszerű és azon kívüli képzésekben is legyen mentori feladatokat is ellátó oktatásszervező/referens; legyenek például nyomkövetési, hallgatótámogatási feladatai az ILIAS-ban;
- a kurzusok készítése során minél több lehetőségét használják ki az ILIAS-nak, például a tutorok kurzusközi kötelező feladatok megoldásain keresztül értékeljék a hallgatók előrehaladását; legyenek online fogadóórák;
- biztosítsanak lehetőségeket a hallgatói csoportok közösséggé szerveződésére az ILIAS-ban is.

Felhasznált irodalom

[1] Nemzeti Biztonsági Felügyelet honlap Jogszabályok menüpont, http://www.nbf.hu/jogszabalyok.html, látogatás napja: 2014.02.04.

[2] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról, Magyar Közlöny 40. szám, 2013. március 8., pp. 4043-4050.

[3] 2012. évi CLXVI. törvény A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről, Magyar Közlöny 154. szám, 2012.11.22., pp. 26099-26106.

[4] Security wihtin the North Atlantic Treaty Organisation (NATO) - C-M(2002)49

[5] G. K. Horváth: Közérthetően nem csak az IT biztonságról, Információ és IT biztonsági kultúra fejlesztése a közigazgatásban, KIFÜ, Budapest, 2013.

[6] 2009. évi CLV. törvény a minősített adat védelméről, Magyar Közlöny 194. szám, 2009.12., 29., pp. 47843-47866.

[7] Zs. Haig, L. Kovács: Kritikus infrastruktúrák és kritikus információs infrastruktúrák, tanulmány, Nemzeti Közszolgálati Egyetem, 2012., p. 298.

[8] 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról, Magyar Közlöny 2012. évi 19. szám, pp. 1378-1387.

[9] Nemzeti Fejlesztési Minisztérium: Digitális Megújulás Cselekvési Terv 2010–2014, Az infokommunikációs ágazat cselekvési terve a társadalom és a gazdaság megújulásáért

[10] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, Magyar Közlöny 47. szám, 2013.03.21., pp. 6338-6342.

[11] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, Magyar Közlöny 69. szám, 2013.04.25., pp. 50241- 50254.

[12] Felhívás biztonsági összekötők képzésére, Katasztrófavédelmi Oktatási Központ honlapja, http://kok.katasztrofavedelem.hu/kokportal/index.php?cid=10, látogatás napja: 2014.08.01.

[13] Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet „Továbbképzések/ Elektronikus információbiztonsági képzések” menüpont, http://vtki.uni-nke.hu/tovabbkepzes/elektronikus-informaciobiztonsagi-kepzesek, látogatás napja: 2014.02.04.

[14] Közszolgálati továbbképzési programkatalógus 2014, Nemzeti Közszolgálati Egyetem, Budapest, 2014.,, http://vtki.uni-nke.hu/srv/www/vtki.uni-nke.hu/web/downloads/Arop/vtki/Interactive_programkatalogus_170x250.pdf, látogatás napja: 2004.08.01.

[15] 12/2013. (III. 14.) KIM utasítása a közszolgálati tisztviselők továbbképzésének minőségirányítási szabályzatáról, Hivatalos Értesítő, 2013. évi 13. szám, 2013. március 14.; pp. 1853-1941.

[16] On-line képzési stratégiák és nemzetközi jó gyakorlatok a közszolgálati továbbképzések terén, ÁROP 2.2.19 Elektronikus képzési és távoktatási anyagok készítése, Nemzeti Közszolgálati Egyetem, Budapest, 2013. november 29., http://vtki.uni-nke.hu/uploads/media_items/arop-2_2_19-online-kepzesi-strategiak.original.pdf, látogatás napja: 2014.08.01.

[17] Gy. Nemes, M. Csilléry: Kutatás az atipikus tanulási formák (távoktatás/e-learning) modelljeinek kifejlesztésére célcsoportonként, a modellek bevezetésére és alkalmazására, Felnőttképzési Kutatási Füzetek 4. Nemzeti Felnőttképzési Intézet, Budapest, 2006

[18] A. Berecz, Gy. Seres: Mobilizáljuk az e-learninget, Journal of Applied Multimedia 2./VIII./2013, Neumann János Számítógép-tudományi Társaság, Multimédia az oktatásban szakosztály, ISNN: 1789-6967, pp. 49-58., http://www.jampaper.eu/Jampaper_HUN/Friss_files/JAMPAPER130202h.pdf, látogatás napja: 2014.08.01.

[19] Gy. Ágoston, A. Budai: Blended learning in Higher Education for student groups having different learning strategies. The integrated Learning Content Management System at Dennis Gabor College, Budapest, EDEN 2004 Annual Conference, 2004.06. 16–19.

[20] P. Gerő: Az élethelyzethez igazított tanulás, ZMNE, Budapest, 2008, ISBN 978 963 7060 54 0

[21] Z. Varga, D. Pálosi: A Modern Economic Approach to E-Ducation, INFORMATIKA Scinetific Review of the Dennis Gabor College, 2010., Vol. XII. No. 2., ISSN: 1419-2527. pp. 31-36.

[22] Vezető- és Továbbképzési Intézet honlapja, http://vtki.uni-nke.hu/, látogatás napja: 2014.02.04.

[23] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Vizsgaközpont - ILIAS, http://kvk.uni-nke.hu/ilias, látogatás napja: 2014.02.04.

[24] Embedded e-learning in the Crown Prosecution Service, martynsloman.co.uk, http://www.martynsloman.co.uk/casestudies/_Teecpp.pdf, látogatás napja: 2014.08.01.

[25] T. G. Gill: Distance learning strategies, part 1: a micro analysis, eLearn Magazine, 2004.08., http://elearnmag.acm.org/featured.cfm?aid=1013200, látogatás napja: 2014.08.01.

[26] T. G. Gill: Distance learning strategies: part 2. Letöltés dátuma: 2013. 11 15, forrás: eLearn Magazine, 2004.09., http://elearnmag.acm.org/archive.cfm?aid=1029486, látogatás napja: 2014.08.01.

[27] D. Palosi, Z. Varga: Comparative economic evaluation of blended learning focusing on the students'benefits. Eden 5. workshop, Párizs, 2008.10. 20–22.

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Gyebrovszki Tamás
gyebrovszki.tamas@nbsz.gov.hu

FOLYAMATOS FENYEGETÉS A KIBERTÉRBEN

Absztrakt

A cikk a kibertérben folyamatosan fennálló fejlett fenyegetésekkel (Advanced Persistent Threat továbbiakban APT) foglalkozik. A számítógépes káros kódok történetének ismertetését követően néhány ismert APT támadást sorolok fel, majd definiálom az APT fogalmát. Végezetül kitekintést adok az APT-k elleni fellépés lehetőségeiről.

This article deals with Advanced Persistent Threat in Cyber Space. It summarizes the history of malicious softwares and some known as APT attack. The article gives a definition of APT. Finally it brings solutions on the field of countermeasure.

Kulcsszavak: *APT, kibertér, rosszindulatú kódok ~ APT, cyberspace, malware*

BEVEZETÉS

Neumann János (1903-1957) matematikus nevéhez kötődik a napjainkban használt számítógép architektúra alapötlete, a tárolt programú számítógépé. A német Konrad Zuse (1901-1995) által tervezett első számítógép, a Z1 [1], programozható volt ugyan, de a programot lyukszalagon tárolta és annak programfutás közbeni változtatására nem volt lehetőség. Az 1938-ban elkészült gépről sajnos csak néhány fénykép maradt fenn. A Neumann elv alapján épült első számítógép az EDVAC (Electronic Discrete Variable Automatic Calculator) volt [2].

1. ábra. Neumann János
http://njszt.hu/sites/default/files/imagecache/belyegkep/miujsag/john-neumann.jpg

Ez a gép az adatokat és a programot is a közös memóriában tárolta. Ez ragyogó ötlet, azonban olyan problémát is okozott, amely a mai napig növekvő mértékű kárt okoz. Norbert Wiener (1894-1964) amerikai matematikus, akit a kibernetika megteremtőjének tartanak [3], az önmagát reprodukáló kód gondolatát is megalkotta. Neumann Wiener gondolatát tovább vitte. Az önmagát reprodukáló géppel foglalkozó tanulmányában leírta, hogy: „Ha valamely rendszer képes önmagát reprodukálni, akkor szükségképpen tartalmaznia kell négy komponenst: egy realizáló alrendszert (amely adott leírásokat meg tud valósítani), az egész rendszer leírását (röviden kódját), egy a kódot megőrizni, lemásolni és továbbadni képes kódátadó alrendszert, végül pedig egy az önreprodukció folyamatát vezérlő alrendszert. Ilyen alrendszerek birtokában a rendszer alkalmas arra, hogy önmagát újraalkossa.” [4], [5]

A számítógépes kártevő programok kifejlődése a Neumann-elv következtében vált lehetővé. A processzor regiszterei, a számítógép műveleti tára felülírható, a futó programjaink jól működő kódrészletei felett az irányítás átvétele lehetséges, egyfajta módosulás történik, mást is fog végezni a program, nemcsak amire programoztuk. Hasonló módon, mint ahogy a biológiában a vírusfertőzés megtörténik. A fő probléma a kibertérben azonban az, hogy ellentétben az élőlényekkel, nincs az immunrendszerrel ekvivalens fejlett önvédelmi mechanizmus, csupán védekezési módszerek léteznek. A kiberbiztonság egyre bonyolultabb eljárásokat, eszközöket és több erőforrást igényel. Mit kellene tennünk?

A SZÁMÍTÓGÉPES KÁRTEVŐ PROGRAMOK TÖRTÉNETE

Neumann bár már 1948-ban publikált és előadást is tartott az önreprodukálás gépi megvalósításáról, elméleti munkássága ezen a téren csak halálát követően, 1966-ban került kiadásra [5]. Szintén ebben az évben Robert Morris olyan játékkörnyezet megalkotását kezdeményezte, melyek egymással „harcolva" felülírva megsemmisítik a másikat. A „harci programok" első példánya a Darwin nevet kapta, ebből alakult ki a Core War [13].

2. ábra. H. R. Giger: Virus Moribundus Ante Ops Systematicae

Az elméleti alapvetés, miszerint hogyan kell önmagát reprodukáló szerkezetet tervezni és készíteni, alapvetően egy matematikai probléma megoldása, amely majdnem harminc évvel megelőzte a korát, hiszen csak 1971-ben készült olyan kód (Creeper), amely ebbe a kategóriába tartozik, az első számítógépes vírusnak tartott kód [7]. Az önmagát reprodukáló gép azonban csak jóval később, a 3D nyomtatás segítségével jöhetett létre [6].

A számítógépes vírusok széleskörű elterjedése a nyolcvanas évekre tehető. Eleinte nem a rosszindulatú szándék vezérelte a programok íróit, de kevés idő kellett ahhoz, hogy kimondottan ártó szándékkal készüljenek vírusok.

A számítógépes vírus fogalma elvont, megfoghatatlan, nehéz elképzelni. A körülöttük tapasztalható titokzatosság számos művészt ihletett meg, pl. Hansruedi Giger 2000-ben készült szobra a 2. ábrán látható. A szobor megjeleníti a megjeleníthetetlent.

Annak érdekében, hogy jobban értsük a kártékony kódok jelenlegi fejlettségét szükséges azok fejlődését áttekinteni. Ennek érdekében az alábbiakban röviden összefoglalom a kártevő programok fejlődéstörténetét évtizedenkénti szakaszokra bontva [8], [13], [14].

Hetvenes évek – az ókor

A hetvenes években csupán néhány kísérleti példány jelent meg, amelyek nagygépes környezetben működtek. Az első önreprodukáló Creeper programot Bob Thomas írta 1971-ben a BBN Technologies-nél. A DEC PDP-10-en, TENEX operációs rendszeren futó vírust tartják az elsőnek. A vírus az ARPANET-en keresztül saját másolatait helyezte el a távoli gépeken, kárt nem okozott, csupán egy üzenetet jelenített meg.

Az 1974-ben készült Rabbit a fork bomb (nyulak) első ismert példája, amely a folyamatok sorozatos duplikálódása útján a támadott gép erőforrásait felemésztve az szolgáltatás kiesését, rendszerösszeomlást okoz.

John Walker UNIVAC gépre, assembly nyelven írt Prevade és Animal vírusa 1975-ben készült. Ez az első trójai program, kárt ugyan nem okozott, mert csupán minden elérhető

könyvtárba egy-egy másolatát helyezte el. Az Animal kérdésekkel traktálta a felhasználót és ezalatt a Prevade elvégezte a másolásokat.

Nyolcvanas évek – a középkor

A mikroszámítógépeket elsőként támadó vírus az Elk Cloner volt. Az Apple II számítógépen futó programot Richard Skentra írta 1982-ben. A vírus a rendszerindításhoz használt floppylemezen a boot szektorban helyezkedett el. Ez tekinthető az első széleskörűen elterjedt vírusnak.

Frederick Cohen, amerikai informatikus 1983-ban definiálta a számítógépes vírust. Eszerint: egy program, amely képes más programok megfertőzésére oly módon, hogy saját másolatával módosítja azokat.

1986-ban a Brain bootvírus megjelenésével kezdetét vette a Microsoft operációs rendszereket fertőző kártékony szoftverek töretlen fejlődése. A vírust két pakisztáni programozó készítette.

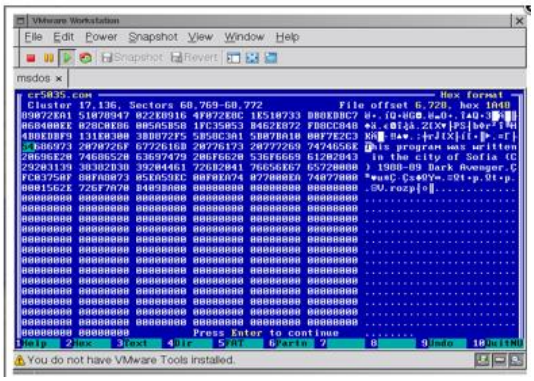
1987-ben jelent meg a Vienna, Lehigh, boot szektor vírusok: Yale, Stoned, Ping Pong. Az első önmagát rejtjelző fájlvírus a Cascade is ebben az évben jelent meg. 1987-ben készült a Jerusalem vírus, mely már 1988. május 13-án (péntek) és ezt követően péntekenként, ha az 13. napja az adott hónapnak, tönkretette az *.exe állományokat.

A Christmas Tree Exec az első levelező rendszer segítségével okozott tömeges rendszerleállást. A nem túl igényesre sikerült karaktergrafikát (3. ábra) tartalmazó üzenet lánclevélként terjedt tovább, elárasztva a postafiókokat, túlterhelést okozott a levelező kiszolgáló szervereknek, valamint jelentősen növelte a hálózati forgalmat.

3. ábra. Christmas Tree EXEC üzenet tartalma
http://securitywatch.pcmag.com/security/291931-malware-for-christmas

Az évtized utolsó éveiben egyre több és több vírus jelent meg. 1988-ban a CyberAIDS és számos változata jelent meg Apple ProDOS rendszerre. Megjelent az első Macintosh vírus a MacMag. A Score Macintosh vírus pedig komoly károkat is okozott. Az első internetes féregprogram is 1988-ban jelent meg a Robert Tappan Morris által írt Morris. A Morris DEC VAX és Sun gépeken BSD UNIX környezetben futott.

1989-ben jelent meg a Ghostball, mely többféle fertőzési módon terjedt. Egyaránt fertőzött *.exe, *com programokat és boot szektorokat is. Érzékeny felhasználói adatokat keresett és továbbított a fertőzött gépről.



4. ábra. A bolgár Dark Avangerben megtalálható szöveg
http://www.eset.hu/tamogatas/viruslabor/virusleirasok/dark_avenger-1800-c

Szintén 1989-ben készült el az első polimorf vírus, a Dark Avenger (4. ábra). Erre az évtizedre a gyors bővülés és a típusok megjelenése volt a jellemző.

Megjelentek a víruskereső módszerek és az első termékek. Az első antivírus szoftverfejlesztő céget, a német G DATA Software-t 1985-ben alapították. A számítógépes kártékony kódokkal, vírusokkal kapcsolatos fogalmak, definíciók is ebben az időszakban alakultak ki.

Kilencvenes évek – az újkor

A nyolcvanas évek tapasztalataiból származó tudást foglalta doktori értekezéssé Szegedi Imre, az Első magyar víruskönyv szerzője. Az akkor még minősített értekezés forráskód szintű elemzéseket is tartalmazott (pl. Jerusalem, Vienna, Dark Avanger).

A nyolcvanas évek végén megjelenő, mintázatalapú vírusvédelmi szoftverek kikerülésére a kilencvenes évek legelején már új módszereket kezdtek el alkalmazni a kártékony kódot fejlesztők. Ilyenek például a polimorf és a rejtjelzést alkalmazó vírusok. A DOS, majd a Windows operációs rendszereket támadó vírusok ebben az évtizedben nagyfokú fejlődésen mentek át. 1991-ben jelent meg az évtized legismertebb vírusa a Michelangelo, mely a Stoned variánsok közé tartozik. A bootszektor vírus masszív károkozása miatt vált ismertté. Michelangelo születésnapján a fertőzött gép összes adatát véletlen karakterekkel írta felül. Egyes becslések szerint tízezer esetben okozott adatvesztést.

A bootszektort fertőző Leandro and Kelly a legsikeresebben fertőző vírusok közé tartozik. A szlovák eredetű Onehalf polimorf vírus 1994-ben jelent meg. A romboló jellegű vírus minden rendszerindításkor két cilindert lekódol a merevlemez első partícióján, ha a merevlemez felével végzett, akkor jelzi azt üzenetével (5. ábra).

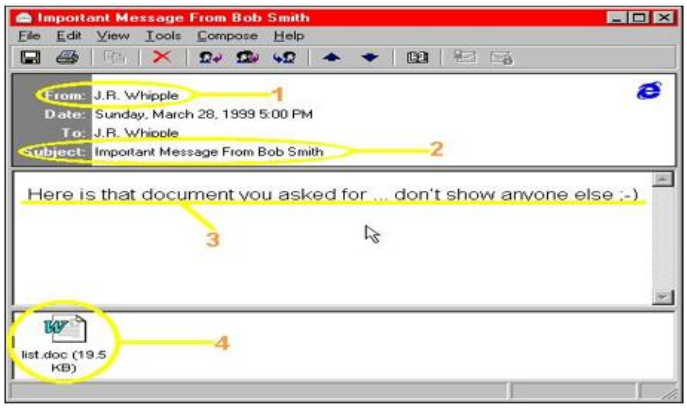
5. ábra. Már a merevlemez felét lekódolta a Onehalf
www.malware.wikia.com

A Concept az első makróvírus, 1995-ben jelent meg. A Microsoft Word programon keresztül terjedt. A Boza az első Windows 95 platformon futó vírus.

Az 1996-ban megjelent Ply kifinomult polimorf vírus, csak *.exe programokat fertőzött, azonban arra vigyázott, hogy az akkortájt ismert antivírus szoftvereket ne fertőzze meg.

A CIH vírus 1998-ban jelent meg. A fertőzési módszere lehetővé tette, hogy elrejtőzzön az antivírus szoftverek elől, mert a fertőzött fájlok méretét nem változtatta meg, azok állományaiba, az üres helyekre másolta be magát. A flash BIOS-t támadta, így okozva 250 millió dolláros kárt. A linken megtekinthető, milyen élmény lehetett elszenvedni a fertőzést (http://www.youtube.com/watch?v=RrnWFAx5vJg).

Ugyanabban az évben kezdődött a Moonlight Maze kibertámadás, amelyet az első APT támadásnak tartanak [15]. 1999-ben négy kártevőt érdemes említeni: a HAPPY99 férget, amelyik az első emailben terjedő vírus volt.



6. ábra. A Melissa fertőzött üzenete
http://www.jrwhipple.com/melissa.html

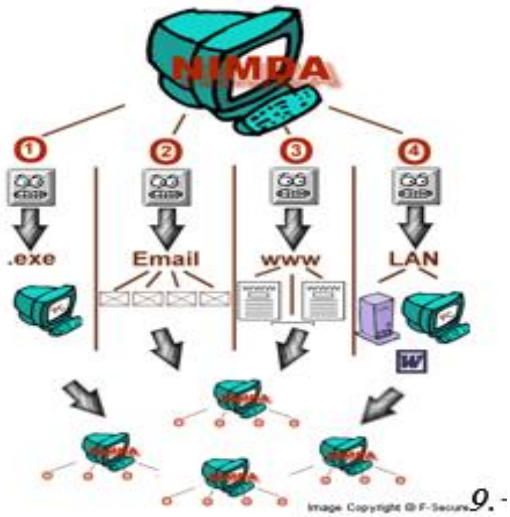
A Melissa makróvírust, mely Microsoft Word dokumentumfertőzéssel több mint 1 milliárd dollár kárt okozott. Az ExploreZip féreg hasonlóan agresszív pusztítást végzett: forráskód, valamint dokumentumfájlokat semmisített meg, míg a javascriptben megírt Kak az Outlook Express bizonyos sérülékenységét kihasználva emailekhez hozzáfűzve terjedt.

Kétezres évek – a legújabb kor

A kártékony szoftverek száma megtöbbszöröződött ebben az évtizedben. Emellett az állami szereplők (hírszerzés, elhárítás, fegyveres erők) felismerték, hogy számukra is kiaknázható eszköz jutott a birtokukba a globális kibertérben. A nem publikált sérülékenységek kihasználása útján hátsó kapuk nyithatók a rendszerekben. Több ország indította ebben az évtizedben a kiberműveleti képességeinek fejlesztését.

2000-ben az ILOVEYOU email féreg járványszerűen terjedt el világszerte. A Visual Basic Scriptben írt csatolmány (7. ábra) megnyitásával a script a Microsoft Outlook címlistája szereplő összes címzettnek továbbította a férget.

7. ábra. Az ILOVEYOU email féreg és Virtual Basic Script csatolmánya
http://2.bp.blogspot.com/-vD4Ub6pgfOM/UAP8yUfPzJI/AAAAAAAAAAc/L9obqByJDnQ/s1600/Iloveyou-virus-ver,J-1-99181-3.jpg



8. ábra. A Nimda terjedési módozatai
www.f-secure.com

Ugyanebben az évben megjelent az első gyermekeket célzó vírus a Pikachu. A futtatható állományt tartalmazó féreg, a pikachupokemon.exe csatolmány módosította az autoexec.bat állományt, melyben elhelyezett parancsok a windows és a windows\system könyvtárak törlését indította el a következő rendszerinduláskor.

2001-ben jelent meg az Anna Kournikova féreg. Hasonlóan működött az ILOVEYOU-hoz. Visual Basic Worm Generator-ral készítették. A Sadmind féreg a Sun Solaris és Windows NT/2000 operációs rendszerekben sérülékenységeket kihasználva volt képes bejutni a számítógépbe. A Deplhiben írt Sircam féreg emailen és közös hálózati meghajtókon keresztül terjedt. Károkozására példa, hogy pl. a teljes C:\ meghajtó tartalmát törölte, vagy épp teleírta a lemezt. Még 2001-ben jelent meg a CodeRed féreg, melynek egyik érdekessége az volt, hogy ha a támadott rendszer kínai nyelvre volt állítva, a féreg agresszívebben terjedt.

A Nimda vírus rendkívül gyors terjedését többféle terjedési mechanizmusa tette lehetővé (8. ábra). Kihasználta a CodeRed által létrehozott hátsó kapukat, emaileken-, fertőzött weblapokon, nyitott hálózati hozzáféréseken keresztül terjedt. 2001 végén és 2002-ben terjedt el a Klez. Az emailben fertőző féreg a Microsoft Windows, Explorer és Outlook sérülékenységeit kihasználva világszerte gyorsan elterjedt. 2003-ban a Simile metamorf vírus jelent meg. A mintegy 14000 soros assembly kódú malware kimondottan komplex, összezavart (obfuszkált) kódolást tartalmazott.

9. ábra. A Beast felülete
http://en.wikipedia.org/wiki/File:Beast_RAT_client.jpg

A Beast trójai program megjelenése is erre az évre tehető. A Remote Adminstration Tool (RAT) névvel is illetett program Windows 95 és XP operációs rendszereket fertőzött. A sikeres fertőzést követően a teljes irányítást képes volt átvenni a támadott gép felett, annak ellenére, hogy a gépet esetleg tűzfal védte. Ezt a reverse connection kapcsolódási módszerrel érte el. Széleskörű tevékenységei közé tartozott a webkamera bekapcsolása és a tárolt jelszavak megszerzése is (9. ábra).

2003-ban a Slammer féreg 30 perc alatt szinte az egész Interneten végigsöpört. A mindössze 376 bájtos malware a Microsoft SQL Server 2000 sérülékenységét kihasználva terjedt hihetetlen sebességgel. Még egy érdekesség jellemezte a Slammert és a CodeRedet is: ezek az első példányok az olyan káros kódokból, amelyek a megtámadott gép háttértárolóján nem hagytak nyomot, mert közvetlenül az operatív memóriában voltak csak megtalálhatók. Az antivírus szoftverek 2000 után kezdtek a memória átvizsgálásába, kártékony kódokat keresve. Szintén 2003-ban fedezték fel a Graybird trójait is, amelyik távoli parancsok futtatását tette lehetővé. Hasonlóképpen a török ProRAT trójai mely véletlenszerűen nyitott portokon keresztül kommunikált a támadóval. A Blaster féreg a DCOM RPC[1] puffertúlcsordulásos sérülékenységét kihasználva terjedt el és véletlenszerű IP címek felé szétküldve magát és SYN elárasztással támadta meg a windowsupdate.com-ot.

A Blasterhez hasonlóan terjedő Welchia (Nachi) féreg jóindulatú, a Blaster által is kihasznált sérülékenységet javító csomagokat töltött le és kiírtotta a Blastert. Ezután önmagával is végzett. A szintén ekkor megjelent Sobig, Swen és a Sober férgek email alapú támadásokat végeztek különféle módszerekkel, míg az Agobot féreg a botnetek alapfunkcióit[2] képes volt megvalósítani.

A Bagle féreg 2004-ben jelent meg. A tömeges levélszétküldési funkciója saját terjesztésére szolgált. A leveleket a már megfertőzött gépek (Bagle botnet ~ 150000-230000) küldték ki. Hasonló volt a MyDoom féreg, a csatolmányokban érkezett a fertőzés. Ez a féreg a leggyorsabban terjedő jelzőt kapta. A több változattal is rendelkező Netsky féreg emailbe csatolt, futtatható állományban érkezett, saját másolatait a helyi és a hálózaton elérhető könyvtárakba helyezte el. A Witty féreg új fejezetet nyitott a támadásokban. Az azonnali üzenetküldés sérülékenységét kihasználva, mintegy 12000 számítógépet fertőzött, meg csupán 45 perc alatt. A rosszindulatú kártevő a fájlrendszer lassú rombolásával okozott kárt. A Sasser féreg sérülékeny hálózati portot kihasználva terjedt. Sok rendszert le kellett állítani világszerte a féreg miatt.

10. ábra. A Caribe féreg Symbian operációs rendszeren
https://www.securelist.com/en/descriptions/old60663

1 A Distributed Computing Environment/Remote Procedure Call a Microsoft elosztott rendszerek szoftverkomponenseinek kommunikációs technológiája

2 Ez általában: a fertőzött gépen lévő „bot” frissítése, eltávolítása, parancsok és programok futtatása, portszkennelés, DDoS támadásban részvétel.

A Caribe féreg az első mobiltelefon operációs rendszert fertőző kártevő. A bluetooth-on keresztül terjedő féreg nem okozott kárt (10. ábra). A Nuclear RAT trójai program szerver és kliens gépeket is fertőzött. A fertőzött gép/rendszer felett átvette az uralmat. Még mindig 2004 terméke a Vundo trójai. A malware emailben, vagy fertőzött webhelyről fertőzött. Az alapvetően a hirdetések megjelenítésére készített malware, sokkal „több funkcióval" rendelkezett. A Bifrost trójai program távoli kódfuttatást tett lehetővé, míg, a Perlben írt Sanity az első webféreg a rendkívül gyors terjedéséről híresült el. A Google keresőszolgáltatását kihasználva a honlaprongáló 3 óra alatt mintegy 40000 honlapot fertőzött meg.

11. ábra. A Sanity féreg ezt az üzenetet jelentette meg a fertőzött honlapokon
http://www.securelist.com/en/blog?topic=199380270

A 2005-ben Farid Essebar[3] által megírt Zotob többek között pénzintézetek rendszereit fertőzte meg. A Zlob trójai program kódeknek[4], vagy kémprogram eltávolító programnak álcázva terjedt el. A Bandook Remote Administrator Tool a Beast-hez hasonlóan hátsó kaput nyitott a fertőzött számítógépen és rendszergazdai jogosultsággal érte el az erőforrásokat. Ebben az évben jelent meg az első MMS-ben terjedő féreg, a Commwarrior. A mobiltelefonos Symbian operációs rendszeren futó program bluetooth-on is terjedt. A javascriptben írt Samy a Myspace személyes oldalait fertőzte XSS[5] technikával. Szintén 2005 terméke lehet a Stuxnet [14]. A jelenleg az első bevetett kiberfegyvernek tartott APT kártevő roppant kifinomult eszközöket alkalmazott.

2006-ban jelent meg az első Mac OS X malware, mely csak a helyi hálózaton terjedt. A Blackworm (Nyxem) féreg fertőzött email csatolmányokon és nyílt hálózati erőforrásokon keresztül terjedt. A féreg a felhasználói fájlok felülírásával fejtette ki romboló hatását. A hacktivista üzeneteket megjelenítő Brontok vírus számos kellemetlen tevékenysége mellett egyszerű DOS[6] támadásokat is végrehajtott. Stration féreg fontos információnak tűnő email csatolmányban érkezett, a rendszervédelmi modulokat lekapcsolva terjedt tovább.

A Storm trójai 2007-ben söpört végig a világon. Az akár 50 millió fertőzött gépet tartalmazó Storm botnet fertőzött emailen keresztül terjedt. A botnet egyes gépei részt vettek az automatizált támadásokban, mint pl. spam-ek küldése, weblap támadása, felhasználói adatok gyűjtése. Ugyanebben az évben a Zeus trójai terjedése indult meg. Az adathalász és letöltések útján fertőző malware nagy botnetet létesített és felhasználók banki adatainak megszerzését végezte, billentyűleütések megfigyelésével.

A 2008-as Mocmex féreg digitális képkeretben érkezett. Önvédelmi modulja többek között kikapcsolta a vírusvédelmi szoftvereket, a tűzfalat, így nehezen lehetett észlelni. Cserélhető adathordozón terjedt. A Torpig trójait is 2008-ban észlelték, hasonló önvédelmi mechanizmusokkal rendelkezett. A felhasználók érzékeny adatait gyűjtő malware-t az addig ismertek legkifinomultabb bűnöző programjának titulálták. A Rustock.C változatot megelőzte a híre, a felfedezhetetlen rootkit[7] utáni hajsza majd egy évig tartott, mire 2008-ban felfedezték. A rejtve terjedő, polimorf malware, drivernek álcázva magát, hatékony önvédelmi modullal

3 Habár a marokkói-orosz állampolgárt letartóztatták, a malware további változatai jelentek meg
4 Kódoló-dekódoló szoftver
5 Cross site scripting: webes alkalmazások sérülékenységi típusa
6 Denial of Service: Szolgáltatás megtagadás
7 Adminisztrátori jogokat szerző, általában rosszindulatú célból használt szoftver

rendelkezett. A harmadik legnagyobb botnetet üzemeltető Rustock eredeti fertőzést bejuttató állományát (dropper) nem sikerült megtalálni. A Bohmini.A a távoli elérést biztosító trójai programok közé tartozik. A Facebook igénybevételével, hirdetéseket közlő hálózat segítségével terjedt el. A célpont gépen futó helyi folyamatokba injektálta a fertőző kódot, mellyel, egy távoli vezérlőszerverrel tartott kapcsolatot. A Koobface is 2008-ban jelent meg. A féreg célpontjai a Facebook, Skype és Yahoo Messenger, Twitter, Google Mail, stb. felhasználók és a bejelentkezési jelszavak megszerzése volt a fő célja. A fertőzés Facebook segítségével történt. A mai napig aktív Conficker vírus is 2008 „terméke". A világszerte elterjedt féreg a számítógépek millióit fertőzte meg az operációs rendszer hibáját kombinálva a szótáralapú jelszópróbálgatás módszerével. A legkiterjedtebb botnetet a Conficker valósította meg. A fennálló fertőzések a kiadott szoftverfrissítések mellőzése és a vírus fejlődése miatt maradt fenn.

2009-ben az email csatolmányban érkező Dozer miután a biztonsági modulokat leállította, DDoS támadásokat végzett az Egyesült Államok és Dél-Korea irányában. A Daprosy féreg a helyi hálózaton, USB meghajtókon, és spamekben terjedt. A főként a billentyűzet leütéseket kifürkésző malware-t a kétezres évek legveszélyesebbek fenyegetései közé sorolják. A kétezres évek második felében olyan kártevő változatok, módszerek (távoli elérés, kifinomult fertőzési vektorok, vírusvédelem kikapcsolása, stb.) jelentek meg, amelyek egyre hatékonyabban rejtették el tevékenységüket. Megjelentek a célzott támadásra alkalmas módszerek, amelyek vonzók lettek a különféle országok állami szereplőinek. Az első kiberfegyver is megjelent, a Stuxnet. Bizonyára több olyan eset is van, amelyek nem kaptak nyilvánosságot.

Kétezer-tízes évek – az APT kor

A kétezer-tízes évek tovább bonyolították a kibertérben folyó védelmi tevékenységet. Amellett, hogy a kiberbűnözés kimondottan megerősödött[8], az állami szereplők is alaposan kivették a részüket a támadásokban. A következő országokról jelentek meg kiberképességeiről információk a tömegmédiában konkrét példák nélkül: Egyesült Államok, Egyesült Királyság, Orosz Föderáció, Észak-Korea, Irán, Kínai Népköztársaság, Szíria, Franciaország.

12. ábra. Az NSA globális APT képessége
https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/

8 Az NSA becslése szerint 250 Mrd USD a kiberbűnözés által okozott kár világszerte (forrás: http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion)

Megnevezés	Támadás észlelése	Valószínűsített támadó	Támadott	Tevékenység
Moonlight Maze	1998	Oroszország	USA Pentagon, NASA stb.	Több tízezer dokumentumot szereztek meg
Titan Rain	2003	Kína	USA	Nem
Stuxnet	2005	USA-Izrael	Irán + kb. 10 ország	Irán urándúsító kapacitásának visszafogása
US Congressmen	2006	?	USA	Kínai disszidensekről szóló iratok megszerzése
Shady RAT	2006	Kína	USA, Kanada, Ensz + 3 ország,	Dokumentumok megszerzése
NIPRNET, SIPRNET támadás	2008	Oroszország	USA	Dokumentumok megszerzése
Red October	2008	Oroszország	Több ország külügyminisztériuma	Adatszerzés
GhostNet	2009	Kína	103 ország	Adatszerzés
Operation Aurora	2009	Kína	USA	Forráskódok elérése, módosítása
Night Dragon	2009	Kína	Energia szektorbeli cégek világszerte	Adatszerzés
Ke3chang	2010	Kína	Több ország külügyminisztériuma	Adatszerzés
Duqu	2011	N.A.	Irán + több ország ipari számítógépe	Adatszerzés
Icefog	2011	N.A.	Dél-Korea, Japán, Kína + 12 ország	Adatszerzés
Teamspy	2012	N.A.	Több ország külügyminisztériuma	Adatszerzés
Flame	2012	USA	Közel Kelet országai	Adatszerzés
Miniduke	2013	Ukrajna	Több ország	Adatszerzés
Kimsuky	2013	Észak Korea	Dél-Korea, Kína	Adatszerzés
Careto	2013	Spanyol nyelvű	31 ország	Adatszerzés
Dragonfly	2013	?	Ipari rendszerek világszerte	Szabotázs, adatszerzés
Snake/Uroburos	2014	Oroszország	Kb. 50 ország	Adatszerzés

1. táblázat. Áttekintő táblázat [15]

Az elmúlt néhány évben egyre több APT besorolású kampány került a nyilvánosságra (1. táblázat). A vélhetően spanyol Careto 31 országot érintett, több platformon is (okostelefonon) működik, szisztematikusan gyűjtötte a szenzitív adatokat, pl. a titkosítási kulcsokat. A Snake/Uroburos valószínűleg orosz kémszoftver. A Ke3Chang vélhetően kínai kémszoftver. Az amerikai NSA 2004 óta fejleszti kiberműveleti hacker képességeit. A Turbine (lásd 13. ábra) fedőnevű intelligens rendszere lehetővé teszi a számítógépes hálózatok támadását százezres nagyságrendben [11]. Az Egyesült Királyság elsőként ismerte el [12], hogy fejleszti mindenoldalú katonai kiberképességeit, mely csapásmérő erőt is tartalmaz.

Az ismertté vált esetek némelyike nagy publicitást kapott, míg másokról kevés információ került napvilágra. Az APT szerű támadások megjelenése óta folyamatosan bővültek, finomodtak a módszerek. A sérülékenységek kihasználásának két válfaját alkalmazzák már a kezdetektől: az ismert illetve a még nem ismerteket. A támadások célzott jellege miatt nagy különbségeket láthatunk az egyes APT-k között. A célpont rendszereibe való behatolás módszere eleinte a fizikai hozzáférés volt. Elsősorban hordozható média közvetlen csatlakozása és a fertőzés kivitelezése dominált azokban az esetekben, ahol erre lehetőség adódott. A közvetlen támadásokban az internetes kapcsolattal rendelkező erőforrások nyitott portjainak letapogatása távoli bejelentkezési kísérletek útján történő bejutás is elterjedt módszer. A

támadások egy részében a célpontra szabott becsapós emailek küldése volt a legelterjedtebb az elmúlt években. Az email káros kódot tartalmazó weblapra mutat, az áldozat a linkre kattintva fertőződik, vagy a csatolmányban küldenek a részükre olyan futtatható állományt, ami dokumentumnak „látszik". A csatolmány „megnyitása" általában egy hamis tartalmú dokumentum megjelenítésén túl elvégzi a rendszer fertőzését, vagy csupán egy fertőzést okozó káros kód fut le.

Legújabban az úgynevezett watering hole támadások kerültek az előtérbe. Az elmúlt években egyre nagyobb számban láthatunk az eddigieknél kifinomultabb módszereket. A támadás első lépcsőjeként olyan legális (kihasználható sérülékenységet tartalmazó) weblapokat változtat meg a támadó, amelyet a célpontjai látogatnak. A változtatás lényege olyan iframe keret elhelyezése, mely rejtett átirányítást tartalmaz. Az átirányítás egy olyan domainre mutat, amit a támadó hozott létre, vagy fertőzött meg és menedzsel. Az átirányított áldozatról adatgyűjtést (fingerprinting) végez a támadó és ha az áldozat értékes és kihasználható sérülékenységet tartalmazó szoftvere van, akkor további átirányítás történik a már káros kódot tartalmazó domainre. Ekkor történik meg a tényleges fertőzés, míg a támadás első két fázisát víruskeresőkkel lehetetlen megtalálni, ugyanis az átirányítások, a telepített pluginek feltérképezése legális műveleteknek számítanak. A fertőzés további lépcsőket is tartalmazhat, például a kezdeti távoli elérést biztosító eszközt lehet frissíteni.

NÉHÁNY APT KAMPÁNY ISMERTETÉSE

Dragonfly [17]

A Dragonfly jelenleg az energiaszektorban működő vállalati rendszereket támadja. A támadó eszközei a Backdoor.Oldrea és a Trojan.Karagany-t. A célpontok között energiaszolgáltató, csővezeték üzemeltető, energiaipari vezérlőrendszer berendezésgyártók is voltak. Az áldozatok Spanyolországban, az USA-ban, Franciaországban, Olaszországban, Németországban, Törökországban, Lengyelországban, Romániában, Görögországban és Szerbiában voltak a legnagyobb számban. A Dragonfly APT támadói technikailag jól képzettek, és stratégiai gondolkodásra képesek. A csoport minden esetben kisebb, kevésbé védett beszállító támadásával jut a célpont közelébe.

A Symantec szakértői a támadás három lépcsőjét írták le. Az elsőben adathalász emailben malware-t tartalmazó csatolmányt küldenek a célpontnak. A másodikban a levelek címzettjeit exploit-okat tartalmazó weboldalakra vezetik. A harmadikban közvetlenül az ipari vezérlőrendszereket előállítót támadják meg, így a malware-eket még a gyárban, eladás előtt elhelyezik a szoftverekben. Ez esetben a fertőzést maga a cég végzi el a telepítésekor. A feltételezett támadó székhelye valószínűleg Kelet-Európa. A Dragonfly hasonló motivációval rendelkezik mint a Stuxnet, de adatszerzést is végez.

Uroburos[18]

A különösen kifimomult APT támadást a G DATA németországi cég hozta nyilvánosságra és a káros kódban szereplő sztring alapján kapta a nevét (lásd a kódrészlet alább).

```
80 FA FF FF D4 CB B9 09 80 FA FF FF 54 C6 B9 09  ............T...

80 FA FF FF 00 00 00 00 55 72 30 62 55 72 28 29  ........Ur0bUr()

73 47 6F 54 79 4F 75 23 00 00 00 00 00 00 00 00  sGoTyOu#........
```

Az APT tevékenységt 2011-ig vezették vissza, így a felfedezés előtt már 3 éve aktív volt. A G-Data szakemberei szerint úgy gondolják, hogy hírszerző ügynökséggel hozható összefüggésbe a támadás, vélhetően több még fel nem fedezett változat is lehet. Az Uroburos egy rootkit, amely két fájlból, egy driver-ből és egy rejtjelzett virtuális fájlrendszerből tevődik

össze. A támadó átveszi az uralmat a megfertőzött számítógép felett, bármilyen programkódot futtathat a gépen, és önvédelmi moduljának segítségével képes rejteni tevékenységét. Az Uroburos adatokat szerez és a hálózati forgalom elfogására is képes. Több víruskutató szerint kapcsolat lehet az Uroburos és egy korábbi APT támadás között, amelyet korábban az amerikai kormányzati szervek ellen használtak. Alább egy példa látható a támadó tevékenységének hálózatból vett mintázatára (a http biztonsági okokból cserélve hxxp-re).

„http GET hxxp://eu-sciffi.99k.org/B/3/6530475040”

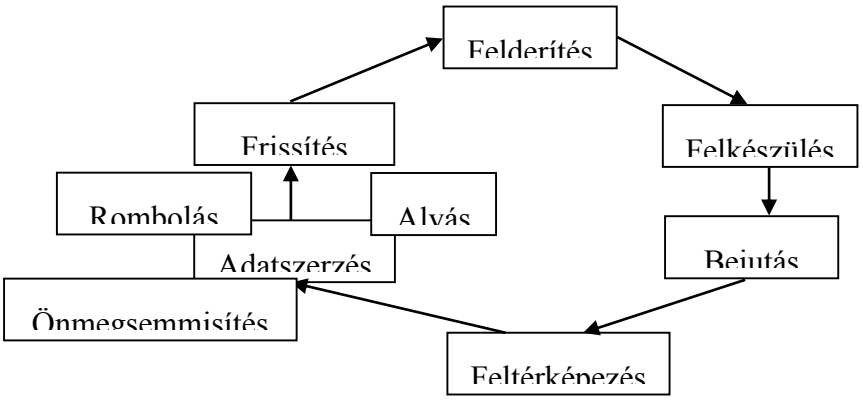
AZ APT TÁMADÁSOK ELLENI VÉDEKEZÉS LEHETŐSÉGEI

Ebben a részben vázlatosan összefoglalom a védekezés lehetőségeit. Elsőként definiálom az APT-t, majd az APT támadás ciklusát mutatom be, végül számba veszem a védekezés módozatait.

Az Advanced Persistent Threat (APT) – Folyamatosan Fennálló Fejlett Fenyegetés (4F) definíciója

Informatikai rendszerekbe észrevétlenül, célzott módon, adatszerzés és/vagy rombolás céljából bejuttatott különleges képességű folyamatok, melyek külső kapcsolat segítségével, távolról kiadott vezérlőparancsok végrehajtásával folyamatosan működve fejtik ki jogszerűtlen tevékenységüket (saját definíció).

Az APT életciklusa, funkciói



13. ábra. Az APT támadás alapsémája, funkciók

Az APT kifejezés 2005 körül jelent meg, annak érdekében, hogy a figyelmet ráirányítsa erre a jelenségre. Nem új típusú kártevő kódcsaládról volt szó akkoriban sem, hiszen az APT első része felfogható egy trójai programnak, a bejuttatott távoli elérést biztosító szoftver pedig egy Remote Access Tool-nak a vezérléstől függően bármilyen tevékenységet végezhet. Az, hogy mégis külön kategóriába kell sorolni az APT támadásokat azért van, mert az első támadások felfedezése idején precedens nélküli volt az ily mértékben körültekintő óvatossággal megtervezett és kivitelezett támadás és információszerzés. Az APT általában nem feltétlenül alkalmaz újabb technológiákat, hanem több fokozatban, egymásra épülő, gondosan kivitelezett lépések megtételével éri el a célját. Az első fokozatban az áldozat rendszerének gyenge pontjainak felderítése, feltérképezése a cél. Ezt követően kerül kidolgozásra a célzott támadás terve, mely meghatározza a rendszerbe bejutás módszerét, egy, vagy több kihasználható sérülékenység útján, majd létrehozásra kerül a támadó infrastruktúra, a vezérlőszerverek, a

támadási vektor végrehajtásának minden eleme. Ezek magukba foglalják szoftverelemek kifejlesztését, domain nevek regisztrációját, hardver elemek biztosítását, a célzott támadáshoz szükséges dokumentumok, emailek stb. elkészítését. A támadás kezdeti szakasza a rendszerbe való bejutást célozza. Még mindig a legelterjedtebb módszer az áldozat rendszerébe való bejutásra a megtévesztő email küldése, vagy egy fertőzött pendrive csatlakoztatása a célpont rendszeréhez.

Email támadási vektor esetén az email tárgya és a feladó email címe úgy kerül megválasztásra, hogy az felkeltse a felhasználó érdeklődését és így a levél nagy valószínűséggel megnyitásra, elolvasásra kerül. A levél tartalma gondosan megtervezett megtévesztés. A károkozó töltetét több formában tartalmazhatja. A levél törzse közvetlenül tartalmazhat károkozó kódot bejuttató hivatkozást, amely egy internetkapcsolattal rendelkező gépre a hivatkozás megnyitását követően letöltődhet. Másik lehetőség az email csatolmány. A különlegesen elkészített csatolmány szintén a megtévesztést szolgálja, valójában a fertőzést előidéző futtatható kódok kerülnek végrehajtásra a csatolmány megnyitását követően. A fertőzés kezdeti lépését követően a rendszerbe bejutott modul kapcsolatot létesít az APT támadás egyik vezérlőszerverével. A szerverről további modul(ok) kerülhetnek letöltésre, majd megindul a gép és a környezetének feltérképezése. A roppant kifinomult technikákat alkalmazó APT lopakodva, folyamatosan figyelheti a hálózaton elérhető szolgáltatásokat, dokumentumokat, kulcsokat, jelszavakat gyűjthet, de akár rombolást is végrehajthat. Általában önvédelmi és önmegsemmisítő modullal is rendelkezik, mely megnehezíti a hatásmechanizmusuk, céljuk, eredetük, tevékenységük felfedését.

Nagy valószínűséggel olyan állami szereplők állhatnak az APT kampányok mögött, mint pl. az ellenérdekelt hírszerző szolgálatok, fegyveres erők.

VÉDEKEZÉSI MÓDSZEREK

Az APT támadásokat legjobb megelőzni. A prevenciót a komplex biztonsági rendszer lehetőségeinek kihasználása segíti elő. Egy jól megtervezett és kivitelezett kiberbiztonsági rendszer is lehet hatástalan, ha a funkcióit nem használják.

Az információ biztonságot több szabványban (ISO 27000 szabványcsalád, ISO 15408, COBIT), valamint a 77/2013. NFM rendeletben megtalálható módon szükséges egyenszilárd módon biztosítani. A védelem adminisztratív, fizikai, humán és technikai aspektusairól a védelmet igénylőnek kell dönteni, az erőforrásokat kiválasztani. A döntés nem egyszerű, alapja a kockázatelemzés. Az alapvetően adminisztratív intézkedések betartása a biztonsági tudatosságon alapul, a szabályok figyelmen kívül hagyása a védelem képességeinek leromlásával jár. Ennek érdekében a felhasználók, üzemeltetők és a vezetők rendszeres biztonsági tudatossági képzése az alap. Szükséges kidolgozni az informatikai biztonsági szabályzatokat, ellenőrizni azok végrehajtását. Ennek keretében a jogosultságkezelés helyes menedzselése, a fizikai hozzáférés korlátozása mellett a megfelelő autentikációs rendszer alkalmazása is nagyon fontos. Szintén fontos a helyes jelszókezelési házirend bevezetése, mely megnehezíti a fiókok jogosulatlan elérését. A felhasználói tevékenység biztonságosabbá tétele, az erős jelszavak alkalmazása, azok gyakori megváltoztatása, bármilyen meglepő is a legolcsóbb, de egyben az egyik legfontosabb eleme a prevenciónak. Fontos a pendrive használat szabályozása, valamint a magántulajdonban lévő eszközök használatának menedzselése, vagy tiltása (BYOD)[9].

Nagyon lényeges a biztonság szempontjából, hogy a szoftverfrissítések lehető leghamarabb megtörténjenek. Az ismertté vált sérülékenységek kihasználhatósága ezáltal kiküszöbölhető. Nagyobb a veszély a 0-napi sérülékenységekkel kapcsolatban, ugyanis ezeket vagy még nem

9 Bring Your Own Device: Csatlakozz a sajátoddal lehetőség

ismerjük, vagy nincsen rendelkezésre álló szoftverjavítás. Ez utóbbi esetben korlátozni kell a sérülékeny szoftver használatát. Ha viszont nem ismeretes a sérülékenység, akkor az nem ismert mértékű kockázatot jelent. A prevenció technikai lehetőségei az ismert mintázatokra vonatkozóan széleskörűen rendelkezésre áll. Nem ez a helyzet az APT támadásokra.

Amennyiben egy APT támadásról partnereinktől tájékoztatást kapunk, akkor azok technikai adatait (vonatkozó IP címek, domain nevek, stb.) a határvédelmi rendszerekben felhasználhatjuk, ennek hiányában azonban nehézségbe ütközünk, mert ismeretlen mintázatú támadásra a behatolásjelző rendszerek, antivírus alkalmazások haszontalanok. A prevenció korlátai itt jelentkeznek. Az APT támadások többnyire áldozatspecifikusak, így technikai adatok korlátozottan állnak rendelkezésre. Ismeret hiányában szükségünk lenne más módszerekre is.

Az APT-k elleni védekezésben jelenleg már több termék van a piacon bár azok árfekvése meglehetősen magas. A Cisco, TrendMicro, Sourcefire és a FireEye rendelkeznek már ilyen megoldással. A védelem lehetséges eszközei ezek mellett az alábbiak.

Az ismert támadásokban elfogott káros kódok pl. hash azonosítóinak vagy hálózati forgalmi mintázatoknak keresésén alapuló módszernek a célzott támadásokban nem elégséges a használata, azonban a védelem még jelenleg is fontos eleme. Idő- és erőforrásigénye egyre nagyobb.

A hálózaton folyó forgalom valósidejű figyelésének számos előnye van. Ezek közül például a behatolásjelző/behatolásvédelmi (IDS/IPS) rendszerek az ismertté vált támadások ellen hatékonyak. A csomagszintű vizsgálat is szóba jön, mint védekezési módszer.

A hálózati anomáliák, vagyis a szokásostól eltérő forgalmi adatok vizsgálata is célravezető lehet egyes ismeretlen támadásokban.

A naplóállományok gyűjtése és elemzése nagyon fontos a támadások felismerésében. A DNS kérések naplózása és elemzése úgyszintén lehetséges.

A fekete- és fehérlisták alkalmazása a tiltandó és az engedélyezendő kapcsolódásokra megoldást jelent, de rendszeres karbantartásigénye merevvé teszi ezt a megoldást.

A futtatható állományok ellenőrzése emulált környezetben képes lehet a káros viselkedés felismerésére. Ilyen például a Cuckoo Sandbox. A káros kódot tartalmazó csatolt fájlok bejuttatása ellen a csomagszintű vizsgálatok jelenthetnek megoldást. A virtuális környezetet kialakító sandboxing technika szimulált környezetben „szabadjára engedi” a vizsgált gyanús objektumokat, viselkedésvizsgálatot végezve. Ez korszerű megközelítés bár egyes támadások védekeznek a sandbox technika ellen és nem árulják el magukat, amennyiben észlelik a sandbox-ban futást.

A különféle csapdák alkalmazása is megoldást kínál az ismeretlen támadások felismerésében. Ennél a megoldásnál például egy áldozati gépet helyezünk el a hálózaton, amelynek szándékosan gyenge védelmi megoldásai vannak. A megfertőződést pedig figyelemmel kísérjük és a támadás adatait felhasználjuk a védelemben.

Lehetőség van továbbá a viselkedési anomáliák vizsgálatára. Az ilyen jellegű termékek a megnövekedett CPU terhelés, szokatlan mennyiségű és idejű aktivitás, nem ismert folyamatok futása, folyamatváltások számának növekedése, új rendszerprogram-szálak megjelenése, egyéb események észlelése útján adhatnak riasztást.

A felsorolt módszerek hatékony alkalmazásához jól képzett szakszemélyzet szükséges. Összességében a megelőzés során a gyanús emailek, a rendszeranomáliák kivizsgálása, az ismert fájltípusokba beágyazott futtatható kódok keresése, valamint a gyanús külső hálózati kapcsolódások vizsgálata áll az eszköztárunkban rendelkezésre, azonban a csomagszintű szűrés és vizsgálatok a sandboxing technika megoldások is ígéretes hatékonysággal segítik az APT támadások elleni fellépést.

Figyelembe véve, hogy az APT támadások fő célpontjai világszerte kormányzati intézmények, tudományos intézetek, illetve kritikus infrastruktúrák üzemeltetői, szükséges

ezen a téren a védelem erősítése és megfelelő kiberbiztonsági menedzsment kialakítása, a képzett szakemberek rendelkezésre állása.

ÖSSZEFOGLALÁS

A kártékony kódok 43 éves történelmük során a számítástechnikával párhuzamosan fejlődtek. A Neumann elvű számítógép architektúra sajnos sikertörténet a számítógépes vírusok számára is.

A kilencvenes években indult meg a víruskeresők és vírusírók ma sem lankadó küzdelme a vírusirtás és a vírusok elrejtőzése területén. Napjainkban már nem elég a víruskereső programok használata, hanem több, egymást kiegészítő módszer kell a hatékonyabb védelem kialakítására.

A kiberbűnözés térnyerése és az APT támadások megjelenése a kétezres éveket jellemezte. A védelem szereplői új módszereket kénytelenek alkalmazni, egyre növekvő költséggel. A folyamatos fenyegetések a kibertérben, a kifinomult APT támadások elleni védelem jelenleg ismert módszerei nem örökérvényű megoldások. Elsősorban az egymásra épülő, rutinfeladatok fegyelmezett végrehajtása, úgymint például a biztonságtudatos eszközhasználat, a szabályok betartása, a különféle viselkedésalapú vizsgálatok, a naplóállományok elemzése növeli a rendszereink védettségét. A kifinomultabb módszerek, mint a csomagszintű vizsgálat, vagy a sandboxing, esetleg a csapdarendszerek alkalmazása tovább javíthatja a védettséget.

Az adminisztratív-, fizikai-, logikai védelmi elemeket az információs rendszerek védelme érdekében a kockázatokkal arányosan kell kialakítani a jogszabályoknak megfelelően.

Nem hagyhatjuk figyelmen kívül a felhasználók és a vezetők felelősségét sem. A legkiválóbban megtervezett rendszer sem hatékony, ha nincs érvényesítve valamely eleme. A támadók a leggyengébb ponton fognak támadni, ugyanis folyamatosan keresik a támadási pontokat.

A védelem továbbfejlesztésének lehetősége az APT támadások teljes körű megértése, a védelem adaptivitása és a reagálási sebesség növelése, proaktív mellett a kiberképességek módszertanának további kutatásában rejlik.

Felhasznált irodalom:

[1] Konrad Zuse Internet Archive (letöltve: 2013.07.07.) http://zuse.zib.de/

[2] http://ttk.pte.hu/ami/phare/tortenet/EDVAC.html (letöltve: 2014.03.16.)

[3] http://www.livinginternet.com/i/ii_wiener.htm (letöltve: 2014.03.16.)

[4] Bakacsi Géza, Csákány Béla: Egy szegedi néptanító emlékezete Ponticulus Hungaricus XIV. évfolyam 7—8. szám 2010. július—augusztus http://members.iif.hu/visontay/ponticulus/rovatok/limes/gaspar_dezso_elete.html (letöltve: 2014.03.16.)

[5] Neumann János: Az önmagát reprodukáló automata elmélete (Theory of Self-Reproducing Automata) 1966 University of Illinois Press Urbana and London http://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf (letöltve: 2014.03.16.)

[6] http://www.mernokbazis.hu/cikkek/egy-gep-ami-onmagat-masolja (letöltve: 2014.03.16.)

[7] Bevezetés az élet játékaiba http://www.szak.hu/konyvek_htm/sample_chapters/artofvirus/chap1.pdf (letöltve: 2014.03.16.)

[8] Timeline of computer viruses and worms http://virus.wikia.com/wiki/Timeline_of_noteworthy_computer_viruses,_worms_and_Trojan_horses (letöltve: 2014.03.23.)

[9] Pintér Róbert: A vírusok és azok fajtái http://artefaktum.hu/oktatashoz/internet05tav/06_biztonsag/virus_Hardwer_OC_attekintes.doc (letöltve: 2014.03.23.)

[10] Szegedi Imre: Személyi számítógépes vírusok elterjedésének veszélyei és az ellenük való védelem a Magyar Honvédségben Első magyar víruskönyv Egyetemi doktori értekezés Budapest, 1990 http://uni-nke.hu/downloads/konyvtar/digitgy/doktori/egyetemi/Szegedi_Imre.pdf (letöltve: 2014.03.23.)

[11] Ryan Gallagher, Glenn Greenwald: How the NSA Plans to Infect 'Millions' of Computers with Malware, 2014.03.12. The Intercept https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/ (letöltve: 2014.03.23.)

[12] James Blitz: UK becomes first to admit offensive cyber attack capability Politics & Policy, 2013. 09.29. http://www.ft.com/intl/cms/s/0/9ac6ede6-28fd-11e3-ab62-00144feab7de.html#axzz2wra94jkt (letöltve: 2014.03.23.)

[13] Szőr Péter: A vírusvédelem története Szak Kiadó 2010.

[14] Gyebrovszki Tamás: Stuxnet - mint az első alkalmazott kiberfegyver - a Tallinni Kézikönyv szabályrendszere szempontjából Hadmérnök, 2014/1 164.-174. oldal

[15] Advanced Persistent Threats: A Decade in Review 2011. http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf (letöltve: 2014.04.12)

[16] http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf (letöltve: 2014.04.13.)

[17] http://www.cert-hungary.hu/node/259 (letöltve 2014.07.23.)

[18] http://www.cert-hungary.hu/node/237 (letöltve 2014.07.23.)

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Györkös Roland István - Nagyné Takács Veronika
kh.ifuf@nav.gov.hu

JAVASLAT AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK 77/2013. (XII. 19.) NFM RENDELET ALAPJÁN ELVÉGZENDŐ BIZTONSÁGI OSZTÁLYBA SOROLÁSA VONATKOZÁSÁBAN

Absztrakt

A közigazgatási szervek számára jelentős feladatokat határoz meg a 2013-ban hatályba lépett új, informatikai biztonsági tárgyú jogi szabályozás, Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény és annak végrehajtási illetve technikai rendeletei. A jogalkotói szándék az informatikai rendszereket használó szervezetek tudatos – tervezett és ellenőrzött – információvédelmi tevékenységének előmozdítása, részben értékelési, tervezési és tényleges információvédelmi feladatok előírásával, részben a feladatok ellátását ellenőrző, koordináló szervezetrendszer létrehozásával. A jogszabályoknak való megfelelés első lépése az alkalmazott informatikai rendszerekkel kapcsolatos helyzetfelmérés, ezt követheti a felmérés eredményei alapján szükséges intézkedések meghatározása és végrehajtása. A jogalkotói elvárás egyértelmű, a végrehajtás módját az érintett szervezeteknek kell egyedileg meghatározniuk. A szerzők a feladatot a Nemzeti Adó- és Vámhivatal szempontjából tekintik át és tesznek javaslatot az első szakaszban meghatározott elvárások teljesítésére.

The new information security Law was issued in the beginning of 2013. This Law and its implementing technical regulations define major tasks for the State or local government agencies in the field of security of electronic information. The main aims of the new law were to enhance the information security activities and provide assessment, planning and effective information management tasks, partially exercising control due the establishment of a coordinating body system. The first step is a survey of regulatory compliance status of the used IT systems, and may be followed by the definition and implementation of the necessary measures based on the results of the survey. The legislative requirements are absolutely clear: the measures have to be determined by the individual organizations. The authors of this study focuse on the tasks and the fulfillments of the National Tax and Customs Administration in the first phase.

Kulcsszavak: *információbiztonság, kockázatelemzés, közfeladatot ellátó szervek adatai ~ information security, security risk management, public sector information*

ELMÉLETI ALAPVETÉS

Az informatikai biztonságra vonatkozó jogi szabályozás 2012 óta zajló megújításának célja - *Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló* 2013. évi L. törvény (a továbbiakban: Ibtv.) indokolása szerint - egy „preventív szabályozási környezet" létrehozása, amely „ténylegesen a megelőzést helyezi előtérbe és ezen keresztül a biztonsági problémák kialakulásának mérséklését és az előforduló biztonsági események számának csökkentését, illetve tudatos kezelését célozza". [1]

A *megelőzés* és a *tudatos kezelés* alapja minden esetben egy teljes körű és korrekt helyzetfelmérés kell, hogy legyen, amely első lépésként a tevékenységgel érintett *vagyontárgyak* számbavételére, második lépésként a *végrehajtandó intézkedések* meghatározására irányul.

Az Ibtv. szerint két kiindulópont van: az *elektronikus információs rendszerek biztonsági osztályba sorolása*, illetve az *elektronikus információs rendszerrel rendelkező szervezetek biztonsági szintjének meghatározása*. Az előbbi a vagyonleltár felvételét és a vagyontárgyak minősítését, az utóbbi a szervezet biztonsági feladatokra való felkészültségének meghatározott szempontok szerinti mérését és az esetleges hiányosságok (a továbbiakban: megteendő intézkedések) azonosítását jelenti az irányadónak tekintett szabványok alapján (lásd később).

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 77/2013. (XII. 19.) NFM rendelet (a továbbiakban: technológiai rendelet) 1. sz. mellékletének 1.2. pontja szerint *az elektronikus információs rendszerek biztonsági osztályba sorolását kockázatelemzés alapján kell elvégezni, amit az érintett szervezet vezetője hagy jóvá. A kockázatelemzés során ajánlott a nemzetközi vagy hazai szabványok, ajánlások, legjobb gyakorlatok figyelembevétele.* [2]

Az említett helyzetfelmérés végrehajtásához a jogalkotói elvárás alapján négy, az érintett szervezet jellemzői alapján további egy elméleti kiindulópontot rögzítettünk.

1. A jogszabály alapján a biztonsági osztály „az elektronikus információs rendszer védelmének elvárt erőssége", aminek alapja „az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása"[1], továbbá magának „az elektronikus információs rendszernek a sértetlensége és rendelkezésre állása" biztosításának követelménye. Az *adat/információ* és a *rendszer* tehát „együtt mozog"; ebből következően *a rendszer biztonsági osztályba sorolása az adatok/információk osztályba sorolásán alapulhat*.
2. Az Ibtv. szerint a biztonsági osztályba sorolást kockázatelemzés alapján kell elvégezni. A besorolás – értékelés – módszere tehát adott, ajánlott szempontjai és számítási módja nem ismertek. Az Ibtv. indokolása néhány irányelvi jellegű utalást tartalmaz (a védelemnek költséghatékonynak kell lennie; a kár meghatározása során a nagyságrend megállapítása elégséges, a pontos értéket nehéz és költséges meghatározni; a besorolásnál mindhárom védelmi szempontot – CIA-elv – figyelembe kell venni), továbbá utal a Közigazgatási Informatikai Bizottság 25. számú Ajánlására. Konkrét eligazítást azonban a biztonsági besorolás, illetve a kockázatelemzés vonatkozásában e dokumentum sem tartalmaz. [3]
3. Az Ibtv. és a technológiai rendelet is ajánlja a nemzetközi vagy hazai szabványok, ajánlások, legjobb gyakorlatok figyelembevételét. Erre figyelemmel a biztonsági

[1] Az eredeti angol kifejezések - confidentiality, integrity, availability - kezdőbetűi alapján a közkeletű rövidítés: CIA-elv.

osztályba soroláskor *az MSZ ISO/IEC 27001:2006 szabvány* (a továbbiakban: 01 szabvány) *ajánlásait vettük figyelembe*. [4]

4. A kockázatelemzés egy lehetséges módszertanával részletesen foglalkozó *MSZ ISO/IEC 27005 szabvány* (a továbbiakban: 05 szabvány) kétszintű kockázatelemzést javasol. Eszerint először egy *magas szintű biztonsági kockázatelemzés* elvégzése indokolt. Részben azért, mert így általános, a legfontosabb szempontokra koncentráló áttekintést lehet nyerni a szervezet vonatkozásában felmerülő kockázati elemekről. Részben pedig azért, mert egy túlzottan részletes kockázatelemzés jelentős energiákat köthet le, ugyanakkor – amennyiben nem állnak rendelkezésre megfelelő (jellemzően pénzügyi) erőforrások az elemzés alapján végrehajtandó intézkedésekre – idő előtti lehet. A szabvány szerint egy-két éves időtávban megvalósítható intézkedések esetén a részletes elemzés korai. Az értékelés második szintjeként valósulhat meg a *részletes biztonsági kockázatelemzés*, amelynek során *minőségi jellemzők* értékelésére kerülhet sor egy 3-5 fokozatú skála mentén. Egy későbbi, matematikai műveletekkel végrehajtandó elemzéshez azonban még ez is kevés lehet. [5]
5. Esetünkben a Nemzeti Adó- és Vámhivatal (a továbbiakban: NAV) elektronikus információs rendszerei biztonsági besorolása és biztonsági szintjének meghatározása a feladat. 2013. évi adatok szerint a NAV-nak 4 központi, 18 közép- és 49 alsó fokú területi szerve, valamint 7 alsó fokú vámszerv kirendeltsége van, engedélyezett létszáma 22.482 fő (ennyi potenciális felhasználó van a Hivatalon belül, ezen túl milliós ügyfélkörrel rendelkezik), hatásköri jegyzéke több mint 1040 elemet tartalmaz, éves szinten mintegy 66 millió dokumentumot kezel, egy évben a levelező rendszereiben mintegy 129 millió dokumentum keletkezik. A NAV tevékenységét támogató informatikai infrastruktúra legtöbb adata nem nyilvános, azonban a nyilvános források megemlítik, hogy a NAV közel 20.500 db PC-t és 3.500 db laptopot üzemeltet és az idézett forrás 26 rendszert/alkalmazást nevesít. [6] A magyar közigazgatás egyik legnagyobb szervezete esetében olyan elemzés és besorolás szükséges, amely a részletek túlzott hangsúlyozása helyett stratégiai szintű áttekintést biztosít, ezzel egyidejűleg az informatikai szempontból jelentős szempontokra helyezi a hangsúlyt.

A technológiai rendelet rendelkezéseinek és a szabványok ajánlásainak való együttes megfelelés vonatkozásában, a NAV szervezeti sajátosságait és informatikai infrastruktúráját alapul véve, az alábbi javaslatot fogalmazzuk meg.

BIZTONSÁGI OSZTÁLYBA SOROLÁS

A 01 szabvány az informatikai osztályozás elveit az alábbiak szerint határozza meg: *Az információkat értékük, a jogi előírások, a szervezet szempontjából képviselt érzékenységük és kritikusságuk szempontjából kell osztályozni.*

Tekintettel a fent már kifejtettekre, a 01 szabvány előírásain alapuló osztályozást az adatokra vonatkoztatva végezzük. Álláspontunk szerint – figyelemmel arra, hogy az informatikai rendszereket nagymértékben meghatározza a bennük kezelt adat – ugyanezen kategóriák mérvadóak az informatikai rendszerek besorolásánál is.

A technológiai rendelet 1. sz. mellékletének 1.1. pontja szerint *az érintett szervezet az elektronikus információs rendszere biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelményét a rendszer funkciójára tekintettel, ahhoz igazodó súllyal érvényesíti.*

A szabvány kategóriáinak való megfelelés

Az *érték* az adatot kezelő informatikai rendszert használó szervezet működését, megítélését befolyásoló tényező, ami alapvetően az adatok hiánya, elérhetetlensége, kitudódása vagy sérülése folytán bekövetkező kár nagyságrendjén keresztül fogható meg.

Ezért javaslatunkban a kár mind a bizalmasság, mind a sértetlenség, mind pedig a rendelkezésre állás vonatkozásában értékelésre kerül, figyelemmel a technológiai rendelet 1. sz. mellékletének 1.2.1.1. pontjára is, amely szerint *az adatok és az adott információs rendszer jellegéből kiindulva a kockázatelemezés alapját* egyrészt *az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának*, másrészt *az elektronikus információs rendszerelemek sértetlenségének és rendelkezésre állásának sérüléséből, elvesztéséből bekövetkező kár, vagy káros hatás, terjedelme, nagysága képezi*.

A technológiai rendelet 1. sz. melléklete 1.4. pontjának alpontjai a fenyegető vagy bekövetkező *károk* fajtáit határozzák meg. Eszerint figyelembe kell venni a

1.4.1. társadalmi-politikai káros hatásokat, károkat vagy a jogsértésből, kötelezettség elmulasztásából fakadó káros hatásokat, károkat (így pl. alaptevékenységek akadályozása, különösen a létfontosságú információs rendszerelemek működési zavarai, a nemzeti adatvagyon sérülései, jogszabályok és egyéb szabályozások megsértése, jogszabály által védett adatokkal történő visszaélés vagy azok sérülése, a közérdekűség követelményének sérülése, személyiséghez fűződő jogok megsértése, bizalomvesztés hatóságokkal, felügyeleti szervekkel szemben, az ország jogrendjének sérülése, vagy ennek lehetővé tétele);

1.4.2. személyeket, csoportokat érintő károk, káros hatások (pl. különleges személyes adatok, banktitkok, üzleti titkok megsértése, szervezet, személyek vagy csoportok jó hírének károsodása, személyi sérülések, vagy haláleset bekövetkeztének - ideértve az elektronikus információs rendszer működésének zavara, vagy információhiány miatt kialakult veszélyhelyzetet - veszélye);

1.4.3. közvetlen anyagi károk (az infrastruktúrát, az elektronikus információs rendszert ért károk, és ezek rendelkezésre állásának elvesztése miatti pénzügyi veszteség, adatok sértetlenségének, rendelkezésre állásának elvesztése miatti költségek, dologi kár);

1.4.4. közvetett anyagi károk (pl. helyreállítási költségek, elmaradt haszonnal arányos költségek, a környezet biztonságának veszélyeztetése, perköltségek).

Természetesen kijelenthető, hogy nem minden szervezet esetében jöhet szóba mindegyik kártípus; az adott szervnél értelmezhető, szóba jöhető és a tapasztalatok alapján releváns károkat kell figyelembe venni. Ezt a rugalmasságot írja elő a technológiai rendelet 1. sz. mellékletének 1.4. pontja is, amely szerint *az érintett szervezetnél szóba jöhető - közvetett, vagy közvetlen kárt okozó hatásokat, veszélyeket és károkat kell - az érintett szervezet jellemzőire tekintettel - figyelembe venni.*

A besorolási táblázatban az egyes környezetek vonatkozásában értelmezhető és szóba jöhető károk összességükben értékelendőek, azok közül nem emelhető ki egyik sem.

A technológiai rendelet 1. sz. mellékletének 2. pontja ajánlást tartalmaz az egyes biztonsági osztályok jellemzői vonatkozásában. E körben megjegyezzük, hogy e jellemzők nem teljesen illeszkednek a technológiai rendelet 1. sz. mellékletének 1. pontja alatt szereplő általános elvekhez. A 2. pont a biztonsági osztályok fő jellemzőjévé a bekövetkező vagy fenyegető kár jelentőségét teszi. Ezzel szemben az 1. pont 1.3. pontja szerint *a biztonsági osztályba sorolásnál nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást kell figyelembe venni.* Tehát nem önmagában a kár nagysága a mérvadó, hanem figyelembe kell venni a káresemény bekövetkezési valószínűségét is.

A kockázatok számba vételénél – megelőzendő a kialakított rendszer szétesését, egyben elősegítve az áttekinthetőséget – mellőztük a bonyolult matematikai képletek és számítások alkalmazását. A NAV informatikai rendszereit fenyegető kockázatok vonatkozásában, az

eddigi tapasztalatok fényében – figyelemmel a kialakult jó gyakorlatra is –, kiemeltük az egyes biztonsági célok megvalósulását fenyegető tényezők közül a legjellemzőbbeket és ezek fennálltához, illetve hiányához (vagy egy háromfokozatú skálán való elhelyezkedésük alapján) rendeltünk besorolási pontszámot.

Meg kívánjuk jegyezni, a NAV esetében – ahogyan az a legtöbb központi közigazgatási szervre jellemző – az objektumvédelemre és a tűzvédelemre vonatkozó szabályozás markánsan elkülönül az informatikai biztonság szabályozásától. Erre figyelemmel az e körben felmerülő kockázatok – mint az informatikai területen túli kockázatok – a biztonsági besorolás tekintetében figyelmen kívül maradtak.

Az előbbiekhez hasonlóan ugyancsak nem kerültek tekintetbe vételre a személyi állomány (felhasználók) személyében rejlő, az informatikai vetülethez közvetlenül nem kapcsolódó biztonsági kockázatok, mivel azok alapvetően a kiválasztási kritériumrendszer működtetésének, valamint a személyügyi biztonsági szabályozás körébe tartoznak. Azonban a személyi biztonság informatikailag közvetlenül leképezhető kockázatai (felhasználók informatikai alapú azonosítása az informatikai rendszerek használata előtt és alatt – autentikáció és autorizáció, naplózás, manuális beavatkozás lehetősége) értékelésre kerültek.

A megoldás a 05 szabvány magas szintű kockázatelemzési eljárására tekintettel az informatikai szempontból releváns elemeket tartalmazza, azonban az egyszerű számbavétel helyett („van-nincs”) a részletes kockázatelemzésnél elvárt – súlyozást is tartalmazó – értékelést valósít meg.

A technológiai rendelet rendszerében a biztonsági osztályok jellemzése során hangsúlyt kap az adatok mennyisége, valamint a különleges személyes adatok érintettsége. E körülmények a NAV tekintetében azonban nem tekinthetőek relevánsnak. A NAV informatikai rendszerei szinte kizárólag hatalmas adattömeget kezelnek, különösen amennyiben a rendszerkapcsolatok létét és számát is figyelembe vesszük, így az adatok mennyisége – a NAV esetében – nem alkalmas szempont az egyes rendszerek jelentőségének megkülönböztetésére.

Ezen túlmenően a különleges személyes adatok kezelése sem tekinthető relevánsnak, mivel a NAV esetében ilyen adatok kezelése nem tekinthető tipikusnak és általánosnak. E jellemzők alapvetően a NAV-ra vonatkoznak, így más szerv esetén ezek a kategóriák alkalmazása természetesen nem kizárt, sőt adott esetben kiemelt fontossággal bírhat.

A *jogi előírások* kategóriáján az informatikai rendszerekben tárolt adatok jogi minősítését értjük. A hatályos jogszabályok több mint 10 adatfajtát nevesítenek, ennek alapján a kezelt adatok körét három kategóriába sorolva célszerű meghatározni: nyilvános adat, törvény által védett adat és minősített adat. A törvény által védett adat fogalmába tartoznak különösen a személyes adat, adótitok, vámtitok, banktitok, értékpapírtitok stb. A rendszerben kezelt adatok fajtája a bizalmasság kategóriájának a részét képezi. Nyilvános adat esetén a bizalmasság kérdése irrelevánsnak tekinthető, figyelemmel arra, hogy azokat bárki megismerheti, míg törvény által védett adat vagy minősített adat kezelése esetén e tény döntő befolyást gyakorol az informatikai rendszer jelentőségére.

Az *érzékenység* szempontja a bizalmasság és a sértetlenség kategóriáin, mint biztonsági célokon keresztül érvényesül, így ez a szempont bővebben e kategóriáknál kerül kifejtésre.

A *kritikusság* szempontja pedig a rendelkezésre állás biztonsági céljának felel meg, így kifejtését lásd ott.

A technológiai rendeletnek való megfelelés

Amint azt fent már említettük, a technológiai rendelet, valamint a 01 szabvány alapján az értéket, és az azt kifejező kárt mind a bizalmasság, mind a sértetlenség, mind pedig a rendelkezésre állás tekintetében értékeljük. A technológiai rendelet 1. sz. mellékletének 1.2.1.2. pontja szerint azonban nem elegendő a kár mértékének a figyelembe vétele, hanem a

kockázatelemzés alapját képezi *a kár bekövetkezésének, vagy a kárral, káros hatással fenyegető veszély mértéke, becsült valószínűsége* is.

A technológiai rendelet 1. sz. mellékletének 1.3. pontja alapján kijelenthető, hogy *a biztonsági osztályba sorolásnál nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást kell figyelembe venni.* A kár bekövetkezési valószínűsége vonatkozásában pedig a technológiai rendelet 1. sz. mellékletének 1.5. pontja szerint pedig *a veszélyeztetettségnek a bekövetkezés valószínűségének megfelelő kárérték szinteknek megfelelő biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelménye külön-külön értékelendő.*

A fentiekre figyelemmel, a technológiai rendelet követelményeinek való megfelelés érdekében mind a bizalmasság, mind a sértetlenség, mind pedig a rendelkezésre állás biztonsági céljai vonatkozásában egyszerre kerülnek értékelésre a biztonsági célok teljesülését veszélyeztető fenyegetések mértéke, valamint a bekövetkező vagy fenyegető kár is.

A *bizalmasság* fogalma alapvetően az adathoz való jogosulatlan hozzáférést jelenti, sérülése az ebből következő, a szervezet működését és megítélését befolyásoló negatív hatás.

A bizalmasság egyik elemének tekinthető a rendszerben kezelt adatok *jogi minősítése*, amely alapján az adat lehet nyilvános adat, törvény által védett adat vagy minősített adat. A törvény által védett, illetve minősített adatot kezelő rendszereknél a bizalmasság alapvető fontosságúnak tekinthető, mivel törvény ezen adatok vonatkozásában korlátozza a megismerésre jogosultak körét. Ezzel szemben a nyilvános adatok esetén a bizalmasság fogalma irreleváns, mivel ebben az esetben az adatokat bárki megismerheti. Meglátásunk szerint a bizalmasság sérüléséből fakadó kár is objektíven a jogi minősítésen keresztül ragadható meg. Egy törvény által védett vagy minősített adat esetében a bizalmasság sérülése okozhatja a szervezetnek a legnagyobb kárt, különös figyelemmel arra, hogy ebben az esetben esetlegesen mind anyagi kár (pl. személyiségi jogok sérelme miatti sérelemdíj, kártérítés), mind presztízsveszteség (pl. negatív sajtóvisszhang, közbizalom megrendülése) nyomatékosan felmerülhet, illetve esetlegesen a szerv alaptevékenységének sikeres ellátása is veszélybe kerülhet (pl. a NAV esetében a kockázatkezelési tevékenységhez kapcsolódó szakmai ismeretek, informatikai programok, algoritmusok stb. kitudódása).

A bizalmasság kérdésköre kapcsán azonban a technológiai rendelet fentebb említett rendelkezése alapján figyelemmel kell lenni a veszélyeztetettség mértékére is. E körben a NAV informatikai struktúrájából fakadó, a gyakorlat alapján felmerülő kockázatokat vettük alapul. Természetesen más informatikai jellemzőkkel bíró szervezet esetében e kritériumok változhatnak.

A bizalmasság körében kockázatként a külső hálózatokhoz (pl. internet) való csatlakozást, továbbá az autentikáció és autorizáció formáját, biztonságosságát határoztuk meg. A külső kapcsolat megléte önmagában kockázatot jelent, ugyanis az fizikailag lehetővé teszi a külső, illetéktelen behatolást az informatikai rendszerbe. Az autentikáció és autorizáció módja is meghatározza a rendszerbe történő illetéktelen belépés kockázatát. E körben jelenleg a tudás alapú azonosítás (jelszavas védelem) jelenti a legkisebb védelmet, így a legnagyobb kockázatot. Amennyiben az azonosító- és jelszóhasználat birtoklás alapú védelemmel egészül ki (pl. hardvereszköz, token), úgy a kockázat csökken. E körben – a jelenlegi elterjedt védelmi megoldások közül – a legnagyobb biztonságot a tulajdonság alapú (biometrikus) azonosítás garantálhatja, e módszerrel gyakorlatilag kizárható az illetéktelen belépés lehetősége.

Az említett tényezők együttes figyelembe vételével valósul meg a technológiai rendelet azon követelménye, miszerint *a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást kell figyelembe venni.*

A *sértetlenség* biztonsági célja az adat megváltozásának, megsemmisülésének, valamint jogosulatlan megváltoztatásának, megsemmisítésének a szervezet működését és megítélését befolyásoló hatását jelenti.

E körben a fentiek alapján értékelendő, hogy az adatok esetleges megváltozása milyen kárt jelent a szervezet szempontjából. Utalva a korábban már kifejtettekre, a szóba jöhető károkat összességükben kell értékelni, anélkül, hogy azok közül bármelyiket is kiemelnénk.

A kockázatok körében értékelendő, hogy az adat helytelensége belső eljárás vagy informatikai megoldás következtében a szervezet belső működése során, az ügyintézés szempontjából releváns időn belül ki derülhet-e. Amennyiben ugyanis az adat helytelensége az adott informatikai rendszeren kívüli módon kiderülhet, ez a körülmény csökkenti a sértetlenség biztonsági célja sérülésének kockázatát. Ugyancsak a kockázatok körében értékelendő, hogy az adott rendszer lehetővé teszi-e a felhasználók és az üzemeltetésben részt vevő informatikusok részéről a (nem indokolt) manuális beavatkozás lehetőségét. Amennyiben ilyen lehetőség nem adott, az nyilvánvalóan csökkenti az informatikai rendszert fenyegető veszélyt. E körben értékelendő még az adott rendszer naplózottsága is az adatok megváltozása vonatkozásában, ez ugyanis szinte biztossá teszi az illetéktelen adatmódosítás felderítését, és az ehhez kapcsolódó felelősségre vonást, ami a felhasználók számára komoly visszatartó erővel bírhat.

E körben is a kár és a kockázati tényezők egyes elemeinek az együttes értékelése adja ki a sértetlenség besorolási pontszámát.

A *rendelkezésre állás* az informatikai rendszer (és így az adat) jogosultak általi elérésének, felhasználásának előre nem tervezett korlátozottságát vagy hiányát jelenti.

E körben alapvető fontossággal bír, hogy milyen mértékben befolyásolja (veszélyezteti, akadályozza, lehetetlenné teszi) a szervezet működését, illetve, hogy a szervezet mennyi ideig tudja nélkülözni az adott adatot, informatikai rendszert bármilyen kár felmerülése nélkül.

A rendelkezésre állás biztonsági céljának a kategóriájában is értékelésre kerül a tűréshatáron túli kieséssel okozott kár.

Ezen túlmenően a veszélyeztetettség két elemből áll össze.

Egyrészt definiálni kell, hogy az adott rendszer kiesése (az adat elérhetetlensége) mennyi idő után okoz a szerv számára bármilyen kárt. Ez sávokban adható meg. Egyrészt vannak olyan rendszerek, amelyek esetében szinte a szünet nélküli működés az elvárás. E rendszerek esetében a helyreállítás elvárt határideje legfeljebb 4 óra. Másrészt vannak olyan rendszerek is, amelyek 4 órán túli hiánya nem gyakorol alapvető befolyást a szerv napi tevékenységi körébe tartozó feladatok elvégzésére. A 4 óra helyreállítási idő, mint határ, a NAV belső munkafolyamatainak és az informatikai rendszereinek jellemzői alapján, a felhasználó szakmai területek igényeinek a figyelembe vételével, valamint az általános helyreállítási idő körében szerzett tapasztalatok alapján került meghatározásra. Természetesen más jellemzőkkel bíró szervezet esetében más időkorlát lehet megfelelő.

Másrészt a veszélyeztetettség körében javasoljuk értékelni azt, hogy az empirikus tapasztalatok alapján az adott rendszer üzemidejéhez képest átlagosan hány százalékot tesz ki az előre nem tervezett leállás, elérhetetlenség. Ennek meghatározásához javasoljuk az utolsó három év adatainak az átlagát venni. Ez a rendelkezésre állás biztonsági céljának sérülése vonatkozásában az utóbbi idők tapasztalatai alapján jelöli meg a valós kockázatot. E dinamikus, minden évben változó értékű kategória kialakítása során mindenképpen középtávú átlagot javaslunk figyelembe venni, ami korrigálhatja az időszakos kilengéseket, illetve tekintetbe tudja venni az egyes fejlesztésekkel járó minőségi javulást is. E körben a skála egyes értékei (kicsi, közepes, magas) kapcsán a százalékos határokat (pl. átlagban 99% feletti rendelkezésre állás – kicsi; átlagban 98-99%-os rendelkezésre állás – közepes; átlagban 98% alatti rendelkezésre állás – magas) minden esetben az adott szerv munkafolyamatai és elvárásai alapján javasoljuk meghatározni.

ÖSSZEGZÉS

Az ismertetett besorolási javaslat megfogalmazásakor a szerzők elsődleges célja egy elvi szempontok szerint *alkalmazható* és a jelenlegi adottságokat figyelembe véve *végrehajtható* értékelési rendszer kidolgozása volt, amely:

- az elvi kereteket tekintve a jogszabályok és a meghatározó szabványok közötti összhang megteremtésével konzisztens alapokat nyújt;
- figyelemmel van a közigazgatási szervek azon sajátosságára, miszerint a különböző információvédelmi aspektusok jellemzően más-más (személyügyi, objektumvédelmi, informatikai) szakterület, szervezeti egység kompetenciájába tartoznak, így a felméréseket, az intézkedések tervezését és végrehajtását egy-egy szakterület önállóan végzi saját feladatkörén belül, és az intézkedések összehangolása már az egyes szervezetek közötti/feletti koordinációval valósulhat meg;
- mivel a jogszabályok hatályba lépésével keletkező, több évre szóló kötelezettségek, feladatok teljesítésére többlet-erőforrás nem lett tervezve, az érintett közigazgatási szerv meglevő erőforrásai teljesítőképességéhez és konkrét adottságaihoz igazodó, a már rendelkezésre álló tudást hasznosító értékelési szempontrendszert biztosít;
- tekintettel arra, hogy kész, azonnal használatba vehető értékelési módszertanok nincsenek, a rendelkezésre álló – a szakirodalom szerint rövid – határidőn belül alkalmazható módszertant bocsát az informatikai szakterület rendelkezésére.

A biztonsági osztályba soroláshoz szükséges értékelési adatokat a mellékelt táblázat tartalmazza.

A közigazgatási szerv biztonsági szintbe sorolásával kapcsolatos elméleti és gyakorlati kérdések egy másik tanulmány tárgya lehetnek.

Felhasznált irodalom

[1] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.)

[2] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 77/2013. (XII. 19.) NFM rendelet

[3] Közigazgatási Informatikai Bizottság 25. számú Ajánlása. 2008. június

[4] MSZ ISO/IEC 27001:2006 szabvány. Informatika. biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények

[5] MSZ ISO/IEC 27005 szabvány. Information technology – Security techniques – Information security risk management

[6] Nemzeti Adó- és Vámhivatal Évkönyve. Budapest, 2013.

Bizalmasság		**pont**	**Sértetlenség**		**pont**	**Rendelkezésre állás**		**pont**	**összes pont-szám**
Kezelt adatfajta	nyilvános adat	0	Megváltozás esetén a kár mértéke	kicsi	0	A rendszer kiesésének tűrési ideje	4 órán belül	1	
	törvény által védett adat	1		közepes	1				
	minősített adat	2		nagy	2		4 órán túl	0	
Azonosítás formája	jelszavas	2	Van-e naplózás az adat megváltozására?	van	0	A tűrési időn túli kiesés által okozott kár	kicsi	0	
	jelszavas + token	1		nincs	1		közepes	1	
	biometrikus	0	Biztosított-e a manuális beavatkozás lehetősége?	igen	1		magas	2	
Van-e a rendszernek külső kapcsolata?	igen	1		nem	0	Átlagos veszélyeztetettség az utolsó három év adatai alapján	kicsi	0	
							közepes	1	
	nem	0	Egyéb módon kiderül-e az adat helytelenségre?	igen	0		magas	2	
				nem	1				
Összes pont:									

Biztonsági osztályba sorolás:

1. biztonsági osztály 0-3 pont
2. biztonsági osztály 4-6 pont
3. biztonsági osztály 7-9 pont
4. biztonsági osztály 10-12 pont
5. biztonsági osztály 13-15 pont

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Kassai Károly
kassai.karoly@hm.gov.hu

A MINŐSÍTETT ADATOK KEZELÉSÉRE FELJOGOSÍTOTT HÍRADÓ-INFORMATIKAI RENDSZEREK VÁLTOZÁSKEZELÉSÉNEK KÉRDÉSEI A MAGYAR HONVÉDSÉGNÉL

Absztrakt

A biztonsági környezet változása, új felhasználói igények megjelenése, technológiai fejlődés, hálózati vagy felhasználói eszközök meghibásodása, vagy szoftverhiba, illetve más indokok miatt válhat szükség a rendszer hardver vagy szoftver konfigurációjának módosítása. A konfigurációváltoztatás egyes esetekben egyszerű, más esetekben összetett felkészülést és támogatást igénylő feladat. A katonai szervezetek vezetése és irányítása gyakran minősített adatok elektronikus kezelését igényli. A kommunikációs rendszerek az akkreditáló hatóság biztonsági felügyelete alatt állnak, így a változtatások engedélyezése esetenként bonyolult hivatalos ügyintézést igényel. A cikk a konfiguráció változás kérdéseit vizsgálja, használható megoldást keresve a katonai szervezetek támogatása érdekében.

Changes in the security environment, the emergence of new user requirements, technological development, network or user equipment failure, software malfunctions or other reasons may require modification in the hardware or software configuration. The configuration change simple in some cases, in other cases require complex preparation and support. Management and control of the military organizations often require electronic handling of classified information. The communications and information systems are under the control of the security accreditation authority, thus authorization of the changes requires official actions sometimes with some complications. The article examines the issue of configuration changes, in search of a solution used to support military organizations.

Kulcsszavak: *információbiztonság, elektronikus információbiztonság, kiberbiztonság, szabályozás, változáskezelés ~ information security, electronic information security (INFOSEC, Information Assurance, CIS Security), cyber security, regulation, change management.*

BEVEZETÉS

A Magyar Honvédség szervezeteinél a minősített adatok kezelése az Alaptörvényben és erre épített jogszabályokban meghatározott szervezeti feladatokból adódó követelmények miatt megkerülhetetlenül szükséges.

A minősített adatok kezelésére – kiemelt figyelemmel a minősített elektronikus adatkezelésre – vonatkozó jogszabályi követelmények hazánkban a NATO csatlakozáshoz kötötten 1999-ben, majd az EU csatlakozás kapcsán 2004-ben, illetve az előbbieket is integrálva, a nemzeti követelményeket is modernizálva 2009-ben jelentősen változtak.

A fejlődés nem kerülhette el a Magyar Honvédséget sem, így a felhalmozódott tapasztalatok alapján célszerű átfogóan, vagy egy-egy területet kiemelve áttekinteni az elektronikus információbiztonsági kérdéseket, ami segítheti a helyzet pontosabb megértését, támogatja a jövőbeli változások előkészítését.

A cikk témája egyszerű kérdést megoldását célozza: a minősített elektronikus adatkezelő rendszerek (katonai terminológia szerint: híradó-informatikai rendszerek) hatósági engedélyezéshez kötött változásaival kapcsolatos teendők egyszerűsítése, a változáskezelési folyamat felgyorsítása.

A kérdés tanulmányozását az a gyakorlati igény váltotta ki, hogy a Magyar Honvédség szervezetei egyre nagyobb számban rendelkeznek a Nemzeti Biztonsági Felügyelet – mint akkreditáló hatóság – által jóváhagyott, elektronikus minősített adatot kezelő híradó-informatikai rendszerekkel. Ezek a rendszerek az üzemeltetés során – ugyanúgy, mint minden más elektronikus adatkezelő rendszerek – meghibásodnak, új felhasználói igény, környezeti változás vagy amortizálódás, új sebezhetőség megjelenése miatt változásokat igényelnek.

A változások hatósági engedélyhez kötöttek, ami nyilvánvalóvá teszi az üzemeltető katonai szervezet, a középszintű vezető szerv, a szakmai irányítási feladatokat végző központi szerv és a hatóság közötti hivatalos kommunikációt. Ez a változási kérelem felterjesztését és az arra adott hivatalos válasz továbbítását jelenti, még a szükségesnek ítélt változások megkezdése előtt.

A katonai műveletek dinamikája, illetve a műveletek környezeti változásainak széles skálája eltérő a napi életben megszokott változási sebességtől. A harcászati környezet kihívásai lényeges ponton eltérnek a hadműveleti, stratégiai vezetési és irányítási rendszerek működési jellemzőitől. Ezek a sajátosságok természetesen nem tükröződnek a közigazgatásra vonatkozó, keretrendszerű jogszabályokban, eljárásokban. Ugyanakkor szükségszerű annak megállapítása, hogy a katonai műveletek támogatását szolgáló, minősített adatok kezelésére feljogosított (akkreditált) híradó-informatikai rendszerek nem mentesülnek a jogszabályokban megfogalmazott követelmények teljesítésétől.

A hatósági ügyintézéshez kapcsolódó szolgálati kommunikáció, az ezzel kapcsolatos nyilvántartási feladatok időigényesek, így nyilvánvaló szükséglet egyrészt a bürokráciacsökkentés, másrészt a katonai feladatok időbeli biztosításához szükséges gyors reagáló képesség kialakítása és biztosítása.

A megfogalmazott – jól láthatóan ellentmondásos – tényezők összehangolása, a bonyolult helyzet megoldása nem tűnik egyszerű feladatnak.

A változások menedzselése (change management), más kifejezéssel élve a változásfelügyelet (change control) kérdéskör nemzetközi szabványokban, nemzeti ajánlásokban, a „bevált gyakorlat (best practice)” típusú dokumentumokban és jogszabályokban más-más szemlélettel és részletezettségben olvasható, mely referenciák segíthetnek a probléma megértésében és a megoldás keresésében.

A cikk első részében e források – tudatosan nem teljes körű – bemutatása történik az általánosan elfogadottnak tekinthető tartalmi megközelítés szempontjainak vázolása érdekében, majd a katonai sajátosságoknak megfelelő válaszhoz szükséges megalapozás olvasható.

A VÁLTOZÁSOKRA VONATKOZÓ AJÁNLÁSOK, KÖVETELMÉNYEK

Az informatikai szolgáltatásirányításra vonatkozó szabvány értelmezése szerint a változásfelügyelet (change control): „azok az eljárások, amelyek biztosítják, hogy minden változás ellenőrzött legyen, beleértve annak kérelmezését, rögzítését, elemzését, a vonatkozó döntés meghozását, jóváhagyását, kivitelezését és a változás megvalósítás utáni áttekintését is."

A változáskezelés célja, hogy minden változtatás kiértékelése, jóváhagyása, megvalósítása és felülvizsgálata ellenőrzötten történjen. Ennek érdekében:

- a szolgáltatások és infrastruktúra területén szükséges változtatásokat pontosan meg kell határozni, a változások végrehajtását dokumentálni kell;
- a változásokra vonatkozó kérelmeket nyilvántartásba kell venni és osztályozni kell;
- a változásokra vonatkozó kérelmeket kockázatuk, hatásuk és hasznuk szerint értékelni kell;
- a változáskezelési folyamatnak tartalmaznia kell a sikertelennek bizonyuló változtatások után a kiindulási helyzet visszaállításához szükséges eljárásokat;
- a változtatásokat jóvá kell hagyni és a végrehajtásukat ellenőrizni kell;
- a változtatások után vizsgálni kell, hogy kitűzött célok megvalósultak-e, illetve az alkalmazott rendszabályok sikeresek voltak-e. [1]

A nemzetközi információbiztonsági menedzsment szabvány is foglalkozik a változások menedzselésével.

A szabvány az üzemeltetési eljárások és felelősség területén szabályozási célként javasolja az adatkezelő létesítmények helyes és biztonságos üzemeltetésének biztosítását. Ennek érdekében az üzemeltetési eljárásokat dokumentálni kell, és a szükséges dokumentumok elérhetőségét biztosítani kell minden olyan felhasználónak, akinek arra szüksége van.

A változások menedzselésére vonatkozó általános követelmény, hogy felügyelni kell a szervezeti változások során, vagy a működési vagy adatkezelő folyamatokban, adatkezelő rendszereknél bekövetkező változásokat, amelyeknek hatása van az információbiztonságra. [2]

Az Amerikai Egyesült Államok közigazgatási szervezeteire és elektronikus adatkezelő rendszereire vonatkozó követelmény szerint az alkalmazó szervezetnek ki kell alakítani, dokumentálni kell és alkalmazásba kell venni egy olyan konfiguráció felügyeleti eljárást, amely:

- meghatározza a szabályokat, felelősségeket, a konfigurációfelügyeleti folyamatokat és eljárásokat;
- folyamatokat határoz meg a rendszer teljes életútján keresztül a konfiguráció elemek azonosítása és a konfigurációfelügyelet érdekében;
- meghatározza az információs rendszerek konfiguráció elemeit és azokat a menedzsment felügyelet hatókörébe rendeli;
- védelmi rendszabályokat alakít ki a konfiguráció felügyeleti eljárás illetéktelen megismerése vagy módosítása ellen. [3]

Az ausztrál nemzeti ajánlás a változáskezelést áttekinthetően tárgyalja, melynek a lényegi elemei a következők.

A változtatás indoka:

- biztonsági sebezhetőség, új fenyegetés megjelenéséhez kötött kockázatnövekedés;
- felhasználó által azonosított problémák vagy a szolgáltatások kiterjesztése;
- a gyártó által kezdeményezett eszközfejlesztés vagy szoftverfrissítés;
- a gyártó által jelzett eszköz vagy életciklus támogatás megszüntetése;
- általános technológiai fejlődés;

- új rendszerek alkalmazása, ami miatt szükségessé válik a meglévő rendszerek változtatása;
- szervezeti változások;
- szervezeti folyamatok változásai;
- a szabványok fejlődése;
- kormányzati követelmények;
- incidensek bekövetkezése vagy a folyamatos szolgáltatásfejlesztési igény.

A változások lehetnek:

- eszköz bevezetése vagy modernizálása;
- szoftver bevezetése vagy frissítése;
- a védelmi rendszabályokban bekövetkezett fontos változás.

A szervezeteknek hivatalos változásmenedzsment folyamatot kell kialakítani, melynek jellemzői:

- azon változások kijelölése, melyek a hivatalos változásmenedzsment folyamaton keresztül valósíthatók meg;
- a változásokat dokumentálni kell;
- a változásra vonatkozó kérelmet hivatalosan jóvá kell hagyni;
- a változások naplóadatait auditálni kell, majd meg kell azokat őrizni;
- a jelentős változások előkészítésekor sebezhetőség vizsgálatot kell tartani;
- a jóváhagyott változásokat tesztelni kell;
- a biztonsági dokumentumokban át kell vezetni a szükséges változtatásokat;
- az érintett felhasználókat értesíteni kell, és ki kell képezni a változáshoz lehetőleg közeli időpontban;
- folyamatosan képezni kell a felhasználókat a változáskezeléssel kapcsolatos feladatokról.

A szervezeteknek biztosítani kell, hogy a normál (rutin) és a sürgősségi változások során:

- a vonatkozó biztonsági dokumentumban meghatározott eljárásokat betartsák a változás menedzsment folyamat során;
- a javasolt változásokat jóváhagyja az arra illetékes, hatóság, szervezet;
- bármilyen változás, melynek a rendszer biztonságára hatása lehet, fel legyen terjesztve az illetékes akkreditáló hatósághoz jóváhagyásra;
- a változásnak megfelelően minden biztonsági dokumentum pontosítva legyen. [4]

JOGSZABÁLYBAN VAGY FELSŐ SZINTŰ SZABÁLYOZÓBAN MEGFOGALMAZOTT KÖVETELMÉNYEK

Az elektronikus információbiztonságra vonatkozó törvény végrehajtási rendelete több szempontot is azonosít a konfigurációváltozások felügyelete (változáskezelés) területén.

Az érintett szervezet:

- meghatározza a változáskezelési felügyelet alá eső változástípusokat;
- meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit (csatolt dokumentációk, teszt jegyzőkönyvek stb.);
- megvizsgálja a változáskezelési felügyelet elé terjesztett, javasolt változtatásokat, majd kockázatelemzés alapján jóváhagyja, vagy elutasítja azokat;

- dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket;
- megvalósítja a jóváhagyott változtatásokat az elektronikus információs rendszerben;
- visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását;
- auditálja és felülvizsgálja a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.

A későbbi problémák elkerülése érdekében a szervezetnek a változások megkezdése előtt vizsgálni kell a változások biztonságra irányuló hatásait (biztonsági hatásvizsgálat).

A változáskezelést támogatja az előzetes tesztelés és megerősítés. A tesztelést elkülönített tesztkörnyezetben kell végrehajtani, ahol kockázat nélkül vizsgálható a működés, a funkcionális sajátosságok, a kompatibilitás, esetleges sebezhetőségek.

A változások végrehajtása során pontosan meg kell határozni a hozzáférési jogosultságokat.

A változáskezelés kötelező része a felülvizsgálat, melynek célja a változások szabályszerűségének ellenőrzése, a kívánt cél eléréséről történő meggyőződés. [5]

A minősített elektronikus adatkezelésre vonatkozó alapvető hatósági követelmény a hatóság által jóváhagyott „biztonsági konfiguráció” alkalmazása.

Engedélyezett rendszeren „az elektronikus biztonságot érintő módosítást végrehajtani a Nemzeti Biztonsági Felügyelet által kiadott rendszerengedéllyel lehet”. [6]

A keretrendszerű jogszabály megfogalmazása egyértelmű, tartalmi kérdések elektronikus információ biztonság szempontjából a követelményekben nem vitathatók. Ezzel együtt az is kijelenthető, hogy az alkalmazó szervezetek működési sajátosságai, az elektronikus információ biztonsági szakmai kultúra, a műveleti sebesség lényegesen befolyásolhatja a jogszabály által megfogalmazott követelmény végrehajtására vonatkozó hatékonyságot.

A változáskezeléssel kapcsolatos kérdések szabályozása szerepel a Magyar Honvédség új Informatikai Szabályzatában is.

A Szabályzatban foglaltak szerint „a változáskezelés a híradó-informatikai rendszerben végrehajtott változtatások hatásának előrejelzésére, valamint a változások összehangoltságának és nyomon követésének biztosítására irányul, amely magában foglalja a kérésteljesítések és az esemény – probléma és incidenskezelések során végrehajtott változásokat”.

Az általános követelmény három pillérre támaszkodik, mint felelősségek, folyamat kijelölési kötelezettség és egyedi esetek kezelése, a következők szerint:

- az üzemeltető szervezetnek meg kell határoznia a változtatásokhoz kapcsolódó, javaslattevő, véleményező és döntésre jogosult, szervezetek, személyek körét;
- az üzemeltető szervezeteknek ki kell alakítaniuk a halasztást nem tűrő változtatások eljárás- és szabályrendszerét;
- központi szolgáltatás üzemeltetési tervétől vagy normatív változáskezelési eljárásrendjétől eltérő módosítás az MH Kormányzati Célú Elkülönült Hírközlő Hálózat hálózatgazdájának engedélyével hajtható végre;

A Szabályzat a híradó-informatikai rendszerek biztonságáról szóló fejezetben olvasható általános biztonsági követelmény között is szerepel a változáskezelés:

- új híradó-informatikai rendszer bevezetése, vagy változást követő alkalmazásba vétele csak a meghatározott engedélyezési eljárás sikeres lefolytatása után történhet;
- az üzemeltetési és biztonsági dokumentumokban azonosítani kell az engedélyezési jogosultságokkal rendelkező hatóságokat és szervezeteket, eljárásokat;
- az üzemeltetési és védelmi rendszabályok engedéllyel, a szükséges dokumentálási és képzési eljárások után változtathatók. [7]

A MAGYAR HONVÉDSÉGNÉL SZÜKSÉGES MEGOLDÁS KÖRVONALAZÁSA

A fentiek alapján az elektronikus minősített adatkezelésre feljogosított híradó-informatikai rendszerek változtatásával kapcsolatos hatósági engedélyezési eljárás a következőkben foglalható össze:

- A keretrendszerű jogszabály részletesen nem szabályozza (nem is szabályozhatja) részletesen a változásokra vonatkozó részletes követelményeket, így a kötelezően betartandó „irányelv"- ként történő értelmezés segíthet a megoldásban. Ez azt jelenti, hogy a jogszabály nem tiltja azt a megoldást, amit a szabványok és bevált gyakorlatként kezelhető dokumentumok ajánlanak: *a normál változáskezelési eljárás megfogalmazását, és a folyamat akkreditáló hatósággal történő jóváhagyatását*. Az akkreditáló hatóságnak így lehetősége van a kezdeményező fél által megfogalmazott eljárásrendet áttekinteni, elemezni, a szükségesnek tartott kiegészítéseket megtenni, majd *a változáskezelési eljárást jóváhagyni*. Az eljárásrend kialakítása során *meg kell fogalmazni a sürgősségi esetekre vonatkozó kivételeket, eljárást is*, mivel a katonai erők alkalmazása elképzelhető olyan helyzetekben, amikor a normál hatósági ügyintézés keretei nehezen alakíthatók ki.
- Az előbbi megállapítást támogatja, hogy a Magyar Honvédségnél lehetőség van a szakfeladatok szolgálati hierarchia szerinti felosztására, a felelősségek szervezeti szintek szerinti meghatározására. Ez azt jelenti, hogy egy honvédelmi szervezet esetében *az akkreditáló hatóság segítségére van a szakirányítási rend szerint a középszintű vezető szerv és a szakmai feladatok irányításáért felelős minisztériumi szerv felügyeleti tevékenysége* (alárendeltségi viszonytól függően egyik vagy mindkettő).
- A Magyar Honvédség esetében lehetőség van az elektronikus minősített adatkezelésre feljogosított híradó-informatikai rendszerek változtatására vonatkozó központi szabályozó kiadására, ami biztosítja az egységes végrehajtáshoz szükséges támogatást. Ez ezt jelenti, hogy *a Magyar Honvédség esetében pontosan meghatározható, hogy mely változási kérelmeket szükséges az akkreditáló hatósághoz felterjeszteni, és mely esetekben lehetséges a helyi engedélyezés (beleértve a szükséges dokumentálási kötelezettséget).*

A források áttekintése után szükség van annak megfogalmazására, hogy miért van szükség minősített elektronikus adatkezelés esetén a hatóság értesítésére, illetve a változások engedélyeztetésére.

Az adatkezelés engedélyezését célzó hatósági eljárás (akkreditálás) célja annak megállapítása, hogy az adott környezetben azonosított fenyegetések, a híradó-informatikai rendszer sebezhetősége és a meghatározott (jogszabályokban, NATO, EU követelményekben vagy hatósági állásfoglalás szerint egyedileg meghatározott) védelmi rendszabályok szerinti állapot az elfogadható kockázat kategóriába tartoznak, az adatkezelés nem tartalmaz nemzeti vagy szövetségi szintű felesleges kockázatokat. A *konfigurációelemek azonosítása (ellenőrzése) ennek megfelelően csak keskeny szeletét adják a hatósági mérlegelésnek*.

Az akkreditáló hatóság (egyszerűbben fogalmazva: a szakértő) így *az üzemeltető szervezet vezetőjének, biztonsági menedzsmentjének garanciát ad* arra, hogy az adott helyzetben, az adott konfiguráció a meghatározott üzemeltetési és védelmi rendszabályokkal felesleges kockázatvállalás nélkül üzemeltethető.

Amikor valamilyen ok miatt szükségessé válik a konfiguráció változtatása, akkor az előbb megfogalmazott *egyensúly felborulhat*, és szükséges lehet annak hatósági vizsgálata, hogy *a változások okán keletkezett-e újabb kockázat és azt milyen kiegészítő védelmi rendszabályokkal lehet ellensúlyozni*, vagy milyen szervezeti érdeket védő eljárást kell életbe léptetni a helyzet

folyamatos kézbenntartása érdekében. Ez az a kulcselem, melynek megértése segít eldönteni, hogy milyen adatok szükségesek a hatósági mérlegeléshez, illetve egyáltalán milyen esetekben van szükség a kockázatok teljes vagy részleges áttekintésére és a védelmi rendszabályok megfelelőségének vizsgálatára.

A jogszabályban meghatározott „biztonságot érintő módosítás" így más megvilágításba kerülhet. Egy meghibásodás miatt cserélendő billentyűzet, monitor, vagy akár az egész felhasználói környezetet biztosító számítógép cseréje a vázoltak szerint olyan változás, amelyet hatósági mérlegelés alá kell vonni? A válasz egyszerű: nem. A kijelölt üzemeltető és biztonsági állomány a biztonsági vezető felügyelete alatt ezeket a változtatási feladatokat kockázatmentesen el kell, hogy tudja végezni! Amennyiben ez kétséges, akkor már az adatkezelés engedélyezése is az volt (tekintettel a szekértői tudással rendelkező üzemeltető és biztonsági állomány hiányára)!

A hatóság szakértői mérlegelésére, *szakmai támogatására akkor van szükség, amikor a védelmi rendszabályok és a biztonsági környezet változásainak összehangolásával kapcsolatos feladatokban valami nem egyértelmű; nem könnyen eldönthető helyzet állt elő, ami felsőbb szintű szervezet hatáskörébe tartozó adatgyűjtést vagy döntést igényel, vagy több megoldásból szakértői tanácsadással lehetséges kiválasztani a fenyegetések ellensúlyozásához szükséges legjobb választ*.

A hatósági feladatok ellátása szempontjából három eset különíthető el:

- változás, ami a biztonsági szint csökkenésével kapcsolatos;
- változás, ami nem befolyásolja a híradó-informatikai rendszer biztonsági szintjét, de hatósági ügyintézést igényel;
- változás, ami nem befolyásolja a híradó-informatikai rendszer biztonsági szintjét, hatósági ügyintézést nem igényel, helyi engedélyezési és felügyeleti eljáráshoz kötött.

Csökkenő biztonsági szint

Ennél az esetnél az esetben az akkreditált konfigurációban vagy az alkalmazási körülmények során olyan változás következik be, ami a jóváhagyott védelmi rendszabályok csökkenését vagy megszűnését jelenti. Példák:

- vírusvédelmi rendszer megszűnése vagy frissítés hiánya;
- TEMPEST védelmi rendszabályok hiányossága, mint árnyékolás, szűrés, biztonsági távolság megszűnése vagy be nem tartása, a felügyelt terület csökkenése;
- fizikai biztonsági rendszabályok hiánya, mint beléptető rendszer kiesése, biztonsági tárolási feltételek megszűnése;
- olyan programok telepítése, melyek az operációs rendszer biztonsági beállításait módosítják;
- összekapcsolás más – esetleg alacsonyabb biztonsági szintű – adatkezelésre feljogosított híradó-informatikai rendszerrel.

Ebbe a kategóriába tartozik a híradó-informatikai rendszerhez kapcsolódó teszt engedélyeztetése is, ami az akkreditált konfigurációval vagy akkreditált környezeten belül történik – akár azonos minősítésű szint kezelésére akkreditált újabb eszközöket vagy rendszert is érinthet –, és új működési rendet vagy konfigurációváltozást okoz, ami az üzemeltetők, akkreditáló hatóság vagy biztonságért felelős személyek számára olyan előre nem látható helyzetet is teremthet, amelyben az adatok, szolgáltatások biztonsági szintje egyértelműen nem azonosítható.

Ezeket az eseteket azért kell jelenteni, mert az akkreditált körülményekhez képest viszonyított információbiztonsági szint csökken, amit kiegészítő rendszabályokkal kell

ellensúlyozni, vagy az új feltételek között kell az üzemeltetést engedélyeznie az akkreditáló hatóságnak.

A bejelentés célja, hogy *a hatóság az új biztonsági szintet mérlegelhesse, a szükséges döntéseket meghozhassa*. A döntések egy része az üzemeltetett híradó-informatikai rendszertől független is lehet, mint gyakoribb hatósági ellenőrzés, időszak utáni adatbekérés.

A döntések másik része lehet kiegészítő védelmi rendszabály vagy korlátozások meghatározása.

Változatlan biztonsági szint, lényeges akkreditálási paraméterek változnak

Az akkreditált híradó-informatikai rendszer környezetében, vagy az üzemeltetett eszközökkel kapcsolatban olyan változások következett be, ami a hatósági eljárás során rögzített olyan lényeges akkreditálási paraméter változását jelenti úgy, hogy a kezelt adatok minősítési szintjéhez rendelt biztonsági szint nem csökken.

A híradó-informatikai rendszer lényeges akkreditálási paraméterei:

- állandó telepítésű híradó-informatikai rendszer esetében a biztonsági terület pontos helye;
- kezelt adatok minősítési szintje;
- operációs rendszer típusa;
- biztonsági üzemmód;
- TEMPEST zónabesorolás csökkenése és ehhez kapcsolódóan az eszköz TEMPEST besorolási szint változása;
- engedélyezett adatcsere formája;
- engedélyezett hálózati kapcsolat technikai paraméter és minősítési szint.

Példák az ebbe a kategóriába tartozó változásokra:

- akkreditált eszköz áthelyezése egy másik, azonos vagy magasabb adatkezelési engedéllyel rendelkező helyiségbe;
- a kezelt adatok minősítési szintjének csökkenése;
- akkreditált eszköz ideiglenes áthelyezése egy biztosítási tervben szabályozott ideiglenes biztonsági környezetbe (gyakorlat, konferencia, bemutató);
- a fizikai biztonsági paraméterek változása, mint technikai védelem élőerős védelemmel történő helyettesítése;
- biztonsági üzemmód változása.

Az ebbe a kategóriába tartozó változások nagy valószínűséggel egyszerűsített hatósági eljárással engedélyezhetők, így ezeket az eseteket nem szabad az előző kategóriához sorolni. az ügyek menedzselésére egyszerűsített eljárást kell kialakítani.

Helyi engedélyezéshez kötött változási esetek

A híradó-informatikai rendszerben, vagy az üzemeltetési környezetben beállt olyan változás, ami a minősítési szinthez rendelt biztonsági szint változását nem okozza, és nem tartalmaz lényeges akkreditálási paraméterváltozást. A változtatás oka lehet meghibásodás, vagy felhasználói igény. Példák:

- új alkalmazás telepítése vagy törlése, amely az operációs rendszer biztonsági beállításaira nincs hatással;
- engedélyezett külső kapcsolat ideiglenes megszűnése;
- a rendszer működését vagy biztonságát nem veszélyeztető ideiglenes konfigurációváltozás, mint nyomtató, monitor vagy egyéb periféria ideiglenes lekapcsolása a rendszerről;

- TEMPEST besorolást nem változtató hardvercsere a híradó-informatikai eszközön úgy, hogy az akkreditálási feltételek a hardverelem változásán kívül nem változnak, mint monitor, billentyűzet, számítógép (egyéb aktív elem), merevlemez csere;
- TEMPEST besorolást pozitívan változtató hardvercsere;
- adatkezelés ideiglenes szüneteltetése felhasználói vagy üzemeltetői okokból, mint: az adott szolgáltatásra meghatározott ideig nincs szükség, az adatkezelő helyiségben a minősített adatkezelés szüneteltetése és a szükséges eszközök ideiglenes tárolásba helyezése munkavégzéshez kötötten (meszelés, szerelés, belső építési munkák, amelyek a fizikai biztonsági rendszabályokra nincsenek hatással és a végzett műveletek felügyelete biztosított).

A helyi engedélyezés lényege, hogy az akkreditáláshoz képest történő változás nyomon követhető legyen (mi változott, ki engedélyezte, ki végezte a változtatást és milyen ellenőrzések biztosították a biztonsági szint megőrzését). Az ideiglenes használaton kívül helyezés esetében lényeges annak biztosítása, hogy *ellenőrzés történjen az inaktív időszak kezdetén és végén a nem kívánt jelenségek azonosítása érdekében.*

Ezeknél az eseteknél a helyi nyilvántartási feladatok elvégezhetők, a konfigurációk nyomon követése és a végzett műszaki feladatok rögzíthetők. Az üzemeltető szervezetnek a változtatási művelethez szükséges üzemeltetői tapasztalattal, tudással rendelkeznie kell, így ezekben az esetekben a hatóságnak nincs szüksége a biztonsági szint változásával kapcsolatos mérlegelésre.

A félreértések elkerülése érdekében ennél a résznél érdemes arra is kitérni, hogy mely esetek nem tartoznak a cikk témája szerinti változáskezeléshez. A változáskezelés körétől eltérő feladatok közé tartoznak az akkreditált híradó-informatikai rendszer működési paramétereinek változtatása, mint egyik üzemmódról történő áttérés egy másik üzemmódra (helyi vezérlés-távvezérlés, rejjtelzéssel védett rádióhálóba történő be és kilépés vagy rádióháló üzemmód változás).

Ide sorolandó a rejtjelzés körébe tartozó teszt vagy gyakorló kulcsokkal történő üzemeltetés is, amikor egy eszköz vagy hálózat üzemképességéről kell meggyőződni, vagy a kezelő állomány képzése vagy ellenőrzése történik. Ezek a változások az üzemeltető szervezet illetékes vezetőjének döntését megvalósító feladatok, melyekkel kapcsolatos adatokat az üzemeltetési dokumentumokban kell rögzíteni, de kifejezetten biztonsági szempontból a műveletek nem tekinthetők engedélyezési eljárás alá esőnek.

ÖSSZEGZÉS

A feldolgozott szakirodalomban megfogalmazottak alapján egyértelműen kijelenthető, hogy a Magyar Honvédség szervezeteinél alkalmazott híradó-informatikai rendszerek esetében kidolgozható olyan eljárásrend, melynek segítségével a változáskezeléshez szükséges hatósági ügyintézés támogatható, gyorsítható.

A normál rendű változáskezelési eljárásban megkülönböztethetők azok az esetek, amikor az akkreditáló hatóság szaktudására és engedélyére van szükség, vagy csak adminisztratív típusú ügyintézésre van szükség. Ezen esetek a hatósággal felé felterjeszthetők, a kialakult lista a hatóság által jóváhagyatható. Az így kialakított „Magyar Honvédség elektronikus minősített adatkezelésre vonatkozó változáskezelési eljárásrend” a szabályozási rendbe beilleszthető és minden rendszerre általános érvényű szakutasítás adható ki a kérdés szabályozása érdekében. Új eset megjelenése, vagy a keletkezett tapasztalatok alapján saját vagy hatósági kezdeményezésre a szabályozás nagyobb probléma nélkül továbbfejleszthető.

Az eljárásrendbe természetesen a cikkben megfogalmazott saját hatáskörben szükséges engedélyezési folyamatot is meg kell fogalmazni.

Az elektronikus minősített adatkezelő rendszereket üzemeltető honvédelmi szervezetek egy ilyen központi szabályozással a jelenleginél lényegesen könnyebb helyzetbe kerülnek. *Az adott híradó-informatikai rendszere vonatkozó biztonsági követelmények és üzemeltetés biztonsági szabályzat dokumentumokba a központi követelmény alapján rendszer-specifikusan meg kell fogalmazni a változáskezelési eseteket és már rendelkezésre is áll a szükséges szabályozó.*

Távolabbi lépésként – már a kormányzati szintű szabályozás korszerűsítésére gondolva – *a jelenlegi kormányrendelet felülvizsgálatakor a keretrendszerű követelmény pontosítható ezzel a megoldással*, így a jogszabályt alkalmazó szervezetek is élhetnek azzal a megoldással, hogy szervezeti hierarchiájuk, működési sajátosságuk figyelembe vételével kialakíthatják saját változáskezelési eljárásrendjüket.

Összefoglalásként megállapítható, hogy a bonyolult szervezeti felépítés estén is van lehetőség a változáskezelési feladatok egyszerűsítésére a folyamatok gyorsítására, melynek megoldását testre szabottan a „bevált gyakorlat" alkalmazása és egyéb szakmai forrásokra támaszkodva ki lehet dolgozni. Az engedélyezés ezek alapján már az illetékes hatóság dolga, mely témakör már kívül áll jelen cikk hatókörén.

Felhasznált irodalom

[1] Informatika. Szolgáltatásirányítás; MSZ ISO/IEC 20000-1:2007; 25. p. és 9. 2 fejezet

[2] Information technology - Security techniques - Information security management systems - Requirements; ISO/IEC 27001:2013 (E); A.12 Operations security

[3] NIST Special Publication 800-53 (Revision 4) Security and Privacy Controls for Federal Information Systems and Organizations; appendix F, p. 75.

[4] Australian Information Security Manual 2012 Controls; p. 53-54.

[5] A nemzeti fejlesztési miniszter 77/2013. (XII. 19.) NFM rendelete az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről; 4. melléklet NFM rendelethez; 3. 3. 1. 3 - 3. 3. 1. 5.p.

[6] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól 34. § (1) és 43. § (1).

[7] 39/2014. (05. 30.) HM utasítás a Magyar Honvédség Informatikai Szabályzatának kiadásáról, 1. sz. melléklet, 5. 5. 4, 8. 4. 3. és 8. 4. 4. p.

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Károly Krisztián
krisztian.karoly@mil.hu

LÖVÉSZ ZÁSZLÓALJ KAPCSOLATI RENDSZEREINEK VIZSGÁLATA HÁLÓZATELEMZÉSI MÓDSZEREKKEL 1. RÉSZ

Absztrakt

Korunk információs társadalmának vívmányai komoly kihívások elé állították a haderőt is. A vezetés- szervezés részét képező döntési ciklusok illetve az információfeldolgozás ideje drasztikusan lecsökkent. A hadviselő felek közül az információs uralmat kialakító fél vezetési fölényhez juthat. Ezen új típusú gondolkodásmód hívta életre a hálózat központú hadviselés rendszerét. Mint minden hálózat a katonai hálózatok is jól vizsgálhatók matematikai módszerekkel. A 2000-es éveket követően komoly hálózatelemzési matematikai modellek születtek, amelyek ismeretében kézenfekvő ezen módszerekkel elemezni a Magyar Honvédség alakulatait a hálózat centrikus műveleti térben. Kutatásaimban önhasonló alakzatokat (fraktálszerű képződményeket) és skálafüggetlen hálózatokat keresek egy lövész zászlóalj függelmi kapcsolati rendszerében. Jelen publikáció egy folytatásos cikksorozat első része.

The army also met the modern applications' challenges of the information based society. The dicision cycles and the time of the information management (part of the command & control system) droped off dramatically. The faster powers at war can reach the leadership dominance. This new headgoal made the Network Centric Warfare (NCW) theory. The military networks (similar to the other networks) is analysed well by mathematical methods (e.g. graph theory).
There was a revolution in the network analysis in dawn of 21th century, and it improved this segment of the mathematic. It is necessary to research the forces of the Hungarian Defence Forces with these new methods. I search for fractals and scale-free networks in the order link system and in the information link system of an infantry battalion. This is the first step of a publication series.

Kulcsszavak: *hálózatelemzés, skálafüggetlen, önhasonló hálózatok, hálózat központú hadviselés, híradás ~ network centric warfare, signal, scale-free network, fractal, logical topology*

„A matematikai igazságok rajta vannak az abszolút igazságok listáján, és mi csak felfedezzük azokat.”
Erdős Pál

BEVEZETÉS

Röviddel az ezredforduló előtt az Egyesült Államok hadseregében megalkották a hálózat központú hadviselés (NCW[1]) koncepcióját [1; p. 190.]. Felismerve a modern Információs Technológiákban (IT[2]) rejlő lehetőségeket, az alegységeket, parancsnokokat és törzseket, valamint a szenzorokat hálózatszerűen kívánták összekapcsolni. Gyakran emlegetett elvárásként támasztották, hogy az USA elnöke akár a lövészárokban lévő katonával is összekapcsolható legyen, ezáltal lerövidítve a hálózati csomópontok közötti utat, amely nagyfokú robosztusságot biztosít a hálózatnak. Mindezen rendszert a világ jelenleg egyetlen domináns haderejére optimalizálták [2][3].

A Magyar Honvédség haladva a kor kihívásaival szintén igyekszik kialakítani a maga hálózat központú hadviselési képességét. Ezeket a már említett információs technológiákra, valamint tudatosan kialakított vezetési rendszerre kell építeni. Azonban a rendszer kiépítése során vizsgálni kell a hálózatot, továbbá a kialakítás lépései során időről-időre felül kell vizsgálni, úgynevezett hálózatelemzést kell végrehajtani.

Az NCW modell megalkotását követően, attól függetlenül, civil vonalon Barabási Albert-László és munkatársai 1999-től folyamatosan publikált hálózatelemzési műveikben, alapjaiban változtatták meg a valóságos hálózatokról alkotott képünket. A korábbi Erdős-Rényi modeltől [4; p. 20.] függetlenül bevezették a skálafüggetlen hálózatok fogalmát. Ez új megvilágításba helyezte többek között a különböző társadalmi, szociológiai, gazdasági hálózatokat.

Ezen ismeretek birtokában érdemes ismét megvizsgálni hálózatelemzési módszerekkel a Magyar Honvédséget érintő hálózat központú hadviselési lehetőségeket. A téma nagyságát tekintve szűkítem a lövész zászlóalj kapcsolati rendszereire.

Kutatási célkitűzésem egy általam választott lövész zászlóalj információs-, függelmi-, kapcsolati rendszerének elemzése. Rész kutatási céljaim önhasonló hálózatok (fraktálszerű képződmények), továbbá skálafüggetlen hálózatok keresése. Illetve a kapott eredmények alapján egy ideális híradó hálózatra javaslatot tenni, amely tovább növelné a zászlóalj túlélőképességét az entrópia - alapú hadviselési környezetben.

HÁLÓZAT KÖZPONTÚ HADVISELÉS

A hálózat központú hadviselés gondolatát először Jay Johnson tengernagy említette meg 1997-ben egy az Egyesült Államok Haditengerészeti Intézetében rendezett konferencián, később 1998-ban doktrínába foglalták [1; p. 190.]. Az elmélet lényege, hogy egyszerűsítse a hálózati szenzorok, parancsnokok, és lövészek bonyolult hierarchiáját, csökkentse a műveleti szüneteket, növelje a precizitást és lerövidítse a vezetés időszükségletét.

Az NCW modell alaptételei a következők:

1. A robosztus hálózatok elősegítik az információ megosztást.
2. Az információ megosztás elősegíti az együttműködés kialakítását.
3. A harchelyzet ismeret (SA3) elősegíti a csapatok műveleti összeszinkronizálódását.
4. Ezek az elemek drasztikus arányban növelik a műveletek sikerességét [2][3].

[1] Network Centric Warfare
[2] Information Technologies
[3] Situational Awareness

Az NCW modellel nagyjából egy időben alakult ki az entrópia alapú hadviselés modellje [5][6]. „Az elv szerint az ellenség rendezetlenségét (az entrópiáját) kell megnövelni a kohéziót biztosító szervezeti elemek (személyek, eszközök, objektumok) kiiktatásával addig a szintig, hogy a személyi állomány már ne legyen képes a szervezett ellenállásra.” [1; p. 190.]

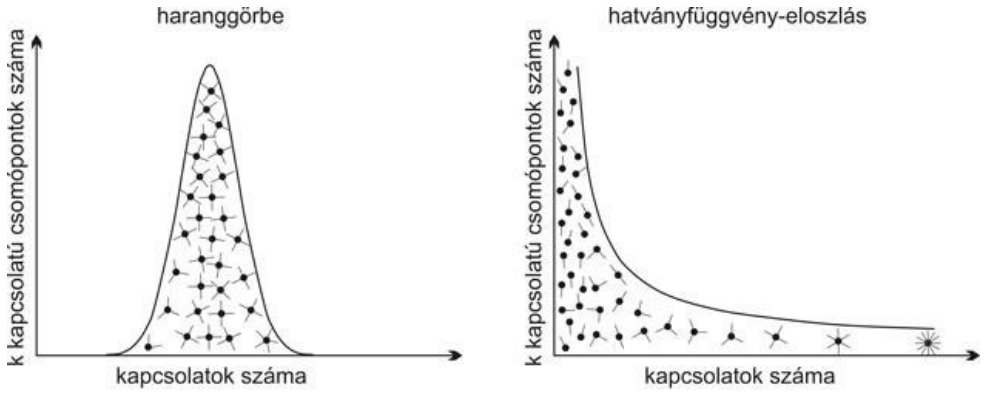
Felmerülhet az olvasóban a kérdés, hogy ezen alaptételek kimondása után miért fontos a Barabási-féle modell vizsgálata a katonai hálózatokban? A válasz egyszerű: Mikor ezek az elméletek születtek, még más volt az általánosan elfogadott kép a valóságos hálózatokról. Barabási és kutatócsapata a skálafüggetlen hálózatok bevezetésével tudományos, matematikai módszerekkel megalapozott választ adtak a valóságos hálózatok viselkedésére, ráadásul a leírt hálózati megoldásokat szélesebb körben tudták alkalmazni, mint a társadalmi hálózatok. Külön érdekesség, hogy a DARPA 1999 őszén kiírt pályázatán, amely „elsődlegesen az új hálózati technológiáknak a fejlesztését tűzte ki célul, amelyek a jövő hálózatai számára lehetővé teszik, hogy a támadások esetén épek maradjanak, és a hálózati szolgáltatásokat fenntartsák” a Barabási- féle kutatócsoportot elutasították, mert akkor még nem értették mi különleges van a skálafüggetlen hálózatokban, pedig nem sokkal előtte hozta le felfedezésüket a rangos Nature című tudományos folyóirat. Azóta tudjuk, hogy a skálafüggetlen hálózatok terén elért sikereik komolyan hozzájárultak a robosztusság, és a hálózatok támadhatóságának vizsgálatában, matematikai modellezésében [4; p. 126.].

HÁLÓZATELEMZÉS MATEMATIKAI MÓDSZEREI

A társadalmi, biológiai, informatikai hálózatok jobb megérthetősége érdekében, célszerű azokat kvantitatív formába önteni, és úgy kezelni. A probléma megoldásához matematikai módszereket hívunk segítségül, mint a diszkrét matematika, a gráfelmélet, fraktálok, matematikai címkézés.

„A hálózat fogalma a hálózattudományban matematikai, ezen belül gráfelméleti alapokra épül. Ennek megfelelően a hálózat csúcsok/csúcspontok (csomópontok) és az ezeket páronként összekapcsoló élek (kapcsolatok) összessége. Az ezzel lényegében megegyező tartalmú gráf fogalom azonban csak a hálózatok legegyszerűbb változatainak leírására alkalmas.” [7; p. 181.] Továbbá meg lehet különböztetni a hálózatokat azok vonalas elrendeződése (pl.: utak, folyók), vagy a csomópontok és az ezek közötti kapcsolatok alapján (pl.: szociális kapcsolatok) [7; p. 181.]. Esetünkben az utóbbi hálózatokkal foglalkozom.

A hálózatok matematikai leírásával először Leonard Euler foglalkozott a Königsbergi hidak problémájában 1736-ban. Ebben fontos alapfogalmakat fektetett le a híres matematikus, melyek az évszázadok során dinamikusan fejlődtek. Eleinte csak a szabályos gráfokat vizsgálták a matematikusok, azonban Erdős Pál és Rényi Alfréd munkássága révén a gyakorlati alkalmazás került előtérbe. Az Erdős-Rényi páros a véletlen hálózatokat vizsgálta, ahol feltételezték, hogy a hálózatok véletlenszerűen kapcsolódnak egymáshoz, így azok fokszámeloszlása normál eloszlást mutat (haranggörbét követ). A következő mérföldkő 1999-ben volt, amikor Barabási Albert-László és Albert Réka felfedezték a skálafüggetlen hálózatokat, amelyek fokszámeloszlása hatványfüggvényt követ (1. ábra). Ezen elméletek, és az alábbi kutatómunka alaposabb megértése érdekében, célszerű néhány alapfogalmat definiálni:



1. ábra. Normál eloszlású és skálafüggetlen hálózatok (hatványfüggvény eloszlású) közötti különbség4

A hálózat egymással összekapcsolt elemek összességéből áll. A legtöbb valós hálózat elemei nem egyszerű pontok (mint a hálózatok matematikai leképezéseinek, a gráfoknak az elemei), hanem maguk is bonyolult hálózatok. Ez azt jelenti, hogy a természetben a hálózatok egymásba ágyazottan fordulnak elő [8]. A hálózatok matematikai elemzésével a gráfelmélet foglalkozik:

A gráf objektumok egy halmazának (csomópontok) és az azok között fennálló kapcsolatoknak (élek) egy absztrakt reprezentációja [9]. Jelölése G(N;k), ahol G: a gráf, N: a csomópontok halmaza, és k⊆NxN az élek halmaza. Amennyiben két csúcsot legfeljebb egy él köt össze, egyszerű gráfról beszélünk. Az olyan gráfot, melynek élein haladva bármely csúcsából bármely másik csúcsába eljuthatunk, összefüggő gráfnak nevezzük [10].

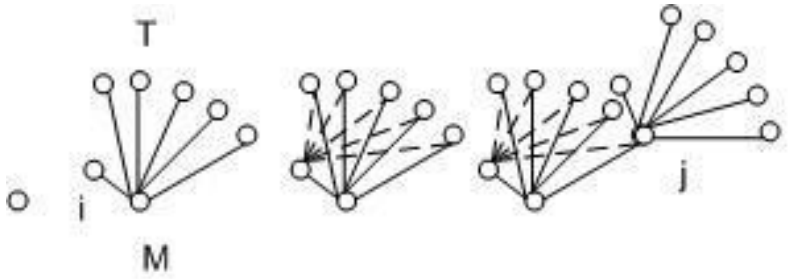
A valós analízis és a topológia megalapozására irányuló vizsgálatok során felfedezték a fraktálokat, melyeknek többféle definícióját is elfogadja a tudományos élet [11]. A következő fogalmak jól körülírják a fraktálokat: A fraktálok olyan önhasonló alakzatok, melyek önhasonló motívumai skálafüggetlen méreteloszlást mutatnak [8]. Egyes megfogalmazások szerint a végtelenségig önhasonló alakzatok [11]. Azonban a természetben előforduló fraktálok (pl.: brokkoli), egyértelműen nem képesek végtelen lépésű önhasonlóságra. Az általam vizsgált társadalmi hálózatok fraktál szempontból végső pontjai az emberek. A Magyar Honvédség jelenlegi maximális létszáma 33 ezer fő, az államigazgatásban pedig mintegy 800 ezren dolgoznak, a Föld lakossága jelenleg valamivel több mint 7 milliárd ember [12]. Azaz a hálózat, amely a fraktált alkotja, nem lehet ennél több elemű. A Csermely Péter-féle hálózat értelmezés alapján, a matematikai absztrakció révén, elvonatkoztathatunk a csomópontok valódi alakjuktól (pl. ember, sejtek, stb.), így kialakulhat egy magasabb indukció.

A hálózat központú hadviselés kutatása során nem újszerű gondolat fraktálokat keresni a hadviselést felépítő komplex hálózatokban. Egy 2000-ben megjelent angolszász tanulmány a frontvonalak fraktál tulajdonságait tanulmányozza. A hadtörténeti adatokat feldolgozó kutatás megállapította, hogy a frontvonalak átlagos fraktáldimenziója D=1,685 [13] [14].

LÖVÉSZ ZÁSZLÓALJ FÜGGELMI KAPCSOLATRENDSZERÉNEK ELEMZÉSE

A katonai szervezet erősen hierarchikus szervezeti keretek között működik. A kis csoportok (rajok, részlegek) élén egy szervezetszerű parancsnok áll. A csoportban van továbbá még egy kitüntetett csúcs ez a parancsnokhelyettes, akinek a csoport tagjai ugyanúgy engedelmességgel tartoznak. Ezt a felépülést a következő gráf mutatja (2. ábra).

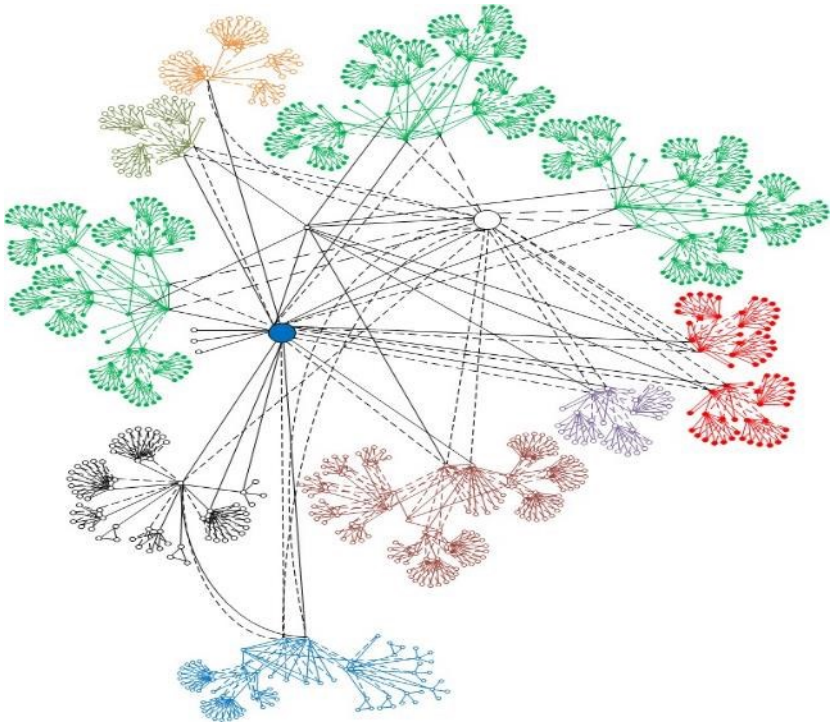
[4] BARABÁSI Albert-László: Behálózva - A hálózatok új tudománya, Helikon Kiadó, 2013. Harmadik kiadás, ISBN 978 963 227 293 1 p. 79.



2. ábra. Függelmi kapcsolatok kialakulásának önhasonló dinamizmusa (szerző)

Gyakorlatilag egy két csomópontú csillag topológia látható, ahol a parancsnok helyettes kapcsolatait szaggatott vonallal jelöltem a megkülönböztethetőség miatt. Ez az elrendeződés a hálózat (zászlóalj) építőkövei, melyek absztrakt felírása egy későbbi kutatómunka része lesz.

Van egy kiinduló csomópont a gráfban, nevezzük M-nek. M-ből kiindul T számú csomóponthoz ugyanannyi számú él, ahol T az alárendeltek számossága, a hozzájuk tartozó élek pedig a parancsnok-beosztott közötti függelmi viszonyt ábrázolják. Egy i csomópont (parancsnokhelyettes) kitüntetett szerepet kap, és egy-egy éllel kapcsolódik a csoport többi tagjához. Harmadik lépésben egy tetszőleges j csomópont azonosan hasonlóan M-hez további hasonló kapcsolatokat épít ki más csomópontokkal (pl.: zászlóaljparancsnok – századparancsnokok – szakaszparancsnokok). Ez a folyamat egy lövészzászlóalj függelmi rendszerében a zászlóaljparancsnoktól kezdve a lövész katonákig négy lépésben zajlik le. A fent leírtak alapján belátható, hogy egy önhasonló hálózatról beszélünk, melyet a következő ábra szemléltet. Azonban ez az önhasonló hálózat önmagában még nem fraktál [11], hisz nem áll fenn, hogy végtelen lépésben önhasonló, de kimondható, hogy fraktálszerű képződményről beszélünk. A fent említett leírás lehetőséget nyújt, hogy magasabb rendű (Magyar Honvédség, államigazgatás), illetve alacsonyabb rendű (emberi szervezet) hálózatokban hasonló önhasonló tulajdonságot keressünk. A fenti leírás alapján belátható, hogy a Magyar Honvédség, és az azt felölelő halmaz a magyar államigazgatás is hasonlóan működik, azaz a zászlóalj önhasonló alakzata egy nagyobb diszkrét elemekből álló önhasonló hálózat (fraktál szerű képződmény) részeleme. Most nézzük meg, hogy teljesül-e a skálafüggetlen felépülés?



3. ábra. Lövész zászlóalj függelmi kapcsolatai (szerző)

A függelmi kapcsolati rendszer megrajzolásával párhuzamosan felírtam a gráf kapcsolati mátrixát, amely egy közel 700X700-as mátrix. A mátrixban két csomópont közötti élek számát beírom a megfelelő helyre (jelenleg maximum 1), ahol pedig nincs kapcsolat oda 0 kerül. A vizsgált gráf több mint 700 csomóponttal, és megközelítőleg 1400 éllel rendelkezik. Azonban, mivel ez egy ritka gráf, amelyben az élek száma sokkal kisebb, mint a csúcsok számának négyzete ($[k]<<[N]^2$), azaz a sűrűsége <<0,5 (számításokat követően ez az érték 0,02), így logikusabb a szomszédsági lista használata, így a mátrix minden egyes csomópontja mellett feltüntetésre kerül a hozzájuk befutó élek száma. Az adatok feldolgozásához Microsoft excel-t használtam.

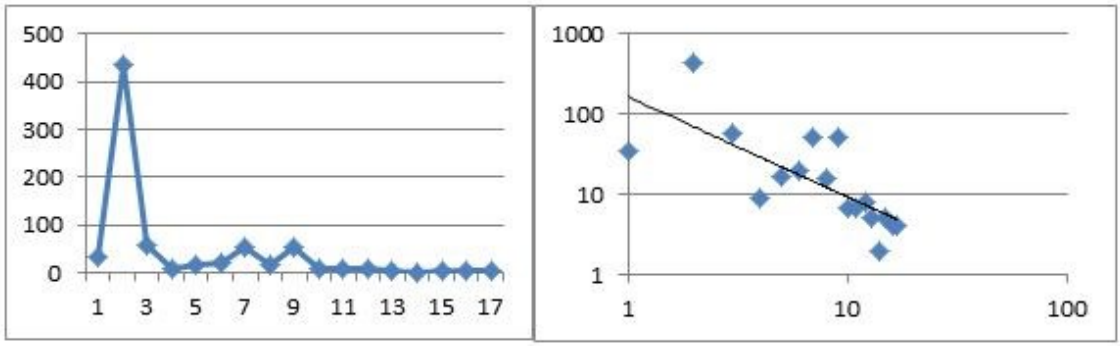
Következő lépésben vizsgáltam a felírt hálózat skálafüggetlenségét. Barabási Albert-László hálózatkutató munkássága alapján, a skálafüggetlen hálózatoknak a következő alapfeltételeknek kell megfelelnie:

1. Növekedés: A hálózatok állandó változására utaló tétel. Az Erdős-Rényi modellel [4; p. 20.] ellentétben, amely statikus, a valóságos hálózatok állandóan változnak. Ennek az állandó változásnak egy pillanata a fenti ábra is. Beosztások jönnek létre, szűnnek meg, esetleg átalakulnak. Az új beosztások mindig egy parancsnokhoz köthetők. Tehát a növekedésként definiált tétel megállja a helyét.
2. Népszerűségi kapcsolódás. Az átalakulás során a csomópontok a függelmi rendszerben egy erősebb csomóponthoz kapcsolódnak (parancsnok).

A skálafüggetlen hálózatok kialakulásához szükséges alapfeltételek teljesültek, azonban a kialakult önhasonló hálózat képét vizsgálva nem látunk sok kapcsolattal rendelkező középpontokat. A skálafüggetlenség kizárásához további méréseket szükséges végrehajtani a hálózaton.

A skálafüggetlen természeti hálózatokban kivétel nélkül megtalálható a Pareto- szabály, más néven a „gazdagabb egyre gazdagabb lesz” [4; pp. 74-90.]. A szabály lényege, hogy az élek 80%-át a gráf csomópontjainak 20%-a birtokolja. Az elvégzett számítások alapján a hálózat 29,5%-a sok kapcsolattal rendelkező vezetők, ezek a pontok azonban csak az élek 62,9%-át birtokolják. Tehát kimondható, hogy a vizsgált gráf a 80-20-as Pareto- szabálynak nem tesz eleget, azonban a 70-30-as Pareto-szabálynak már eleget tesz. Itt érdemes megjegyezni, hogy a skálafüggetlen hálózatoknál definiált alapkövetelmények a 80-20-as szabályt alkalmazzák. A jelentkezett eltérésre az alábbiak adhatnak választ.

Következő lépésben két grafikonon vizsgáltam a fokszámok eloszlását. A skálafüggetlen hálózatokra jellemző, hogy hatványfüggvény eloszlást mutatnak (lásd 1. ábra) [4]. Amennyiben a koordináta rendszer hatványokat megjelenítő koordináta tengelyét dekádos osztással veszem fel, és itt jelenítem meg a függvényt, akkor egy egyenes menti szórást kell mutatnia, melyet az alábbi jobb oldali ábrán egy fekete segédegyenes jelez.



4. ábra. Zászlóalj függelmi kapcsolati rendszerének fokszám eloszlása (szerző)

Az ábrákat tanulmányozva a bal és jobb oldali függvények hatványfüggvény jellegű eloszlást mutatnak, így azok nem feltétlenül elégítik ki a támasztott követelményeket.

Összegezve a fent felsorolt pontokat, megállapítható, hogy a lövész zászlóalj kapcsolati rendszere önhasonló hálózat, azonban a skálafüggetlenség bizonyításával gond van. Hasonló problémával küzdöttek a világ vezető hálózatkutatói 1999 és 2001 között. A megoldás a moduláris hálózat elvében van [4, p.205.]. Térjünk vissza a 2. és a 3. ábrához, ahol a lövész zászlóalj függelmi kapcsolati rendszerét és annak kialakulási dinamikáját ábrázoltam. Ha ezt a hálózatoz úgy tekintem, mint modulokból felépülő hálózatot, akkor könnyen belátható, hogy az egyes modulok skálafüggetlenek. Lehetséges, hogy az egész hálózatra közvetlenül nem alkalmazható a 80-20-as törvény, azonban az egyes modulok eleget tesznek a feltételeknek, azaz kimondható, hogy a lövész zászlóalj egy moduláris skálafüggetlen hálózat, továbbá a Csermely-féle megfogalmazás szerint egy skálafüggetlen önhasonló hálózat (fraktál szerű képződmény). Mint korábban utaltam rá a természeti hálózatok ilyen skálafüggetlen önhasonló fraktálok, melynek jelentősége abban rejlik, hogy azok a szervezetek amelyek, ezen természeti tulajdonságot másolják sokkal ellenállóbbak, vallják a modern kutatások ezrei. Ez kedvező eredmények hozhat az entrópia alapú hadviselési térben.

A moduláris skálafüggetlenség bizonyítását követően vizsgáltam, hogy a hálózat rendelkezik-e a kis világ tulajdonságokkal [4; pp. 48-63.]. A katonai híradásszervezésben nagyon fontos mérőfaktor, hogy hány kézen megy át az információ, mert minden egyes lépés az információ torzulását eredményezi. Hálózatelméleti megközelítésben, minél kevesebb kézfogásra vannak egymástól a csomópontok, annál kevésbé torzul az információ. Természeti modelleket tanulmányozva 2-14 lépés közé teszik a kis világok mérőszámát. Barabási és kutatócsapata kimutatta, hogy a nagy hálózatokban az átlagos összekapcsoltság logaritmikus emelkedést mutat. Kritérium érték a pontonkénti összekapcsoltság 1 körüli legyen. Elfogadva a kis világról alkotott tézist, és figyelembe véve a vizsgált hálózat moduláris skálafüggetlen tulajdonságait, az alábbi összefüggésekkel leírható, és számolható a lövész zászlóalj függelmi kapcsolatrendszerének kis világ tulajdonsága:

$$k^d = N$$

$$d = \frac{lgN}{lgk} = 5{,}23$$

Ahol N a csomópontok száma, k egy pont átlagos kapcsolatainak száma, d pedig a szükséges lépések száma. A számításokat elvégezve 5,23-at kaptam eredményül, azaz átlagosan 6 lépéssel elérhető egy tetszőleges csomóponttól egy másik csomópont. Ezzel bizonyítottam, hogy kis világ tulajdonságokkal rendelkezik a hálózat, mely pozitív az információtorzulás kiküszöbölését tekintve, de ez még nem elegendő. Természetesen függelmi szempontból kevésbé érdekes, hogy két lövész katona a szervezetben milyen távol van egymástól, sokkal érdekesebb, hogy a parancsnokok hány lépésre állnak a beosztottaiktól, és ezt lehet-e csökkenteni? Egy megfelelő hírrendszer alkalmazásával kell e több csomópont (ember) közbeiktatása, vagy lehet közvetlenül az egyénnek feladatot szabni? A 3. ábrát elemezve belátható, hogy a zászlóaljparancsnok maximum 4 lépés távolságra van a lövész katonától, amely nem feltétlenül probléma, hisz nem az ő hatásköre egyes harcos szintre lebontani a harcparancsot, de pozitív az információtorzulás kiküszöböléséhez vezető úton.

Vizsgálva a lövész zászlóalj híradó és informatikai rendszerét, szűkebben a rádióhíradást, látszik, hogy a felépített rendszer leköveti a függelmi kapcsolat rendszereket. Előnye, hogy a parancsnok meg tudja valósítani a parancskiadást, akkor is ha fizikálisan távol van beosztottjaitól, azonban az információáramlás, a szervezés nehézkes lehet ezeken a csatornákon, többnyire a koordinációra korlátozódik. Hálózatkutatók bizonyították, hogy a csillagpontos munkaszervezés lényegesen lassabb a teljes gráf jellegűnél (mindenki mindenkivel kommunikálhat), adott esetben dupla időbe is kerülhet. [15] Ez pedig lényegesen lassítja a vezetési fölény kialakításának menetét [16]. Lehetséges-e olyan rendszer, amely gyorsítani tudja a vezetési fölény kialakítását? Ehhez a publikáció sorozat második részében vizsgálom a lövész zászlóalj információs kapcsolati rendszereit.

SKÁLAFÜGGETLEN FELÉPÜLÉS KÖVETKEZMÉNYEI

Az entrópia alapú hadviselési térben rendkívül fontos adat, hogy a vizsgált hálózat, esetünkben a zászlóalj függelmi kapcsolatrendszere, amely a parancsadási kötelékeket mutatja, milyen hibatűrő képességgel rendelkezik. Fontos momentum, hogy hány csomópontot kell eltávolítani a hálózatból, ahhoz hogy az darabjaira essen?

Egy hálózat csomópontjainak a meghibásodása a hálózatot könnyen széttördelheti elszigetelt egymással nem kommunikáló részekre. Nyilvánvaló, hogy minél több csomópontot távolítunk el a hálózatból, annál nagyobb valószínűsége annak, hogy a hálózat darabjaira essen szét. Régóta ismert tény, hogy néhány véletlenszerűen kiválasztott csomópont eltávolítása alig befolyásolja az összekapcsoltságot. Azonban, ha az eltávolítást folytatjuk, egy bizonyos szám után a gráf apró, egymással nem kommunikáló részekre esik szét, melyet kritikus küszöbértéknek nevezzük. A skálafüggetlen hálózatok meghibásodásai során a kritikus küszöbérték alatt a rendszer alig szenved kárt, ezen érték felett azonban a hálózat egyszerűen szétesik. [17]

Tetszőleges skálafüggetlen hálózatokon végrehajtott kísérletek azt mutatták, hogy a hálózatból véletlenszerűen eltávolítható a csomópontok jelentős része anélkül, hogy a hálózat széttöredezne. Azonban, ha tudatosan támadjuk a hálózatot, és a nagy fokszámmal rendelkező csomópontokat, illetve a modulokat összekötő csomópontokat távolítjuk el a rendszerből a hálózat könnyen fürtökre (cluster) hullik szét. [4, p. 125] Ez egy régóta ismert tény volt katonai tekintetben, a parancsnokok likvidálásával megnövekszik az alegység entrópiája. A skálafüggetlen hálózatok bevezetésével, azonban megjelent ennek egy matematikai modellezési lehetősége. Ugyanakkor a kimutatták azt is, hogy ezen csomópontok javítása (pótlása) során egy bizonyos mértékig fenntartható a hálózat robosztussága, azonban egy másik küszöbérték elérésekor lavinaszerűen omlik össze a hálózat apró darabokra. Gyakorlatban a likvidált parancsnokok helyére a szervezetszerű parancsnokhelyettesek lépnek be. Amikor elfogynak ezek a lehetőségek, és az utódlás rendszerében zavar áll be, a hálózat entrópiája drasztikusan megnő, és nem fürtökre, hanem apró darabokra hullik szét (rajok, kezelőszemélyzetek gyakran vezetés nélkül).

ÖSSZEGZÉS

A XX. század végén a hadviselés klasszikus dimenziói (szárazföld, tengerek, levegő, űr) egy újabb szegmenssel, az információs dimenzióval bővült. Toffler szavaival élve korunk „harmadik hullámú háborúit” alapjában határozza meg az információ feldolgozásának gyorsasága, jutatva ezzel a hadviselő feleket az információs fölény, az információs uralom, végső soron a vezetési fölény kialakításához [18]. Ezen új kihívásokra adott válaszul új vezetési koncepciók alakultak ki, mint például a hálózat központú hadviselés modellje.

Kutatásomban vizsgáltam egy lövész zászlóalj függelmi kapcsolat rendszerét matematikai módszerekkel. Az elvégzett mérések összegzéseként megállapítottam, hogy a hálózat skálafüggetlen tulajdonságokkal rendelkezik. Az irodalomkutatást követően összegeztem a skálafüggetlen hálózatok tulajdonságait rámutatva ezáltal a vizsgált hálózat sebezhetőségi tulajdonságaira. Kutatásaim során a függelmi rendszerben olyan önhasonló elemeket találtam, amelyek fraktálszerű képződmények.

Ezen kutatási eredmények megkönnyítik a számítógépes modellezés lehetőségét, és a hálózat robosztusságának illetve sérülékenységének megértését a hálózat központú és a entrópia alapú hadviselési térben.

Felhasznált irodalom

[1] Kun István, Fáy Gyula, Bukovics István: Logikai hadviselés – pontok harca, Hadmérnök, VI. évfolyam 4. szám – 2011. december

[2] United States Army (2003). Mission Command: Command and Control of Army Forces. Washington, D.C.: Headquarters, United States Department of the Army, Field Manual No. 6-0.

[3] United States Marine Corps (1996). Command and Control. Washington, D.C.: Department of the Navy, Headquarters, United States Marine Corps, Doctrine Publication MCDP 6.

[4] Barabási Albert-László: Behálózva - A hálózatok új tudománya, Helikon Kiadó, 2013. Harmadik kiadás, ISBN 978 963 227 293 1

[5] Arquilla, J. – Ronfeldt, D.F. (1995): Information, Power, and Grand Strategy (unpublished) Santa Monica: The RAND Corporation, July 1995, p. 19.

[6] Herman, Mark (1997): Entropy-based warfare: A unified theory for modeling the Revolution in Military Affairs, Booze, Allen and Hamilton Inc, 1997.

[7] Munk Sándor: Hálózatok fogalma, alapjai, Hadmérnök, V. évfolyam, 3. szám – 2010. szeptember, ISSN 1788-1919

[8] Csermely Péter: Hálózatok sejtjeinkben és körülöttünk, Mindentudás Egyeteme 2.0, 2005. 09.12 http://mindentudas.hu/elodasok-cikkek/item/113-h%C3%A1l%C3%B3zatok-sejtjeinkben-%C3%A9s-k%C3%B6r%C3%BCl%C3%B6tt%C3%BCnk.html, 2014. április 15.

[9] MUNK Sándor: Operációkutatás 1-2. ppt előadás, ZMNE

[10] Vicsek Tamás: Munkahelyi hálózatok, Mindentudás Egyeteme 2.0, 2008.02.02. http://mindentudas.hu/elodasok-cikkek/item/168-munkahelyi-h%C3%A1l%C3%B3zatok.html, 2014. április 15.

[11] Molnár Katalin: Lindenmayer-rendszerek a középiskolában, ELTE TTK Budapest 2010.

[12] 35/2013. (V.16.) OGY határozat a Magyar Honvédség részletes bontású létszámáról valamint https://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_qli010.html, 2014. április 27.

[13] Lauren M. K.: Modelling Combat Using Fractals and the Statistics of Scaling Systems. Military Operation Research. (2000.) 5 No. 3. pp. 47-58.

[14] James Moffat: Complexity Theory and Network Centric Warfare. CCRP publication Series. 2010. ISBN 1-893723-11-9 www.dodccrp.org, 2014. április 27.

[15] Behálózva (televízió sorozat) Spektrum, 2013.

[16] HAIG Zsolt: Információs műveletek, SIGINT és EW kapcsolatrendszere. Felderítő Szemle, Budapest, Magyar Köztársaság Felderítő Hivatala. VI. évf. Különszám, 2007. február. ISSN 1588-242X pp. 27-48.

[17] BARABÁSI Albert-László: A hálózatok csodálatos világa a sejtektől a világhálóig, 2005. 10.10. Mindentudás Egyeteme v.2.0 http://mindentudas.hu/elodasok-cikkek/item/117-beh%C3%A1l%C3%B3zva-a-h%C3%A1l%C3%B3zatok-csod%C3%A1latos-vil%C3%A1ga-a-sejtekt%C5%91l-a-vil%C3%A1gh%C3%A1l%C3%B3ig.html; 2014. május 6.

[18] Alvin TOFFLER: A harmadik hullám. Typotex Kiadó, ISBN 978-963-9326-21-7, 1980.

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Kovács Zoltán
zkovacs@nbsz.gov.hu

HORDOZHATÓ INFOKOMMUNIKÁCIÓS ESZKÖZÖK HASZNÁLATÁHOZ KAPCSOLÓDÓ BIZTONSÁGTUDATOSSÁGI KÉPZÉSI TEMATIKA VÉDETT VEZETŐK SZÁMÁRA

Absztrakt

A védett vezetők mindennapi tevékenységéhez szorosan hozzátartozik a kommunikáció, és az ezekhez szükséges hordozható infokommunikációs eszközök (pl. okostelefon) használata. Védelmüket ezen a területen is biztosítani kell, hiszen ők mindig is kiemelt célpontjai voltak az információszerző támadásoknak. A védelem egyik legolcsóbb és leghatásosabb módja a biztonságtudatos használat, amelyre a védett vezetőket fel lehet készíteni. A "Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából" című cikksorozat áttekintette a védett vezetők információbiztonsági védelmének főbb kérdéseit, és összefoglalta az említett eszközök és szolgáltatások használata során jelentkező veszélyeket. Jelen cikk pontosítja a személyre szabott oktatás keretrendszerét, majd felállítja egy lehetséges, az említett eszközök és szolgáltatások használatára vonatkozó biztonságtudatossági alapképzés tematikáját.

The communication and the use of portable infocommunication devices (e.g. smartphone) form an inherent part of the everyday activities of protected leaders. Their protection has to be provided in that field as well, because they have always been emphasised targets of attacks of unauthorized access for information. One of the most cost efficient and effective means of protection is the security awareness which the protected leaders can be trained for. The article series titled "The Risks of Using Portable Infocommunication Devices in Terms of Security Awareness Training for Protected Leaders" reviews the main issues of data security of protected leaders and summarizes the threats appearing while using the above mentioned devices and services. This article assigns the framework of the personalized training and establishes a possible theme of a basic security awareness training concerning the use of the devices and services mentioned above.

Kulcsszavak: *védett vezető, hordozható infokommunikációs eszközök, internet-technológián alapuló szolgáltatások, biztonságtudatossági képzés ~ protected leader, portable infocommunication device, Internet Based Services, security awareness training*

BEVEZETÉS

A védett vezetők mindennapi tevékenységéhez szorosan hozzátartozik a kommunikáció, és az ezekhez szükséges hordozható infokommunikációs eszközök (pl. okostelefon, táblagép, hordozható számítógép) használata. Gyorsan, egyszerűen, és nem utolsó sorban olcsón akarnak beszélni másokkal, adatokat, információkat elérni, cserélni, továbbítani. Sokszor mindezt úgy, hogy az érzékeny információkat csak az a néhány ember ismerhesse meg, akinek feltétlenül szükséges, az általuk közétenni kívánt információkhoz viszont az emberek széles köre is gyorsan, egyszerűen hozzáférhessen. Ez utóbbihoz sok esetben mindenki által elérhető, sokszor ingyenes internet-technológiára épülő szolgáltatásokat használnak fel, vagy kívánnak felhasználni. Ráadásul a hivatali-, és magánjellegű kommunikációt, az érzékeny és a széles körnek szánt információk továbbítását lehetőleg egyazon eszköz segítségével kívánják lebonyolítani. Ez azonban jelentős veszélyeket rejt magában.

Az elektronikus úton folytatott kommunikációs és adattovábbítási lehetőségek, az internet-technológiára épülő, ezen belül is a felhő alapú szolgáltatások rohamos fejlődése új, korábban nem ismert kihívások elé állította/állítja az illetékeseket, döntéshozókat és a szakembereket egyaránt. A kibertérben ma minden felhasználót veszélyek egész sora fenyegeti, a kiberbűnözéstől az idegen titkosszolgálatok adatszerző tevékenységéig. Fokozottan igaz ez a védett vezetőkre, akik mindig is kiemelt célpontjai voltak az információszerző támadásoknak. Ráadásul külön problémakánt jelentkezik, hogy a védett személyek által használt eszközök – hordozhatóságuk és személyhez rendeltségük okán – általában vegyes felhasználásúak, azaz hivatali és magán célokat egyaránt szolgálnak.

Éppen ezért fontos megvizsgálni, hogy mit is tehetünk a védett vezetők információinak – azon belül is legfőképpen elektronikus információinak – megvédése, biztonságának garantálása érdekében. Az internet-technológiára épülő szolgáltatások, és a személyi használatú hordozható infokommunikációs eszközök esetében a védekezés egyik leghatékonyabb módszere biztonságtudatos használata. A védelemre fordítható összegek ugyanis korlátozottak, ráadásul a megfelelő biztonság technikailag sokszor nem, vagy csak irreálisan magas költségek mellett lenne a megfelelő szinten kialakítható.

A biztonságtudatos használatra fel lehet készíteni a védett vezetőket. Ehhez érdemes egy személyükre szabott, általános jellemzőiket figyelembe vevő oktatási tematikát kidolgozni. A "Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából" című cikksorozat első része áttekintette a védett vezetők információbiztonsági védelmének főbb kérdéseit, körülhatárolta a veszélyek szempontjából vizsgálandó személyi használatú hordozható infokommunikációs eszközöket, valamint internet-technológiára épülő szolgáltatásokat, majd számba vette az elemezendő biztonsági kategóriákat. A második rész az elsőben megadott kritériumok alapján összefoglalta az említett eszközök és szolgáltatások használata során jelentkező veszélyeket. Ez pedig már megfelelő alapot teremt az oktatási tematika kidolgozásához.

Jelen cikkben a "Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából" című cikksorozatban leírtak, valamint saját tapasztalataim alapján fogalmazom meg gondolataimat a témáról.

A SZEMÉLYRE SZABÁS KERETRENDSZERE

A védett vezetők személyre szabott oktatási tematikája kidolgozásának egyik alapfeltétele tehát a lehetséges veszélyek felmérése. Ez a "Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából" [1] [2] című cikksorozatban megtalálható. A másik alapfeltétel a személyre szabáshoz a védett vezetők speciális helyzetének felmérése. Figyelembe kell venni ugyanis az élethelyzetükből,

munkájukból, elfoglaltságukból adódó feltételeket, amelyek egyfajta keretrendszert, feltételrendszert képzenek az oktatási tematikához.

Bár kifejezetten a védett vezetők felhasználói szokásairól nem készült felmérés a személyi használatú hordozható infokommunikációs eszközök, valamint az internet-technológiára épülő szolgáltatások használata kapcsán, ám a normál felhasználói szokásokból lehet általánosítani és ide vonatkozó következtetéseket levonni.

A figyelembe veendő feltevések, megállapítások a következőek:

- Használnak személyi infokommunikációs eszközöket.
- Az első egy értelemszerű, de fontos megállapítás.
- Hordozzák ezeket az eszközöket.

Szintén értelemszerű megállapítás, ám fontos tényező a kialakítandó biztonság szempontjából. Az eszközök hordozása ugyanis olyan plusz kockázatokat rejt, amelyeket már érdemes, vagy inkább be kell építeni a biztonságtudatos képzésbe. Ilyenek lehetnek a "Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából" [1] című cikksorozatban megtalálható veszélyek, mint például az eszközök felügyelete, mások általi hozzáférése, kapcsolódás más hálózatokhoz, stb.

Az eszközök jórészt normál kereskedelmi forgalomból származó, kommersz eszközök. Ez azt jelenti, hogy ezek jellemzően nem rendelkezik egyéni biztonsági funkcióval, ha igen azok is más országok által gyártottak. Ugyanakkor a világméretű elterjedtség, ismertség okán számos ismert sebezhetőséget, valamint akár a gyártó által beépített, esetleg ki is használt, információszivárgást okozó „funkciót" is tartalmaznak.

Vegyes (részben magán, részben hivatali) jellegű használat a jellemző. A személyi használatú, hordozható infokommunikációs eszközöket a védett vezetők általában hivatalból kapják, de – teljesen szabályos módon – magáncélra is használják, használhatják. Ez nem azonban nem csak a kommunikáció tartalma miatt, hanem a felhasznált internet-technológiára épülő szolgáltatások, ezáltal a készülékek ellenőrzése és a biztonságtudatossági képzés tartalma okán is figyelembe veendő tény. De éppen ezért az ellenőrzéshez és a biztonságtudatossági képzéshez is egészen más lehet a védett vezetők hozzáállása, mint egy tisztán hivatali célra igénybevett eszköz esetén.

Mások (pl. családtagok) is hozzáférhetnek az eszközökhöz, sőt használhatják is azokat. A magánjellegű használatból eredő kockázatot fokozza ez a kitétel, hiszen az eszközök egy részénél nehezen, vagy egyáltalán nem megvalósítható a jogosultságkezelés, a családtagok letölthetnek, telepíthetnek alkalmazásokat, esetleg véletlenül is feltölthetnek fájlokat. Ez pedig olyan, amelynek kockázatait, és azok csökkentésének lehetőségeit szintén ismertetni kell a képzés során.

Iskolai végzettségük (diplomáik szakterületei) óriási szórást mutat (pl. közgazdász, jogász, agrármérnök, stb.) A képzés kialakítása szempontjából ez egy meghatározó tényező, hiszen mindenki számára érthetően, sőt a későbbiekben alkalmazható módon kell az oktatást kialakítani.

Jellemzően nem mély számítástechnikai, informatikai, kommunikációs és információbiztonsági ismeretekkel rendelkeznek, sőt ez a tudás csekélynek tekinthető. Az előző ponthoz szorosan kapcsolódó, de az oktatás kialakítására nézve önállóan is fontos megállapítás.

Jellemzően az érdeklődés a normál használat iránt is vegyes. A védett vezetők egy része szereti „nyomkodni a telefonját, táblagépét", más részük normál felhasználónak tekinthető, míg vannak köztük olyanok is, akik csak akkor használják, amikor feltétlenül szükséges. Ez hatással van a felhasználói ismeretekre, de a védendő információk mennyiségére is.

A "megszokott" felhasználási módokat keresik, a biztonságosabb használat miatti korlátozásokat, nehezen fogadják el. Minden olyan elem, amely a biztonságot emeli, várhatóan

korlátozza a felhasználót és/vagy nehezíti a használatot. Ezt pedig akárcsak az „átlagfelhasználók" általában, a védett vezetők is nehezen fogadják, viselik el.

Bonyolult azonosítási, felhasználási eljárások a védett vezetőket elriasztják a használattól, vagy keresik az elkerülő lehetőségeket. Adott esetben a magasabb biztonsággal járó, bonyolultabb azonosítási eljárások okozta kényelmetlenségek ilyen reakciókat is kiválthatnak a védett vezetőkből. Ennek megelőzésében nem csupán az eljárások gondos megválogatása, hanem a biztonságtudatos képzés is sokat segíthet.

Egy részük szereti, sőt akár presztízskérdésnek fogja fel az új mobil infokommunikációs eszközök birtoklását. Az új eszközök új technikai lehetőségeket, ezáltal új biztonsági előnyöket és kockázatokat egyaránt jelentenek. Az oktatásnak figyelembe kell vennie, és a lehetőségekhez mérten fel kell készítenie a védett vezetőt egy új készülék használatából adódó biztonsági kockázatokra és lehetőségekre.

Számolni kell a személyes infokommunikációs eszközök elvesztésével, ellopásával. Az oktatás során ki kell térni az ebből adódó kockázatokra, valamint azok csökkentésére vonatkozó lehetséges ellenlépésekre is. Tudatosítani kell, hogy mi a felhasználó feladata és felelőssége, és mi az rendszergazdáké.

Jellemzően rendelkeznek közösségi oldalon, oldalakon profillal, és azt, azokat aktívan használják is. A közösségi oldalakkal kapcsolatos veszélyek részint tartalmazzák az egyéb internet-technológiára épülő szolgáltatásokkal kapcsolatos kockázatokat, ugyanakkor máshol nem, vagy legalábbis nem ilyen formában jelentkező veszélyeket is. Az oktatás során ezekre is fel kell hívni a figyelmet.

Jellemzően használnak egyéb felhő alapú szolgáltatásokat levelezésre, adattárolásra stb. (pl. gmail, dropbox). A közösségi oldalak mellett a felhő alapú rendszerek használata is rejt speciális, csak ezekre jellemző veszélyeket. Ezekre a jellegzetes problémákkal, kockázatokkal ugyanúgy foglalkozni kell az oktatás során, mint a közösségi oldalak esetében.

Jellemzően töltenek le és telepítenek újabb alkalmazásokat eszközeikre. Ma már a legegyszerűbb alkalmazások is szinte minden esetben teljes hozzáférést kének adatainkhoz, telefonkönyvünkhöz, pozíciónkhoz stb. A szerződés elfogadásával pedig a felhasználó saját maga járul hozzá ezek átadásához. Ráadásul, mint minden szoftver, ezek is tartalmaznak, tartalmazhatnak olyan sérülékenységeket, netán tudatosan beépített hátsó kapukat, amelyet kihasználva a támadók szintén hozzáférhetnek a felhasználó minden adatához. A biztonságtudatos használat egyik alappillére, hogy a védett vezető ezekkel a kockázatokkal is tisztában legyen.

Jellemzően a letöltött és telepített alkalmazások egy része, vagy akár egésze ingyenes. A fentiek kiemelten igazak abban az esetben, ha a kiválasztott alkalmazás ingyenes. Ekkor ugyanis jóval több hozzáférést kell engedélyezni a szerződés elfogadásakor, mint fizetős társaiknál. Különösen jól megfigyelhető ez azoknál a szoftvereknél, ahol fizetős és ingyenes verzió is létezik ugyanabból a verzióból.

Jellemzően kevés idővel rendelkeznek, amelyet oktatásra, biztonságtudatosság növelésére lehet fordítani. Lényeges szempont a tematika összeállításánál egy időkorlát meghatározása. Ez természetesen nemcsak azt is jelenti, hogy nem csak a képzés anyagát kell nagyon gondosan megválogatni és tömören, de érthetően előadni, hanem azt is, hogy az összeállított tematika egyfajta alapképzés lehet, amelyet a későbbiekben lehetőség és igény szerint további, akár hosszabb oktatásokkal kell kiegészíteni.

Az információbiztonság fontos számukra. Szintén egyértelmű tény, hogy a védett vezetők tisztában vannak azzal, hogy sokszor kezelnek érzékeny információkat, amelyek megvédése fontos számukra. Ezáltal fogékonyabbnak tekinthetők az információbiztonság területén jelentkező problémák megértésére, mint az „átlagfelhasználó". Ennek elősegítésére érdemes olyan példákat hozni az oktatásban, amely ismert, éppen ezért az információszerzés miatt kiemelt személyekkel kapcsolatosan mutat rá a lehetséges veszélyekre.

A védett vezetőknél technikai elhárítás is segíti az információbiztonságot. A védett vezetőknél az információbiztonság teljes körű garantálásának érdekében rendszeresen tartanak technikai elhárítást is. A "Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából" [1] című cikksorozatban megtalálható a technikai elhárítás kiterjesztett értelmezése. Az ebben megfogalmazottak szerint ennek ki kell terjednie a védett vezetők hordozható infokommunikációs eszközeire is. Ez pedig nagyobb fokú biztonságot garantál, amelyet meg kell ismertetni a védett vezetőkkel is.

OKTATÁSI TEMATIKA

Az említett cikksorozatban feltárt veszélyeket, valamint a fenti feltételeket és feltevéseket figyelembe véve már kidolgozható az védett vezetők számára a személyükre szabott oktatási tematika.

A fent leírtak alapján a védett vezetőknek szóló, a személyi használatú hordozható infokommunikációs eszközök, valamint internet-technológiára épülő szolgáltatások igénybevétele kapcsán jelentkező biztonságtudatos használatának alapképzési tematikájánál a következőkből célszerű kiindulni:

- A képzést célszerű a – kiterjesztett értelemben vett és végrehajtott – technikai elhárítással összekötni, azzal párhuzamosan végrehajtani. Ekkor ugyanis átvizsgálásra kerülnek a védett vezető eszközei, és feltérképezésre kerülnek az esetleges információszivárgási csatornák, lehetséges információbiztonsági veszélyek.
- Az oktatás megtartását célszerű a technikai elhárítást végző szervre bízni. Itt ugyanis a megfelelő időben rendelkezésre állnak a megfelelő ismerettel rendelkező szakemberek.
- Az alapképzés időtartamát célszerű körülbelül 60 percben meghatározni. Ennél több, egyedi oktatásban az alapképzésre fordítható ideje a védett vezetőknek várhatóan nem lesz több, ennyi viszont feltétlenül szükséges a megfelelő információ átadásához.

Mindent egybevetve a következő tematika alapján célszerű elvégezni az oktatást:

Oktatási cél: Az oktatás keretében a védett vezető ismerje meg a személyi használatú hordozható infokommunikációs eszközök, valamint internet-technológiára épülő szolgáltatások igénybevétele kapcsán jelentkező veszélyeket, azok elhárítása, vagy legalábbis csökkentése érdekében általa elvégzendő teendőket, a biztonságtudatos használatot.

Elvárt eredmények:

A védett vezető:

- megértse a veszélyeket és elfogadja a biztonság fontosságát,
- megértse és elfogadja a technikai elhárítás keretein belül a személyi használatú hordozható infokommunikációs eszközeinek vizsgálatát,
- megértse egy hosszabb idejű képzés fontosságát, a részvételhez érdeklődéssel és készségesen álljon hozzá,
- támogassa az oktatás és a vizsgálat kiterjesztését közvetlen munkatársaira és családtagjaira,
- az általa használt személyi használatú hordozható infokommunikációs eszközeit, valamint internet-technológiára épülő szolgáltatások a képzést követően a korábbiaknál sokkal nagyobb biztonságtudatossággal legyen képes használni.

Tematika:

1.	Veszélyek bemutatása példákkal
	a. Illetéktelen hozzáférés, lehallgatás
	i. Snowden ügy tanulságai,
	ii. Egy pénzlopás ügy rövid bemutatása,
	iii. Egy híres ember adatait illetéktelenül megszerzésének és felhasználásának esete rövid bemutatása
	b. Másodlagos adatok fontossága
	i. OSINT bemutatása, példával,
	ii. Helymeghatározás bemutatása, példával
	c. Adatvesztés bemutatása - Cryptolocker példa
	d. Nem valós adatfeltöltés, lejáratás bemutatása, példával
2.	Biztonság megteremtésének módjai, beállítások, biztonságtudatos használat
	a. Üzembiztonsághoz kapcsolódó lehetőségek
	i. Felhő alapú rendszerek – szerződés elfogadás/elutasítás
	ii. Eszköz - biztonsági mentés
	b. Egyéb biztonsághoz kapcsolódó lehetőségek
	i. Jogi lehetőségek - korlátozott lehetőségek bemutatása
	ii. Fizikai védelem - tudatos viselkedés bemutatása, példákkal
	c. Adatbiztonsághoz kapcsolódó lehetőségek
	i. Adatkészítés - biztonságos környezet kérdésköre
	1. Frissítések fontosságának bemutatása
	2. Minimalizált szoftverkörnyezet fontosságának bemutatása
	3. Új szoftvertelepítések elkerülésének fontossága
	4. Biztonsági szoftverek naprakészen tartásának fontossága
	5. Felhasználók kezelése, jogosultságok fontossága
	ii. Adattovábbítás kérdésköre
	1. Kapcsolódó(tt) hálózatok veszélyei, beleértve a hardveres eszközöket pl. BT billentyűzet is
	2. Távoli, passzív lehallgatás veszélyei
	3. Titkosítás fontosságai, korlátai
	iii. Bejelentkezés, adatmegadás, jelszó kérdésköre
	iv. Törlés, megsemmisítés, fióktörlés kérdésköre
	v. Social engineering veszélyei
3.	Ellenőrzés lehetőségei, fontossága
4.	Összefoglalás, kérdések

Ütemezés:

A technikai elhárítás alkalmával, kb. 60 perc időtartamban.

Irodalom és további információk:

- Az oktatók által elkészített 2-3 oldalas anyag, a személyi használatú hordozható infokommunikációs eszközök, valamint internet-technológiára épülő szolgáltatások biztonságtudatos használatához szükséges legfontosabb információkkal.
- Az oktatók által elkészített 2-3 oldalas anyag, a személyi használatú hordozható infokommunikációs eszközök biztonságtudatos használatához szükséges legfontosabb beállításokkal kapcsolatos információkkal.
- Az oktatók által elkészített rövid, 10-15 perces flash animáció, a személyi használatú hordozható infokommunikációs eszközök biztonságtudatos használatához szükséges legfontosabb beállításokkal kapcsolatos információkkal.
- Egy kontaktszemély adatainak átadása, akit a későbbiekben felmerülő kérdésekkel akár telefonon, akár e-mailben megkereshet.

A tematika alapján a tényleges, teljes ismeretanyag kidolgozása, annak napra készen tartása már a képzést tartó szervezet szakembereinek, vezetőinek a feladata.

A TOVÁBBLÉPÉS LEHETŐSÉGEI

Az oktatási tematika természetesen csak az első lépés a védett vezetők információbiztonságának minél magasabb szintű megteremtéséhez a személyi használatú hordozható infokommunikációs eszközök, valamint internet-technológiára épülő szolgáltatások használata során. Bár nyilvánvalóan 100 %-os védelmet nem lehet kialakítani, de mindenképpen törekedni kell rá. A jelen, valamint a korábban már hivatkozott „Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából I.-II.” című cikkből kiolvasható, hogy a felvázolt oktatási tematika tartalommal való megtöltése, és az oktatás végrehajtása mellett is vannak további feladatok, amelyek végrehajtásával a biztonsági szint tovább emelhető.

Ezek közül az első csoportba azok a feladatok tartoznak, amelyek minden, a cikkekben említett szereplőkön (védett vezető, technikai elhárítók, helyi biztonsági vezető, rendszergazdák) túlmutató, magasabb szintű megközelítést igényelnek. Ilyen például a megfelelő jogszabályi háttér kialakítása, átalakítása, ezen belül pedig bizonyos biztonsági elemek kötelezővé tétele. Ilyen kötelező elem lehet(ne) a kiterjesztett értelemben vett technikai elhárítás előírása bizonyos vezetői szintig, meghatározott biztonságtudatossági oktatáson való kötelező részvétel, vagy a hordozható infokommunikációs eszközök esetében, azok teljes életciklusára (fejlesztés, beszerzés, rendszerbe állítás, használat, kivonás stb.) vonatkoztatva kötelező biztonsági előírások kialakítása, betartatása, és hatósági ellenőrzése. Szintén a jogszabályi háttér kialakításakor kell gondolni a védett vezetők környezetben lévő személyekre, a technikai elhárítás rájuk történő kiterjesztésére is (pl. családtagok, közvetlen munkatársak, titkárság stb.). Ez azért is fontos, mert sokszor ők is kezelik a védett vezetőhöz kapcsolódó információkat, így az érzékeny adatok szivárgását náluk is meg kell előzni, akadályozni.

De ugyan ebbe a csoportba tartozik a védett vezetők felhasználási szokásainak felmérése is. Ilyen célzott felmérés ugyanis még nem készült, márpedig ez segítheti a specifikus kockázatelemzést. Bár jelen cikkben említett alap biztonságtudatossági képzéshez ez nem elengedhetetlenül szükséges, a hosszabb, például 1 napos képzések tematikájának kialakításában, valamint a szükséges biztonsági szintek meghatározásában nagy segítséget nyújthat. A felmérés során választ kell kapni azokra a kérdésekre, hogy ki, milyen személyi használatú hordozható infokommunikációs eszközöket, valamint internet-technológiára épülő szolgáltatásokat használ, és azokat mikor, hol, hogyan és mire. A felmérés természetesen – a lehetőségekhez mérten – lehet anonim, a „ki” kérdésnél sokkal érdekesebb a vezetési szint. Elsősorban azért, hogy meg lehessen állapítani, van-e statisztikailag is kimutatható markáns különbség az egyes vezetési szinteken lévő vezetők felhasználói szokásaiban.

A második csoportba a védett vezető által megtehető további feladatok tartoznak. Ilyen lehet a korábban említett, további hosszabb biztonságtudatossági képzésen való önkéntes részvétel, az önképzés, az egyéb lehetőségek, például konzultációs lehetőségek kiaknázása a biztonsági szakemberekkel, vagy a kiterjesztett értelemben vett technikai elhárítás aktív, segítő támogatása.

A harmadik csoportba sorolhatóak az eszközök üzemeltetéséért, biztonságáért permanensen felelős helyi biztonsági vezető, a rendszergazda és munkatársaik feladatai. Ide tartoznak a felhasználási előírások megalkotása, betartatása, a meghajtó programok és a feltelepített alkalmazások naprakészen tartása, az eszközök biztonságos működéséhez szükséges beállítások megtétele, ismert, de javítatlan biztonsági rések esetén az adott szoftver esetleges cseréje hasonló tudásúra, a felesleges, ezáltal biztonsági kockázatot jelentő szoftverek

eltávolítása, az incidensek kivizsgálását elősegítő alkalmazások telepítése, beállítások megtétele.

A negyedik csoportba sorolható további feladatok a technikai elhárításért felelős szervezetek felelősségi körébe tartoznak. Míg a helyi szervezetek feladata a permanens biztonság megteremtése, addig a technikai elhárítóké egy mélyebb biztonsági pillanatkép felvétele. Ebbe beletartozik a helyiségek mellett a hordozható infokommunikációs eszközök átvizsgálási metodikájának kidolgozása, majd gyakorlati megvalósítása, helyi előírások áttekintése, azok megvalósításának ellenőrzése, az eszközök speciális – hardver sebezhetőségi, kémszoftverek elleni – vizsgálata. Szintén ide sorolható a védett vezetők által leggyakrabban használt internet-technológiára épülő szolgáltatások, ezen belül is a felhő alapú rendszerek folyamatos vizsgálata, majd ezek alapján a védett vezető figyelmének felhívása az általa használt rendszerek ismert sérülékenységeire, kockázataira.

A feladatok részletes kibontása és az egyes szereplők közötti megosztása azonban már túlmutat jelen cikk keretein, az egy későbbi feladat.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

Jelen cikk összefoglalta a védett vezetők személyi használatú hordozható infokommunikációs eszközei, valamint internet-technológiára épülő szolgáltatások használata kapcsán felmerülő biztonságtudatossági alapképzés keretfeltételeit, figyelembe véve a védett vezetők speciális helyzetét. Erre, valamint a „Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából” című cikksorozatra építve felvázolta az alapképzés egy lehetséges tematikáját, majd bemutatta a biztonsági szint további emelését elősegítő továbblépési lehetőségeket. Mindeközben olyan általánosításokat tett, amely lehetővé teszi, hogy az oktatott anyag nem csak a védett vezető által éppen aktuálisan használt eszközre és szolgáltatásra legyen megfelelő, hanem azokat a védett vezetők képesek legyenek alkalmazni például egy új szolgáltatás vagy eszköz igénybe vétele esetén is.

A továbblépés lehetőségeiben megfogalmazottak mellett azonban más, az alapképzéshez szorosan kapcsolódó feladatokat is célszerű elvégezni. Először is a cikkben leírt tematikát tartalommal kell kitölteni, amely a képzést tartó szervezet szakembereinek, vezetőinek a feladata. Ugyancsak az ő felelősségük az oktatáshoz kapcsolódó anyagok (2-3 oldalas leírások, flash animáció, stb.) elkészítése.

Szintén az ő feladatuk, hogy a későbbiekben figyelemmel kísérjék a technológiai változásokat, az új eszközök új tulajdonságait, a megjelenő új internet-technológiára épülő szolgáltatásokat, az azokból eredő új veszélyeket, és ezeknek megfelelően – ha szükséges – javítsák, módosítsák, változtassanak, frissítsenek a képzés tartalmán, vagy adott esetben magán a tematikán is.

Célszerű további elméleti kutatásokat végezni és a technikai elhárításra, annak kiterjesztett értelmezése szerint egy új, pontos definíciót adni. Ennek kapcsán kell részletezni, pontosítani és elhatárolni a technikai elhárítók, valamint a helyi, elektronikus biztonságért felelő személyek, szervezetek feladatait, hatáskörét.

Mihamarabb szükséges kidolgozni egy, az alapképzésnél jóval többet adó, az elektronikus információk védelmét előíró jogszabályokkal összhangban lévő, hosszabb időtartamú, képzés tematikáját. Ennek fontos pontja az alapképzéshez hasonlóan az alábbiak:

- veszélyek bemutatása,
- biztonság megteremtésének módjai, beállítások, biztonságtudatos használat,
- ellenőrzés.

Ezt a lehető leghamarabb el kell indítani, még azelőtt, hogy azt jogszabályban kötelezővé tennék az érintett vezetői körnek.

Bár a továbblépés lehetőségeinél már szerepel, de kiemelést érdemel, hogy ugyancsak a lehető leghamarabb célszerű jogszabályi javaslatot megfogalmazni a hordozható infokommunikációs eszközök teljes életciklusát átfogó hatósági felügyeletére. Ebbe bele kell foglalni a beszerzendő eszközök engedélyezésétől kezdve, a használathoz kapcsolódó biztonsági előírások jóváhagyásán keresztül, a kivonáskor a használt adathordozók megsemmisítésének ellenőrzéséig minden olyan feladatot, amely hatósági eszköztárral segíti az elektronikus információbiztonság további emelését.

Felhasznált irodalom

[1] Kovács Zoltán: Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából I. Hadmérnök, IX. Évfolyam 2. szám - 2014. június pp. 277 – 289 -ISSN 1788-1919

[2] Kovács Zoltán: Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából II. Hadmérnök, IX. Évfolyam 2. szám - 2014. június pp. 290 – 296 -ISSN 1788-1919

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Mészáros Gergely
meszaros.gergely@gmail.com

ELOSZTOTT VERZIÓKEZELÉS A KÖZIGAZGATÁSBAN

Absztrakt

Napjainkban a szoftverfejlesztés nehezen elképzelhető verziókövető rendszer segítsége nélkül. Szinte minden nagyobb szervezet alkalmaz valamilyen a verziókövető megoldást, a fejlesztés vagy általában a dokumentum-kezelés területén. Ugyanakkor megfigyelhető, hogy egyre nagyobb népszerűségnek örvendenek az eredetileg nyílt forrású fejlesztéseket támogatására kifejlesztett elosztott verziókövető rendszerek. Cikkünkben arra keressük a választ, milyen vonzó lehetőségeket nyújthat ez a feltörekvő megoldás a közigazgatási információs rendszerek vagy a kapcsolódó létfontosságú rendszerelemek információs rendszereinek területén. Bemutatjuk az elosztott verziókövetők potenciálisan hasznosítható képességeit és feltárjuk a közigazgatási rendszerek azon tevékenységeit, ahol az ilyen eszközök használata előrelépést jelenthet.

Nowadays it is hard to imagine software development without help of version control systems. Almost any mayor organizations are using some kind of version control in the field of development or document management. In the same time one can observe the increasing popularity of distributed version control systems that were originally created for supporting open source development. In this paper we are seeking for opportunities that can be exploited in the area of governmental information systems and related critical information infrastructures. We are specifying the potentially usable features of distributed version control systems and exploring government activities where application of these tools may introduce improvements.

Kulcsszavak: *DVCS, közigazgatás, verziókövetés ~ DVCS, government, version control*

BEVEZETÉS

A nyílt forrású programfejlesztés támogatására kifejlesztett verziókövető rendszerek valóságos virágzásnak indultak az utóbbi évtizedben. Tucatnyi különféle változat versenyez az első helyért [1], és ma már szinte elképzelhetetlen olyan komolyabb fejlesztés, amelynek forráskód változásait ne lehetne legalább valamelyik elterjedtebb verziókövető megoldás segítségével megfigyelni.

Ezeket a rendszereket ugyan elsősorban a programkód változásainak követésére tervezték, valójában bármilyen szöveges, illetve bizonyos korlátok között bináris adatok verziókövetésére is alkalmasak. Tekintettel arra, hogy a demokratikus társadalomban az állami szektor dokumentációinak és informatikai megoldásainak könnyen kereshető archiválása, adott esetben publikálása kiemelt fontossággal bír, joggal merül fel a kérdés hogy hasznosíthatóak-e az elterjedt verziókövető rendszerek képességei ezen a területen.

Mint látni fogjuk, ma már nem példa nélkül való, hogy az állami szféra nyílt forrású verziókövető rendszert használjon fel saját céljaira, sőt, a nyíltság fontosságát hangsúlyozó, és a közösség erőteljesebb bevonását szorgalmazó demokratikus irányvonal kifejezetten előnyben részesíti ezeket a megoldásokat.

A modern elosztott verziókövető rendszerek felhasználhatósága kapcsán két fontos kérdésre kell választ kapnunk. Egyrészt melyek azok a közigazgatási felhasználási területek, amelyek működése hatékonyabbá tehető a verziókövetés integrálásával, másrészt melyek azok a kritériumok amelyek teljesülése ezeken a területeken elvárható illetve alapkövetelmény. E két alapvető kérdés megválaszolása után a szerencsésen széles választékból már ki lehet keresni a céljainknak leginkább megfelelő variánst, illetve meghatározhatóak az esetlegesen fejlesztésre szoruló területek.

Ez a cikk a közigazgatással kapcsolatos munkafolyamatokban felhasználható elosztott verziókezelő rendszerek vizsgálati kritériumainak meghatározására koncentrál. Az első fejezetben röviden összefoglalom a verziókövetés céljait és bemutatom a vizsgálat tárgyát képező elosztott verziókezelő rendszereket (továbbiakban DVCS[1]). A második fejezetben néhány pozitív példán keresztül szemléltetem a verziókövetők jelenlegi alkalmazási lehetőségeit a közigazgatásban, és meghatározom azokat a közigazgatási felhasználási területeket és feladatokat, ahol a DVCS alkalmazása feltehetően előnyt jelenthet. A harmadik fejezetben meghatározom a DVCS értékelésének lehetséges szempontjait valamint javaslatot adok a második fejezetben meghatározott felhasználási területek esetében célszerűen alkalmazható prioritási sorrend felállítására.

1. VERZIÓKÖVETÉS HÁTTERE

A modern verziókövető rendszerek elsődleges felhasználási területe a szoftverfejlesztés, különösen a közösségi, elosztott szoftverfejlesztés támogatása. A ténylegesen kezelhető dokumentumok köre azonban ennél jóval bővebb; bizonyos korlátok között bármilyen dokumentumtípus kezelhető ezekkel a rendszerekkel.

A közigazgatás folyamataiban felhasznált dokumentumok esetében alapvető fontossággal bír a változások pontos, esetenként nyílt nyomon követhetősége. Az elterjedt verziókövető rendszerek használata tehát előnyt jelenthet. Az egyre inkább előtérbe kerülő, és döntő részben valamilyen verziókövető megoldást alkalmazó nyílt forrású szoftverekkel való kapcsolattartás igénye szintén azt sugallja, hogy kormányzati, közigazgatási szinten érdemes ezzel a területtel behatóbban foglalkozni.

1 distributed vagy decentralized version control system, röviden DVCS

1.1. Verziókövetésről röviden

A mérnöki tudományokban és a szoftverfejlesztés területén különösen elterjed gyakorlat a tervek, dokumentumok vagy forráskód változásainak rögzítése, azaz a verziókövetés. Az egyes változatokat valamilyen jelöléssel, számmal vagy betűjellel, más néven verziókóddal ellátva és tárolva a dokumentum korábbi állapota visszakereshetővé és összehasonlíthatóvá válik. Amennyiben a változtatást végző személy azonosítóját valamint a változtatás időpontját is rögzítjük, a dokumentum módosításainak teljes naplója rendelkezésünkre áll. A technológia fejlődésével a dokumentumok száma jelentősen megnövekedett, és egyre nagyobb igény mutatkozott a különféle verziókon párhuzamosan végzett munka esetleges konfliktusainak kezelésére is.

A verziókövető rendszerek ezt a két a feladatot végzik el automatikus vagy félautomatikus módon. Használatukkal jelentős mértékben leegyszerűsödik az összehasonlítás és keresés, bizonyos dokumentumtípusok esetén lehetőség nyílik az eltérő verziók különbségeinek kezelésére is, emellett követhető naplót kapunk a dokumentumok változásairól.

A verziókövető rendszer (az irodalomban általában VCS[2]) lehet önálló alkalmazás, illetve valamilyen dokumentumkezelő szoftverbe ágyazott képesség is. Ez utóbbira példa a Google Docs, a Wikipedia Page history vagy a LibreOffice és Microsoft Word beépített verziókezelő képessége [2]. Az alkalmazásba ágyazott verziókövetés értelemszerűen az adott dokumentumtípus és formátum kezelésére korlátozódik. Ezekkel a rendszerekkel itt nem foglalkozunk, a vizsgálatunk tárgyát az első csoportba tartozó általános célú verziókezelő rendszerek képezik.

Felhasználási területét tekintve napjainkban a VCS rendszereket elsősorban a forráskód nyilvántartására használják, de találhatunk alkalmazási példát az eredeti cél, a konfiguráció menedzsment valamint az általános értelemben vett dokumentum-kezelés területén is. A modern, olvasható XML struktúrájú dokumentum állományok változásai jól kezelhetők az általános célú verziókövetőkkel.

A verziókezelés számos változata között kialakult egy közös képesség készlet, egységes nyelvezet, amely kifejezések alatt minden rendszerben hasonló elveket értünk. Mivel az irodalom gyakran használja ezeket a kifejezéseket, röviden összefoglalom a legfontosabb fogalmakat:

- *Commit:* Érvényesítés, átvezetés. Változások mentése a rendszerbe.
- Atomi műveletek: A modern verziókövetők tulajdonsága. A rendszer a műveletek megszakítása esetén sem kerülhet inkonzisztens állapotba. A legfontosabb ilyen művelet az érvényesítés (commit).
- *Merge:* Összefésülés. Két eltérő verzió különbségeit a rendszer automatikusan vagy emberi segítséggel képes összeolvasztani.
- *Tag, label:* Címke. A legtöbb verziókövető képes egyes állapotokat egyedi címkével megjelölni, amellyel utólag az adott állapotra hivatkozni lehet.
- *Branch:* Elágazás. A rendszer képes egy adott állapotnál elágazást képezni és több eltérő változásfolyamot párhuzamosan vezetni. A két változat függetlenül fejlődhet, az eltérések később általában összefésülhetők.

A verziókezelők részletes képességeiről további információk találhatóak a Wikipédia oldalain [1].

2 Version Control System

1.2. Elosztott verziókövető rendszerek

A párhuzamos munkavégzés során kialakuló ellentmondások feloldására két módszer terjedt el: a kérdéses adathalmaz zárolása illetve a változatok összefésülése. A CAP[3] tétel alapján egy mai modern hálózatos rendszerben, ahol a particionálódás teljes kivédése gyakorlatilag lehetetlen, választani kell a rendelkezésre állás vagy a konzisztencia előtérbe helyezése között. [3] A zárolás lényegében a konzisztencia előtérbe helyezése a rendelkezésre állás rovására, az utólagos összefésülés pedig az azonnali rendelkezésre állás biztosítása a feltétel nélküli konzisztencia feláldozása árán. A hatékony párhuzamos munkavégzést támogató verziókezelő rendszerek általában ez utóbbi utat követik, igaz, néhányuk esetében lehetőség van az állományok zárolására is. A rendelkezésre állás biztosítása tekintetében az elosztott rendszerek általában sokkal jobban teljesítenek, mint a központosított rendszerek [4], az egyre összetettebb fejlesztési folyamatok pedig robusztus megoldást igényeltek, így az elosztott verziókezelők megjelenése és térhódítása csupán idő kérdése volt.

1997-ben jelent meg a Bitkeeper, az elosztott irányvonal egyik úttörője [5]. A Linux kernel fejlesztése során is használt rendszer azonban nem volt nyílt, így a kernelfejlesztők saját céljaikra megalkották az azóta is töretlenül növekvő népszerűségű Gitet, amelyet hamarosan számos újabb elosztott verziókezelő megjelenése követett.[6] Napjaink három legismertebb nyílt forrású elosztott verziókezelő rendszere a Git, a Mercurial és a Bazaar. Kevésbé elterjedt, de figyelemre méltó projekt a Darcs és a Fossil. A jövőben minden bizonnyal további versenytársak is megjelennek majd. Az Ohloh nyilvántartásában szereplő nyílt forrású projektek elemzésével készült statisztika szerint 2014 elején az elosztott verziókezelők részaránya körülbelül 40%, amelynek döntő hányadát a Git felhasználás adta [7]. Az elosztott verziókezelők alapvető céljai nem különböznek a központosított megoldásétól, viszont az elosztott kialakítás néhány igen előnyös tulajdonsággal jár. Az elosztott verziókezelők gyakran említett előnyei az alábbiak [8, 9]:

- minden csomópont tartalmazza az alapadathalmazt (egyenrangúság);
- a felhasználók központi adminisztráció nélkül is együttműködhetnek;
- nincs egyetlen gyenge pont4;
- lehetőség van gyors, helyi (offline) commit végrehajtására;
- az összefésülés művelete egyszerű;
- a munkafolyamat rugalmasan alakítható ki;
- tesztelés nélkül egy helyen bejegyzett változtatás nincs hatással fejlesztés egészére.

Ez utóbbi szempont elsősorban programfejlesztés során érdekes és létező problémát enyhít, ugyanis a verziókövető rendszerekbe a forráskód egy része valóban tesztelés nélkül kerül be: Negara et. al. megfigyelései szerint a változtatások 24%-a ilyen volt [10]. A központi adminisztráció nélküli együttműködés természetesen nem előfeltétel, pusztán csak lehetőség. Megfelelő munkafolyamatot választva szükség szerint elosztott, hierarchikus vagy akár központosított fejlesztési rend is kialakítható [11]. Az egyenrangú csomópontok közül ki lehet jelölni egyet, amelyen a hivatalos változatot tartjuk nyilván, így megfelelő szervezéssel szimulálni tudjuk a központosított verziókövetést. Ezek alapján az elosztott verziókövetést tekinthetjük bővebb képességkészletnek, azaz központosított verziókövető rendszerben funkcionális előnyt nem fogunk találni. Ennek ellenére van néhány olyan tulajdonság, amely bizonyos körülmények közt a DVCS alkalmazása ellen szólhat [5]:

- Nagyobb helyi méret. Az elosztott rendszer minden csomóponton minden adatot tárol, így több erőforrást igényel a csomópontokon.

3 Consistency, Availability, Partition tolerability
4 single point of failure

- Meredekebb tanulási görbe. A több funkció hatékony kihasználása több ismeretet igényel a felhasználótól.
- Nehezebb karbantartás. A fejlesztési struktúra kialakítása és tudatosítása időigényesebb, az elosztott tárolóhelyek karbantartása pedig nehezebb.
- A helyi commitok miatt a csomópontok valójában nem teljesen egyenrangúak. A helyi csomópont meghibásodása esetén a lokális változási információk elveszhetnek.

Mint látható elosztott verziókezelők működése néhány elv tekintetében hasonlít a felhő alapú rendszerek működéséhez. Ugyanakkor fontos látni, hogy a hagyományosan felhő alapú megoldáson alapuló verziókezelő rendszerek éppúgy lehetnek elosztottak mint központosítottak, ahogy napjainkban valóban láthatunk mindkét esetre példákat. Vizsgálatunk szempontjából azonban ez a fajta felhőalapúság pusztán implementációs részletnek tekinthető.

1.3. Verziókezelés mint szolgáltatás

A nyílt forrású programok fejlesztése esetében nem mindig áll rendelkezésre központi tárhelyet biztosító vállalati infrastruktúra. Ezen a problémán azonban könnyen segíthetnek az egyre népszerűbb közösségi szoftvertárhelyek. Ilyen szolgáltatások közel két évtizede léteznek, és az utóbbi években jelentősen bővült a választék és a szolgáltatások minősége. A tucatnyi lehetőségből a kiszolgált projektek száma alapján a legjelentősebb szereplők: GitHub, SourceForge, GoogleCode, Bitbucket, Assembla, CodePlex, Launchpad, Gitorious[5]. Használatuk olyan széles körű, hogy szinte minden nyílt szoftver forrása megtalálható legalább az egyik ismertebb szolgáltatón. A közös kommunikációs felülettel segített együttműködésre és fejlesztésre új kifejezés is született: a "közösségi programozás[6]".

A verziókezelés, mint webszolgáltatás mindamellett jóval többet ad egyszerű közös tárhelynél. A legtöbb szolgáltatás komplett infrastruktúrát nyújt: közös kommunikációs csatornaként működik, egyszerűen kezelhető felhasználói felületet biztosít a projektkezeléshez, kódvizsgálati és hibakövető rendszert szolgáltat, valamint átjárást biztosít az több különféle verziókövető megoldás között. [13]

A GitHub egyik általánosan használt DVCS stratégiája a beolvasztási kérelmen (pull request) alapuló együttműködés. Ennél az együttműködési formánál a központi kódtárat nem osztják meg minden fejlesztő között. Ehelyett a fejlesztők klónokat (fork) készítenek róla, és egymástól függetlenül végzik a módosításaikat. Amikor a változást elküldésre érdemesnek ítélik, a GitHub felületén létrehoznak egy pull request kérelmet, amely meghatározza melyik ágat kívánják a központi tárolóba olvasztani. A projekt vezetőségének egyik tagja átnézi ezeket a változtatásokat, majd esetleges egyeztetés és javítási körök után, beolvasztja vagy elutasítja a kérelmet. G. Gousios et al. kutatásaiból kiderül, hogy pull request alapú fejlesztési stratégia használata egyelőre nem túl magas, körülbelül 14% körüli értékre tehető [14], azonban a vonzóan egyszerű kezelőfelület, a kötetlen csatlakozás lehetősége és könnyen ellenőrizhető változások a jövőben akár uralkodó formává is tehetik ezt a fajta fejlesztési modellt.

2. VERZIÓKÖVETÉS A KÖZIGAZGATÁSBAN

Amint arról korábban szó volt, a verziókövető rendszerek képességei hagyományosan három területen hasznosíthatók: a konfiguráció menedzsment, a dokumentáció nyilvántartás és fejlesztés, valamint a programfejlesztés területein. Információs technológiákkal sűrűn átszőtt világunk minden nagyobb szervezetének munkájában, így a közigazgatás szervezeteinek feladatai közt is felfedezhető mindhárom terület.

---

5 https://github.com/, http://sourceforge.net/, https://code.google.com/, https://bitbucket.org/, https://www.assembla.com/, https://www.codeplex.com/, https://launchpad.net/, https://gitorious.org/

6 social coding

Ugyanakkor, bár a feladatok és célok hasonlóak, a prioritások eltérőek lehetnek egy nyílt forrású közösség és a közigazgatás területén. A verziókezelők, különösen a elosztott verziókezelők újszerű képességeinek kihasználása iránt egyértelműen érezhető a kormányzati szféra érdeklődése, amit az alábbiakban néhány példán keresztül igyekszem illusztrálni. Az érdeklődés egyik oka az lehet, hogy az állami szektor dokumentumkezelési eljárásai nem mindig felelnek meg korunk igényeinek. A Coleman Parkes Research által 2012-ben végzett felmérés szerint az állami szektorhoz közel álló európai vállalatok kevesebb, mint felében találták az alkalmazottak fejlettnek a dokumentum-kezelési stratégiát [15]. Emellett a nyílt kormányzat[7] digitális megvalósítása kapcsán szintén felmerülhet a DVCS rendszerek lehetőségeinek kiaknázása.

A kormányzati szervezetek sok szempontból erősen hasonlítanak a nagyvállalatok működéséhez, a nagyobb szervezetek működtetéséhez pedig hozzá tartozik a folyamatos fejlesztés. Ez a fejlesztés hagyományosan erősen központosított, ugyanakkor egyre gyakrabban támaszkodik nyílt forrású elemekre. A DVCS alkalmazása ilyenformán két területen kerülhet előtérbe. Egyrészt, mint a belső központosított fejlesztés új eszköze, másrészt, mint a felhasznált nyílt forrású komponensek ellenőrzésére és támogatására használt kapcsolattartó eszköz.

A konfiguráció-menedzsment céljaira ma már többnyire integrált célrendszereket alkalmaznak, valamint alapvetően az üzemeltetés témakörébe esik, ezért – bár néhány helyen alkalmazzák – ezzel a területtel itt most nem foglalkozunk. Vizsgálatunk tárgyát képező közigazgatási DVCS felhasználási területek tehát az alábbiak lesznek:

1. dokumentumkezelés, jogszabályok;
2. belső fejlesztések;
3. F/LOSS8 biztonsági audit és kódkövetés.

Az alábbiakban ezekkel a területekkel kapcsolatos példákat mutatunk be, felhívva a figyelmet néhány érdekes lehetőségre és körülményre.

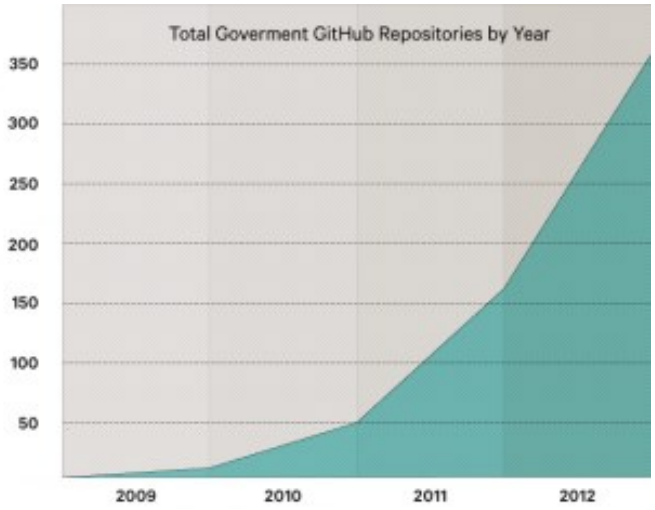
2.1. Példák a DVCS kormányzati alkalmazására

Az utóbbi években láthatóan felerősödött az érdeklődés a DVCS nyújtotta képességek iránt az közigazgatási szféra részéről. Bár használatuk messze nem széles körű, több olyan projekt is ismert, amelyek a nyíltság vagy egyszerűen csak technikai előnyök miatt a DVCS használata mellett tették le a voksukat. Az alábbiakban néhány ilyen példát mutatok be.

A Govcode[9] portálon összegyűjtött, DVCS alapokon elérhető számos nyílt forrású kormányzati projektek tanúsága szerint az Államokban már a valóságban is érezhető az Obama kormányzat fémjelezte Nyílt Kormányzás[10] hatása. Ágazatok széles skáláját felölelő projektek közt válogathatunk. Többek közt megtalálható itt számos API definíció, például a Fehér Ház weblap adatelérési szabványa[11], petíció keretrendszer, kézikönyvek, földrengés-esemény előrejelző rendszer, NASA küldetés irányító technológiák[12], rákkutatással kapcsolatos rendszerek, rádiótorony helymeghatározó rendszer és számos más projekt. Témánkat tekintve feltétlenül érdekes és tanulságok lista, amit azonban túlértékelni sem szabad. A Govcode egyéni kezdeményezés és nem állami portál, ráadásul számos projekt igencsak kezdetleges állapotban van, sokszor egyetlen commitot tartalmaz. A projektek elérhetőségének technikai hátterét sem mindenhol a kormányzati biztosítja, a legtöbb projekt a GitHub oldalain érhető el.

7 Open Government
8 Free / Libre and Open Source Software
9 Government Open Source Projects, http://www.govcode.org
10 Open Government Initiative
11 White House Web API Standards
12 NASA Mission Control Technologies, MCT.

Az Egyesült Királyság kormányzati portáljának forráskódja[13] megtalálható a Githubon. Kanada és Finnország kormányzata szintén tart fenn tárhelyet a Github oldalain. [16] Összességében a Githubon tárolt kormányzati tárhelyek száma jelentősen emelkedett az utóbbi években, 2013-ban már elérte a 350-et. [17]



1. ábra. Kormányzati tárhelyek a Githubon. (Forrás: Brian Ross/Wired)

Stefan Wehrmeyer aktivista és fejlesztő jóvoltából a teljes Deutche Bundesgesetze megtalálható GitHub portálon[14] [18]. Az írás születése pillanatában 126 fork létezik, ami jól mutatja az érdeklődést. A DVCS változat ugyanakkor nem hivatalos. A Git tárolóban lévő anyag a német kormányzat által elérhetővé tett XML formátumú állományokból generált Markdown[15] formátumú szövegeket tartalmaz.

2.2. Törvényalkotás

A törvények és jogszabályok rendszere néhány tekintetben igen hasonló a programok forráskódjához. A jogszabályok között függőségi viszony áll fenn, akárcsak a programrészek között. A módosításokat több időpontban több entitás végzi, és a tervezés során több alternatív vázlat létezhet egy időben hasonlóan az ágakhoz. A korábbi változatok ismerete és a változások kereshetősége éppúgy fontos, mint a forráskód esetében. A jogszabályokat azonban jelenleg a társadalom igen szűk rétege alkotja, valahogy úgy, ahogy az üzleti szoftverek forrását is egy igen szűk programozócsapat készíti.

Manapság a nyílt forrású szoftverek dinamikus térhódítását tapasztalhatjuk [19]. Az átláthatóság, nyíltság, és nem utolsósorban a DVCS rendszereknek köszönhető hatékony közösségi munka nagymértékben megnövelte a nyílt fejlesztési modell népszerűségét. Mint láthattuk néhány ország már meg is tette a az első lépéseket egy nyílt, áttekinthető törvényi rendszer felé.

Clay Shirky TED talks előadásában érdekes kérdést feszeget. Elképzelhető-e vajon, hogy egy napon a törvényalkotás folyamata a jelenlegi nyílt forrású fejlesztési modellhez hasonló szerkezetűvé váljon? [20] Az előnyök nyilvánvalóak: bárki felvethet változtatásokat, egyes csoportok önállóan és szabadon alkothatnak jogszabály variánsokat, a változtatások könnyen és gyorsan áttekinthetőek, a változások beolvasztása a hivatalos verzióba pedig egyszerű és követhető. Arra is lehetőség lenne, hogy az egyes változások szerzőségi információit nyilvántartsuk.

13 http://gov.uk
14 https://github.com/bundestag/gesetze
15 XHTML formátumba konvertálható, könnyen olvasható és írható strukturált szöveges állomány.

Természetesen rengeteg a nyitott kérdés ezen a területen. Bár a technológia adott és a programfejlesztésben évek óta hatékonyan használják, a nyílt, elosztott törvényalkotásra valószínűleg a fejlett demokráciákban is jó ideig várni kell, még ha egyébként életképesnek is bizonyulna a módszer. Egyrészt a felhasználók tábora a jogi területen lényegesen kevésbé technikai beállítottságú, másrészről a hagyományosan erősen központosított törvényalkotás folyamatának elosztottá alakításához a teljes társadalom részéről alapvető koncepcióváltás szükséges. Mivel ezek nem technológiai feltételek, a tényleges megvalósításhoz megfelelő környezetet valószínűleg csak egy generáció váltás teremtheti meg. A jövő lehetőségei és jelenleg is kihasználható előnyök viszont azt mutatják, hogy igenis érdemes foglalkozni a DVCS-szerű képességek kihasználásának gondolatával a törvényalkotás területén.

2.3. Belső fejlesztés és együttműködés a FLOSS közösséggel

Szinte minden nyílt forrású projekt használ valamilyen VCS rendszert, egyre gyakrabban DVCS rendszert a forráskód követésére. Pontos statisztikát készíteni a nyílt forrású VCS felhasználásról igen nehézkes, de a népszerű verziókövető szolgáltatások felhasználóinak és projektjeinek száma azt sugallja, hogy napjainkban már ez a nyílt forrású fejlesztések domináns, majdhogynem kizárólagos formája. Referenciaként említhető, hogy a GitHub népszerűbb közösségi fejlesztői oldal 2014-ben 5.7 millió felhasználót és 12.1 millió projektet tart nyilván[16]. Természetesen a legnagyobb nyílt forrású projektek, mint a LibreOffice, OpenStack, Hadoop, Android, Webkit, Firefox, Apache vagy a Linux forráskódja az interneten keresztül néhány kattintással legalább egy VCS rendszeren keresztül elérhető.

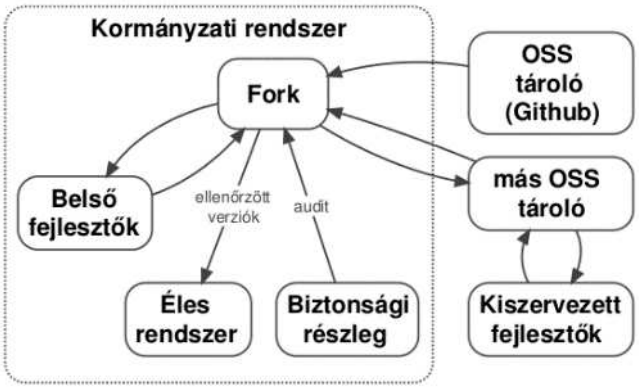
Általában véve a nagyvállalati szférában és a kormányzati környezetben is egyre gyakrabban találkozhatunk nyílt forrású fejlesztésekkel. A nyílt forrás felbukkanhat beágyazott rendszerként, mint az Android vagy routerek szoftvere, használhatjuk önálló alkalmazásként, ahogy az Apache webszervert vagy a Chrome böngészőt, és megjelenhet, mint valamely üzleti szoftver felhasznált komponense, mint a Python, az OpenStack, MySQL vagy egyéb FLOSS[17] szoftverkönyvtár. A közigazgatási és kormányzati rendszerek esetében különösen fontos szempont a gyártófüggetlenség és a biztonság, amelyet nyílt forrás segítségével biztosítani lehet. Ugyanakkor a nyílt fejlesztési modell sajátosságai miatt pusztán felhasználóként viszonyulni a nyílt fejlesztésekhez kockázatos. A nyílt projektek, különösen a kisebbek, elhagyatottá válhatnak és folyamatos kapcsolat nélkül a fejlesztés koordináló személyi állományra vagy a fejlesztés minőségére éppúgy nincs rálátásunk mint a üzleti szoftver esetében. Míg azonban az üzleti szoftver esetében bizonyos garanciát jelenthet a fejlesztők egzisztenciális függése a projekttől valamint az esetleges külső audit, a nyílt forrás esetében erről gyakran le kell mondanunk.

Gyakran előfordul, hogy egy széles körben alkalmazott OSS projekt karbantartói financiális problémákkal küzdenek. Az OpenBSD alapítvány például pénzügyi források híján 2014-ben közel állt a megszűnéshez. A probléma súlyosságát a közelmúlt nagy publicitást kapott sérülékenysége, a „Heartbleed bug” példája mutatja meg a legjobban. Az igen népszerű, számos alkalmazásban használt OpenSSL projekt egyik moduljában 2014 áprilisában súlyos sérülékenységet fedeztek fel, amellyel jelszavak illetve a privát kulcs is megszerezhető. A sérülékenységet hordozó változat 2012 márciusában került az éles változatba, azaz két éven át felderítetlen maradt. [21] A kódot számos vállalat és kormányzat használta, a probléma weblapok, VPN[18] hálózatok, levelezőszerverek és webalkalmazások tömegét, egyes becslések szerint a titkosított weblapok kétharmadát [22] érintette, ugyanakkor az igen összetett kód ellenőrzésére az erőteljesen alulfinanszírozott alapítványnak nem volt erőforrása. Steve Marquess az alapítvány elnöke szerint: “bár az OpenSSL az embereké, nem realisztikus és nem

16 https://github.com/about/press
17 Free Libre and Open Source, azaz szabad (nyílt forráskódú) szoftver
18 Virtual Private Network, virtuális magánhálózat.

is helyénvaló elvárni, hogy néhány száz vagy akár néhány ezer magánember biztosítsa a financiális támogatást". [23] Vizsgálódásunk tárgyát illetően különösen fontos, hogy a jelek szerint a kormányzatok kifejezetten lassan reagálhatnak egy ilyen problémára. A hiba publikálását követő napon a kanadai adóhatóságtól[19] 900 társadalombiztosítási számot tulajdonítottak el a lassú reagálás miatt [24]. Az események tükrében szakmai körökben felmerült a kormányzat felelősségének kérdése, illetve hogy szükséges lehet a kritikus nyílt forrású alkalmazások biztonsági ellenőrzését központi forrásból finanszírozni [22].

A fentiek alapján, véleményem szerint a nyílt forrású szoftverek biztonságos és hatékony felhasználása csak aktív állami együttműködés mellett képzelhető el a közigazgatás területén. Az állami szerepvállalás formája lehet például a visszacsatolt fejlesztés (aktív fejlesztés), az egységes kódfelügyeleti információ biztosítása (információs adatbázis, portál), financiális és jogi támogatás illetve a kormányzati eseménykezelő központok kifejezetten nyílt forrásra specializálódott részlege.



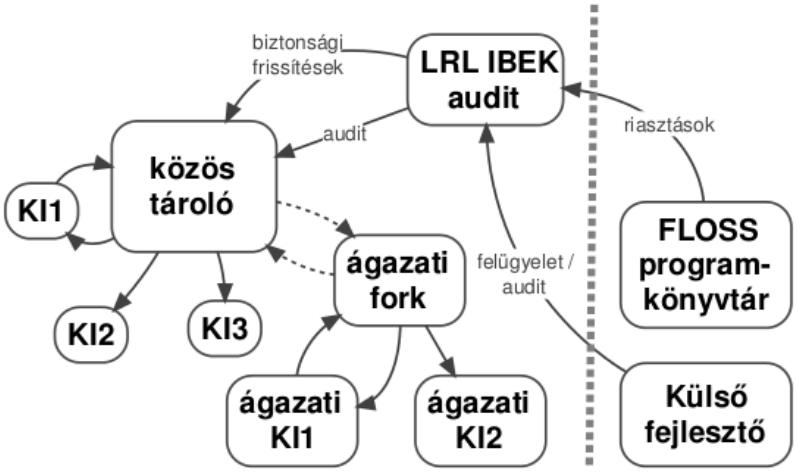
2. ábra. Példa az OSS-kormányzati fejlesztés kapcsolatára

Elosztott verziókövetők segítségével fejlesztés igen sokrétűen szervezhető. Illusztrációként bemutatok két önkényesen választott vázlatos lehetőséget, amelyeken keresztül talán jobban érzékelhető a rugalmasság és változatosság.

A 2. ábrán valamely nyílt forrású komponenseket hasznosító kormányzati rendszer lehetséges fejlesztési struktúráját mutatjuk be. A felhasznált szoftver Github tárolójáról helyi fork[20] készül, amelyben a belső fejlesztéshez külön ágat hozunk létre. A belső audit (kódminőség, biztonság, minőségbiztosítás) ezt az ágat ellenőrzi, a problémákat a belső hibakövető rendszeren keresztül jelenti. Az egyes fejlesztők saját másolataikon végezve a munkát, ami így lehet távmunka is, rendszeres időközönként beolvasztják a módosításokat a belső ágba. A OSS kapcsolattartó részleg ezek közül a változtatások közül bizonyosakat visszaolvaszt a közösségi változatba. Amennyiben a belső fejlesztői kapacitás elégtelennek tűnik egy bizonyos feladat elvégzéséhez, a kiszervezett fejlesztőcsapatnak nem feltétlenül szükséges hozzáférést adni a belső változathoz, a szükséges változtatásokat a közösségi változat megfelelő ágán elvégezve, azok folyamatosan visszaolvaszthatók belső rendszerbe. Mindeközben a ténylegesen használt éles rendszer kizárólag a biztonsági részleg által jóváhagyott folyamatosan ellenőrzött változatokból álló kóddal fut.

19 Canada Revenue Agency

20 A szoftvercsomag teljes forráskódjának lemásolásával induló független fejlesztés.



3. ábra. Egy lehetséges audit konfiguráció

A 3. ábrán a DVCS egy másik lehetséges alkalmazási módját mutatom be a kritikus infrastruktúrák területén. Az széles körben használt szoftver (amely lehet OSS vagy zárt belső fejlesztés) központi korlátozott hozzáférésű DVCS tároló készül. Az egyes szervezetek minden verziót innen szereznek be, amennyiben egyedi fejlesztéseket végeznek külön ágba szervezve ide csatolják vissza. Az egyes ágazatok speciális igényeihez saját ágazati forkot vagy ágat hoznak létre. Mindeközben a változtatások cseréje egyszerű marad. A kritikus infrastruktúrákkal kapcsolatos hálózatbiztonsági feladatok elvégzéséért és sérülékenységek publikálásáért felelős Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (LRLIBEK) folyamatos ellenőrzi a tárolók változásait, valamint elvégzi a szükséges biztonsági frissítéseket a külső forrásból felhasznált elemeken. Az egyes szervezetek közötti együttműködés egészen magas szinten valósítható meg, azonos funkciókat nem szükséges többször implementálni, a külső forrásból származó kódellenőrzést egyetlen szervezet végzi egy alkalommal és nem pusztán riasztásokat szolgáltat, hanem aktívan azonnali hatállyal javítja azokat. A kritikus infrastruktúra fejlesztőinek pusztán a megfelelő funkció ágat (feature branch) kell az stabil és a fejlesztői ágba olvasztaniuk.

A hatékony együttműködés és kódvizsgálat előfeltétele, hogy ismerjük és hatékonyan használjuk azokat az eszközöket, amellyel maga a fejlesztőközösség is dolgozik. A fenti példákon keresztül talán sikerült rámutatni, hogy e hatékony eszköz alkalmazása az egyszerű együttműködésen jóval túlmutató előnyökkel is járhat. Az elosztott verziókövetők használata az ellenőrzési folyamatokban elengedhetetlen, ugyanakkor érdemes megjegyezni, hogy az a kódot vagy a fejlesztés módszertanát elemző vizsgálat, amely kizárólag a verziókövetők adataira támaszkodik nem feltétlen nyújt átfogó képet [10].

3. DVCS ÉRTÉKELÉSI SZEMPONTRENDSZERE

Az eddigiekben felvázoltuk azokat a lehetséges kormányzati felhasználási területeket, ahol a DVCS alkalmazása előnyös lehet. A következő kérdés, hogy mi alapján választhatjuk ki a leginkább megfelelő variánst, illetve a jelenleg használatban lévő megoldások valóban teljes mértékben biztosítják-e a szükséges képességeket. Ennek érdekében első lépésként meghatározom az elosztott verziókezelők gyakran felmerülő értékelési szempontjait, majd kiemelem közülük azokat, amelyeket az adott területen a legfontosabbnak tartok. Természetesen a pontos eredmény érdekében minden esetet egyedileg kell megvizsgálni, itt mindössze felhasználási területenként egy-egy lehetséges prioritási sorrendet mutatok be.

A kiemelt tulajdonságok alapján viszonylag gyorsan eldönthető, hogy az esetleges előnyök arányban állnak-e a várható befektetéssel, létezik-e minden igényt kielégítő megoldás, illetve milyen szempontokra érdemes odafigyelni a szoftverválasztás során.

3.1. Elosztott verziókövetők értékelési szempontjai

Az általános verziókövető rendszerek azonos célokat valósítanak meg, közel azonos vagy hasonló képességkészlettel rendelkeznek, de néhány jellemzőjük eltérő. A vizsgálathoz használható értékelési szempontok gyűjtésénél két módszert használtam. A népszerű verziókövető rendszerek dokumentációjában előnyként említett tulajdonságokat vettem alapul, ezt egészítettem ki internetes fórumokon és portálokon (Stack Exchange különféle portáljai) jellemzően előforduló észrevételekkel, azaz olyan szempontokkal, amelyeket a kérdezők vagy válaszolók saját területükön fontosnak tartottak. Ezek alapján az elosztott verziókezelők legfontosabb paraméterei az alábbiak:

- Tanulhatóság (learning curve). a hatékony használati szint elsajátításához szükséges erőforrás mennyisége. Esetükben a képzés idejét és költségét befolyásolja.
- Adatbiztonság.
- Konzisztencia. Azonos állapot megőrzése valamennyi csomóponton. Magas elérhetőségű elosztott rendszereknél nem kivitelezhető, tehát az inkonzisztencia elfogadható mértékét és jellegét értjük alatta.
- Rendelkezésre állás és megbízhatóság. Mennyire stabilan és biztosan tudja a rendszer biztosítani az adatok elérhetőségét és az elvárt működést. Esetünkben kritikus rendszereknél nagy jelentősége lehet.
- Karbantarthatóság. Az infrastruktúra működtetésének erőforrás igénye.
- Átjárhatóság. Az adatok konvertálhatósága más verziókezelő rendszerek alá.
- Használhatóság. Az aktív használat egyszerűsége és gyorsasága. Felhasználó interfész és sebesség, azaz a felhasználói élmény megfelelősége.
- Elterjedtség. A szoftverfejlesztés területén általános értelemben véve.
- Sértetlenség védelme (data integrity). A változási napló sértetlenségének biztosítása.
- Commit szerzőjének azonosíthatósága.
- Naplómódosítási képességek. A napló egyszerűsítési lehetőségei (rebase, squash) az átláthatóság érdekében.
- Jogosultságrendszer. Az adathalmaz objektumainak, esetleg korábbi verzióinak hozzáférési jogosultság-ellenőrzése.
- Ágak egyszerű kezelése.
- Skálázhatóság.
- Egyszerű offline munka. A központ elérése nélkül is egyszerű munkavégzés.

Az utóbbi két kritériumot az elosztott kialakításból kifolyóan valamennyi DVCS jól teljesíti, nagy eltérések nem várhatók, de a teljesség kedvéért helye van a felsorolásban. A népszerű verziókezelők teljes körű értékelése a fenti szempontrendszer alapján jócskán túlmutat írásunk lehetőségein. A jelen cikk célja éppen egy ilyen jellegű kutatás előkészítése, ezért itt most csak néhány kiragadott, jellemző esetet mutatunk be. Az igen népszerű git verziókezelő viszonylag magas tanulási igényű, ugyanakkor igen rugalmas, ellenőrző összegek és GPG[21] kulcsok segítségével képes az adatintegritás megőrzésére, lehetővé teszi a napló módosítását, és szinte minden belső művelete vezérelhető parancssorból. Az egyre növekvő népszerűségű mercurial verziókezelő ezzel szemben a könnyű kezelhetőséget tartja szem előtt, parancsai hasonlítanak

21 Gnu Privacy Guard. A PGP kriptográfiai szoftver GPL licenszű implementációja.

a még mindig vezet SVN utasításaihoz de nem ad lehetőséget a napló módosítására. Beépített jogosultságrendszert egyik megoldás sem tartalmaz, ezt inkább külső megoldásra bízzák.

3.2. Dokumentum kezelés

A közigazgatási szféra dokumentum-kezelési feltételei alapvetően az adott jogi környezettől függenek, ezért az alábbiakban a hazánkban alkalmazható megoldásokra koncentrálunk. A közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményeket Magyarországon a 24/2006. (IV. 29.) BM-IHM-NKÖM együttes rendelet szabályozza. A hazai szervezetek ennek megfelelő ügyiratkezelő rendszert működtetnek, tehát DVCS alkalmazása csak akkor lehetséges amennyiben a szabályozásnak megfelelő ügyiratkezelő rendszerbe integrálható. A jogszabály előírja az elektronikus ügyiratokkal kapcsolatos összes változtatásra irányuló művelet és változtatás dátum szerinti naplózását, a tartalmi módosítások rögzítését ugyanakkor nem szabályozza. A dokumentum integritásának védelmét a jogszabály kiemeli, de az elektronikus aláírás használatát nem teszi kötelezővé.

Véleményem szerint egy dokumentum-kezelő rendszer csak akkor teljes értékű, ha megfelelő jogosultságok kikényszerítése, integritás védelem és az eseménynaplózás mellett képes az információ változását is gyorsan és hatékonyan megjeleníteni. A fájlonként tárolt verziókból ugyan elvben kinyerhető a változás, de amellett, hogy a tárolás így feleslegesen redundáns, a két eltérő verziójú állomány összehasonlítása is nehézkes. Különösen igaz ez ha két verzió közt formátum vagy platformváltás történt. Az irodai szoftverek beépített változáskövető funkciója bizonyos szintig megoldást jelenthet, ugyanakkor a redundáns tárolás és a platformváltás problémája továbbra is fennáll.

Gyártófüggetlen, hosszú távú megoldást csak a nyílt szabványok alkalmazása jelenthet. A European Interoperability Framework for Pan-European e-Government Services ajánlásai közt szerepel a nyílt szabványok, nyílt forráskód használata, az információbiztonság megőrzése úgy, hogy minél szélesebb rétegek nyerjenek hozzáférést, továbbá hangsúlyozza a központilag egyeztetett XML séma alkalmazásának fontosságát [25]. A tömörítetlen XML alapú állományok jól kezelhetők az általános célú VCS rendszerekkel, így alkalmazásuk a dokumentum-kezelés terén indokolt lehet.

A jogszabály előírásait és a DVCS rendszerek képességeit összehasonlítva egyértelműen látszik, hogy önmagukban ezek a rendszerek elégtelenek a nyilvántartás vezetésére. A részletes, objektum szintű jogosultságrendszer, nagy mennyiségű metaadat tárolási lehetőség nemigen szerepel egy átlagos DVCS rendszer kitűzött céljai között. Ugyanakkor figyelembe véve, hogy a nyílt rendszerek egyik nagy előnye éppen a könnyű módosíthatóság és jó integrálhatóság, ez a probléma megfelelő ráfordítással áthidalható.

A jogszabályi előírásokat figyelembe véve a közigazgatásban dokumentumkezelés céljára alkalmazott DVCS rendszer legértékesebb tulajdonságai az adatbiztonság, megbízhatóság, napló sértetlenségének biztosítása és a szerző azonosíthatósága valamint a jogosultságrendszer. Ez utóbbit jelenleg egyetlen DVCS rendszer sem valósítja meg az elvárt mértékben. Nagy mennyiségű adathalmaz esetén a skálázhatóság szintén fontos szempont lehet, bár ebben az esetben valószínűleg nem járható út, hogy minden csomópont a teljes adathalmazt tárolja, tehát hierarchikus, részekre osztott felépítés kialakítása tűnik célravezetőnek. Tekintve, hogy esetünkben a végfelhasználók szakmáját figyelembe véve a parancssorból való működtetés lehetőségét nyugodtan kizárhatjuk, a tanulhatósági és karbantartási szempontok kisebb súllyal esnek latba, hiszen egy esetleges integráció során a szükséges grafikus felületeket amúgy is ki kell alakítani.

Úgy vélem a alkalmazhatóság legkomolyabb akadálya a megfelelő jogosultság rendszer hiánya. A DVCS rendszerek elsődleges alkalmazási területe a nyílt forrású programfejlesztés, ahol a teljes adathalmaz definíció szerint hozzáférhető. A közigazgatás dokumentumainak esetében ez sokszor szintén kívánatos, más esetben, például minősített adatok vonatkozásában

viszont jogszabály által tiltott. Néhány verziókövető rendszer lehetővé teszi az információ elérésének korlátozását, másokhoz található ilyen célú kiegészítés, egyes üzleti DVCS változatok pedig kifejezetten támogatják az ACL[22] listák alkalmazását [26], tehát a probléma nem megoldhatatlan, de további vizsgálatokat igényel.

Milyen előnyöket lehet szembeállítani a várható nehézségekkel? A DVCS rendszerek alkalmazásától várható legfontosabb előnyök: robosztusság, gyártófüggetlenség, nyíltság, precíz és gyors eltérésvizsgálat valamint a távoli (otthoni vagy kiszervezett) munkavégzés esetén elérhető nagyobb hatékonyság. Hazánkban ugyan a távmunka még nem túl elterjedt gyakorlat, a világban tapasztalható trendek mindenképpen efelé mutatnak.

3.3. Belső fejlesztés

A kor követelményeinek megfelelni akaró szoftverprojekt ma már nehezen képzelhető el valamilyen verziókezelő rendszer alkalmazása nélkül. Ez természetesen éppúgy igaz a közigazgatás szervezeteinek belső projektjeire is, különösen akkor, ha az adott területen nagyobb létszámú fejlesztőcsoport dolgozik. A megfelelő rendszer kiválasztásának szempontjai jobbára egybeesnek a szoftverfejlesztés általános szempontjaival, de esetünkben kicsit erősebb hangsúlyt kapnak az együttműködést, dokumentum- és gyártófüggetlenséget célzó elvek. Az európai együttműködést segítő JoinUp portál[23] például több száz közigazgatással kapcsolatos projektet fog össze. A fejlesztések eredménye alatt nem feltétlenül forráskódot kell érteni. Az együttműködés keretében megosztandó információ nagy része API definíció, XML séma, szótár és taxonómia.

A fent említett adatok modern formátumokban kiválóan kezelhetők verziókezelő rendszerekkel, tehát a DVCS bővebb képességkészletének kihasználása itt is előnyökkel járhat. A bizonyítottan sikeres együttműködést megvalósító nyílt fejlesztői modellek akár mintaként is szolgálhatnak egy ágazatközi, nyílt fejlesztési-információ, dokumentum, API és forráskódmegosztó rendszer kialakításakor. A fent említett JoinUp portál alkalmazásai például valószínűleg szorosabb együttműködést tehetnének lehetővé, ha egyszerű tömörített fájlok helyett DVCS alapokon osztanák meg a forrásokat. Az együttműködési platformok szervezett DVCS támogatása nagyban ösztönözheti a technológia aktív belső használatát.

A belső fejlesztések esetén általános elvárás a jó tanulhatóság, a magas rendelkezésre állás, használhatóság és a karbantarthatóság. A közigazgatás területén nem ritka kritikus rendszerek esetén viszont a sértetlenség védelme lesz az egyik legfontosabb szempont.

Amennyiben belső fejlesztést segítő együttműködési hálózatban gondolkodunk, előtérbe kerül a jogosultságrendszer, valamint a változások szerzői információinak nyilvántarthatósága. A nagyfokú skálázhatóság igénye a várhatóan hierarchikus kialakítás miatt csak különlegesen nagy projektek esetében merülhet fel. Feltételezve a intraneten meglévő illetve szervezetközi dedikált, jó hálózati kapcsolatot, az egyszerű offline munka nem jelent nagy előnyt. Amennyiben viszont a vezetés kiszervezett munkavégzésben illetve távmunkában gondolkodik, az offline munkavégzés képessége jelentősen felértékelődik.

3.4. Szoftverellenőrzés

A nyílt forrású szoftverek kiválasztási és ellenőrzési folyamata az egyetlen, ahol elkerülhetetlenül kapcsolatba kerülünk a DVCS rendszerekkel. Maga az ellenőrzés is csak így valósítható meg, továbbá, mint korábban felmerült, a tartós, hatékony és biztonságos nyílt forrás felhasználás előfeltétele a közvetett vagy közvetlen részvétel a fejlesztésben.

Felhozható érvként, hogy nem sok értelme van a megfelelő DVCS rendszer kiválasztásával bajlódni, hiszen ha a fejlesztés irányítása nincs a kezünkben, legfeljebb alkalmazkodni tudunk a meglévő megoldáshoz. Ez azonban nem feltétlenül igaz. Egyrészt sok elosztott verziókövető

22 Access Control List, jogosultságlista
23 https://joinup.ec.europa.eu

szolgáltató több eltérő verziókövető formátumban is elérhetővé teszi ugyanazt a tárhelyet, tehát a választás lehetősége adott. Másrészről, a kormányzat irányából érkező pénzügyi vagy szakmai támogatás igen kedvező feltételeket teremthet egy nyílt projekt számára, így jó eséllyel meggyőzhető a közigazgatás számára inkább megfelelőbb megoldás használatáról. Mindamellett az sem példa nélkül való, hogy egy nyílt forrású fejlesztés központi irányítását állami szerv végezze[24]. Ennek fényében talán mégis van értelme a szoftverellenőrzés céljaira leginkább alkalmas DVCS platformról beszélni.

Figyelembe véve, hogy elsődleges célunk a folyamatos biztonsági audit és a projektkövetés, a legfontosabb képességek a napló sértetlenségének védelme valamint a commit szerzőjének azonosíthatósága. Fontos szempont természetesen az elterjedtség illetve átjárhatóság, hiszen annál kevesebb esetben kell a konverzióval járó esetleges információveszteséggel számolni. A naplómodosítási képesség szempontunkból kétélű fegyvernek számít. Részben tisztább és egyértelműbb projekttörténetet kapunk, hiszen ez az elsődleges célja, ugyanakkor információt veszítünk, ami egy esetleges fejlesztői profil felállításakor vagy statisztikai adatok képzése során hiányozhat.

Aktív részvétel esetén a belső fejlesztések szempontjai köszönnek vissza, leszámítva a karbantarthatóságot, melynek terhét ez esetben valószínűleg amúgy sem a szervezet viseli.

4. ÖSSZEFOGLALÁS

A cikkben röviden összefoglaltam a jellemző DVCS képességeket majd ismert példák és következtetések alapján a beazonosítottam azokat a felhasználási területeket a közigazgatásban ahol ezek a képességek előnyösen kihasználhatók. Felhívom a figyelmet a megfelelő szabványos szöveges formátumok használatának fontosságára, amely az általános célú verziókezelők hatékonyságát nagyban megnöveli. Az általános értékelési szempontok meghatározása után röviden kiemeltem néhány, véleményem szerint fontos képességet minden egyes területen. A fentiek alapján látható, hogy a DVCS rendszerek változatlan formában történő felhasználásának egyik legnagyobb akadálya, kivált a dokumentum-kezelés és belső fejlesztések terén, a megfelelő részletességgel szabályozható jogosultságrendszer hiánya. A DVCS alkalmazása a közigazgatásban ugyanakkor kivitelezhető megoldás, sőt, egyes esetekben, mint például a nyílt rendszerek biztonsági ellenőrzése, tulajdonképpen elkerülhetetlen.

A bemutatott eredmények értékelésekor szem előtt kell tartani, hogy csak a kutatási területemhez kapcsolódó nyílt forrású verziókövető rendszerek képességeit vizsgáltam, az üzleti verziókövető rendszerek vagy hasonló feladatkört is ellátó integrált rendszerekre, mint például a Sharepoint szerver, nem tértem ki. A cikk csak az elemzési szempontokat és a potenciális felhasználási területekkel foglalkozik, az egyes változatok konkrét összehasonlító vizsgálata további kutatás feladata lehet. Az írás célja éppen egy ilyen elemzés megalapozása volt, de az eredmények önmagukban is felhasználhatók az állami szféra informatikai rendszereinek korszerűsítése során. Az bemutatott képességek és szempontrendszer annak eldöntésében nyújthat segítséget, hogy egy korszerűsítés keretében érdemes-e az adott rendszer esetében megfontolni egy modern DVCS képességeinek integrálását, hol várhatók előnyök illetve milyen akadályokkal kell számolni.

Felhasznált irodalom

[1] http://en.wikipedia.org/wiki/Comparison_of_revision_control_software

[2] http://en.wikipedia.org/wiki/Revision_control

24 https://github.com/WhiteHouse

[3] Nancy Lynch, Seth Gilbert: Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. ACM SIGACT News. 2002, Vol. Volume 33, no. Issue 2, pp. 51–59.

[4] Andrew S. Tanenbaum, Maarten Van Steen: Distributed Systems: Principles and Paradigms. 2nd edition. S.l.: Prentice Hall, 2007. ISBN 0132392275.

[5] D.M.B.D. Kuhn: Distributed Version Control Systems. [online]. 2010, http://www.sonicwaves.de/downloads/publications/Distributed-Version-Control-Systems.pdf [2013-06-28]

[6] P. Mukherjee: A fully Decentralized, Peer-to-Peer Based Version Control System [online]. Ph.D. Thesis. TU Darmstadt, 2011. <http://tuprints.ulb.tu-darmstadt.de/id/eprint/2488> [2013-06-28]

[7] http://www.ohloh.net/repositories/compare [2014-05-08]

[8] C.F. Malmsten: Evolution of Version Control Systems-Comparing CENTRALIZED against DISTRIBUTED Version Control models [online]. Bachelor of Applied Information Technology Thesis. Gothenburg, Sweden: University of Gothenburg, 2010. <http://gupea.ub.gu.se/handle/2077/23474> [2013-06-28]

[9] Ian Clatworthy: Distributed Version Control Systems - Why and How. OSDC 2007. 2007.

[10] S. Negara, M. Vakilian, N. Chen, R.E. Johnson, D. Dig: Is it dangerous to use version control histories to study source code evolution? ECOOP 2012–Object-Oriented Programming [onlinel] http://courses.cs.washington.edu/courses/cse590n/12sp/danny.pdf [2014-05-08].

[11] Vincent Driessen: A successful Git branching model [online] http://nvie.com/posts/a-successful-git-branching-model/ [2014-03-10]

[12] D.M.B.D. Kuhn: Distributed Version Control Systems. [online]. 2010, http://www.sonicwaves.de/downloads/publications/Distributed-Version-Control-Systems.pdf [2013-06-28]

[13] Comparison of open-source software hosting facilities http://en.wikipedia.org/wiki/Comparison_of_open-source_software_hosting_facilities [2014-03-28]

[14] Georgios Gousios, Martin Pinzger, Arie van Deursen: An Exploratory Study of the Pull-based Software Development Model. Delft University of Technology Software Engineering Research Group Technical Report Series. 2013, ISSN 1872-5392.

[15] Coleman Parkes Research: Ricoh Document Governance Index 2012. http://www.ricoh.hu/about-ricoh/news/2013/ricoh_allam_dokumentum_felho.aspx [2014-03-10]

[16] Nico Adams: Version control for open government [online] http://scimantica.com/blog/2013/3/10/version-control-for-open-government [2014-03-10]

[17] Robert Mcmillan: How GitHub Helps You Hack the Government [online] http://www.wired.com/2013/01/hack-the-government/ [2014-04-16]

[18] Robert Mcmillan: German Federal Law Now on GitHub http://www.wired.com/2012/08/bundestag/ [2014-02-02]

[19] Amit Deshpande, Dirk Riehle: The Total Growth of Open Source. Proceedings of the Fourth Conference on Open Source Systems (OSS 2008) [online]. Springer Verlag, 2008. pp. 197–209. http://dirkriehle.com/publications/2008-2/the-total-growth-of-open-source/ [2014-03-26]

[20] Clay Shirky: How the Internet will (one day) transform government [online]. TED talk. 2012. https://www.ted.com/talks/clay_shirky_how_the_internet_will_one_day_transform_government

[21] Codenomicon: The Heartbleed Bug http://heartbleed.com/ [2014-04-10]

[22] Heartbleed Shows Government Must Lead on Internet Security http://www.scientificamerican.com/article/heartbleed-shows-government-must-lead-on-internet-security/ [2014-04-16]

[23] OpenSSL foundation president asks for more financial support in the wake of heartbleed http://www.digitaltrends.com/computing/openssl-foundation-president-asks-financial-support-wake-heartbleed/ []

[24] Heartbleed bug shows governments slow to react https://ca.finance.yahoo.com/news/heartbleed-bug-shows-governments-slow-react-090000961.html [2014-04-16]

[25] Budai Balázs Benjámin: E-Közigazgatás Axiomatikus megközelítésben. Doktori értekezés. Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2008.

[26] Pablo Santos: Distributed Version Control Systems in the Enterprise. InfoQ [online]. 2012 http://www.infoq.com/articles/DVCS-Enterprise [2014-04-18]

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Zoltán Papp
pappz.szeged@gmail.com

PROFESSINAL AREAS OF PROTECTION AGAINST INFORMATION TERRORISM

Abstract

For the undisturbed operation of today's developed and complex society the maximum operation safety of information infrastructures assuring the sustenance of social processes. With respect to the complexity and reciprocal dependence of information infrastructures with other systems the expected operation safety and arranging the protection of handled data is an important task which has to range every dimension of information security.

Napjaink fejlett és összetett társadalmának zavartalan működése szempontjából kiemelt fontosságú az, hogy a társadalmi folyamatok fenntartását biztosító információs infrastruktúrák üzembiztonsága lehetőség szerint maximális legyen. Tekintettel az információs infrastruktúrák összetettségére, bonyolultságára, illetve más rendszerekkel kialakult kölcsönös függőségére az elvárt üzembiztonság és a kezelt adatok védelmének megszervezése fontos feladat, melynek ki kell terjednie a komplex információbiztonság minden dimenziójára.

Keywords: *information terrorism, information terrorist attacks, complex information protection, critical information infrastructures ~ információs terrorizmus, információs terrortámadások, komplex információvédelem, kritikus információs infrastruktúrák.*

INTRODUCTION

Protecting critical information infrastructures providing the basis for information processes which encompass the days of the 21st Century man is crucial for the effective operation of information society. At the same time, entities operating in a narrower segment (private individuals, economic companies, social organizations) can also operate information systems which from their perspectives can be considered to be critical with regards to their own activities. The operators of information systems – practically independently from their designation and size – must identify those processes, system elements which have an effect on the significant parameters determining the criticality of their own system and that which dimensions of protection influence the appropriate level of information services. It is subservient to determine those potential functions and the components providing them which's protection is of high priority. The critical factors endangering information systems can basically be enlisted in four groups:

- Data security: Alteration, loss of, unauthorized access to information as a result of some hostile turmoil or act.
- Availability: Significant increase of accessing time to information or services, partial or whole inaccessibility as a result of some kind of external impact.
- Performance: Significant failure of capacity of some component or the whole of the system.
- Compliance with regulations: The system cannot comply with rules, norms regulating operation during functioning.

The entities of information society use information systems to achieve their goals. At the same time, every such system has its critical point which's malfunction severely endangers the achievement of the given goal. When a malfunction or an attack hits a component or subsystem which although is vulnerable, but from the perspective of tending the basic functions is not critical, it can cause damage, loss of prestige but does not endanger the basic functions.

When configuring information systems the parameters of infrastructures greatly depend on the quality of equipment used, the available parameters of the circle of five services to be used (data collection; information-forwarding; storing, processing and servicing), the quality of know-how and the special requirements of the entity, which is almost unique and is only characteristic of the given information system. With respect to the above, those wishing to attack the information infrastructure have to decide what services they want to damage. For this they have to determine which components' vulnerability exploitation can lead them to reaching their goal.

The success of the attack greatly depends on the motivation of the invader, attacking potential and on what is the relation of the pending infrastructure's parameters. In other words, does the invader have the knowledge, ability and means to attack the parameters of the system, which's failure or damage can result the desired goal. From the aspect of the effective protection the operator has to be acquainted with all the effects, interdependent consequences which an attack against a critical system element results in the whole of the system.

From the perspective of the operator of the infrastructure the protection of the systems is a much more complex task. Different risk analyzing methods (i.e.: CRAMM-model, Monte-Carlo simulation) are at the disposal of professionals responsible for the protection of information systems. With the help of these they can work out defense strategies but there may be a great difference between the theoretical system management and the actual realization of defense. As a basic goal, the linear solid protection system should be constituted, because by it the effectiveness can be increased greatly. An overall, complex protection strategy should be

applied with which the security gaps and the further threats resulting from them can be eliminated.

COMPLEX INFORMATION PROTECTION

One of the most important demand from security subsystems is to provide continuous availability and high level of protection for the given information infrastructure. The components of the security subsystems reflecting the highest standards of technology is crucial both from the aspect hardware and from the aspect of software since many risk sources can be induced by an invader being on a higher level of technology, greatly increasing the attacking potential.

To avoid disturbance and shortfall of critical elements protecting the information infrastructure and the continuance of service-portfolio provided by it and the accessibility and confidentiality of handled data it is advisable to set security priorities in order to keep the availability indicators on the highest level possible and to minimize damage in case of the occurence of extraordinary events. When setting the security protocols they have to extend to the elements appropriate for the systems' cycles of data-collection, information forwarding, and storing, processing and servicing and influencing criticality.

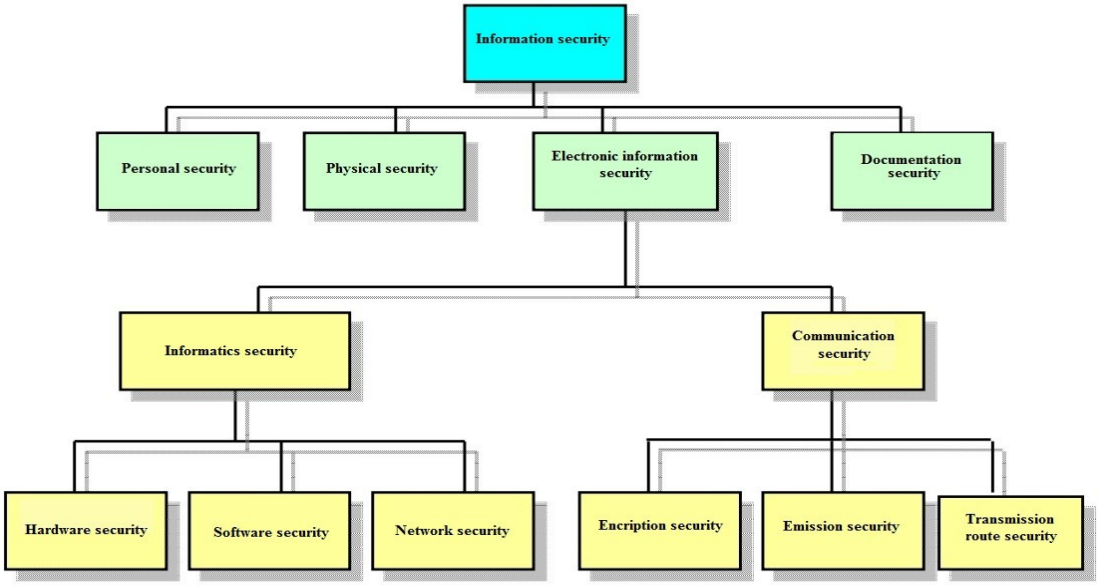
Due to the complexity of risk factors it is necessary to apply some kind of alignment, but as a result of interdependence the individual groups can add up or strengthen each other, thus the individual groups' mode of action cannot be analyzed separately. The forthcoming threats can be human, physical, logical, or risks impending during the life-time of the system [1]:

- *Human factors:* The mistakes or damages grouped in this circle of danger sources can be led back to non intentional or deliberate human acts. The motivation of non intentional acts can be diverse like for example personal incapacity, lack of qualification, negligence, irresponsibility, monotony, etc. The English literature refers to deliberate, malicious human acts as 7-E groups:

  a) Ego
  b) Eavesdropping
  c) Enmity
  d) Espionage
  e) Embezzlement
  f) Extortion
  g) Error

  Again, there may be many reasons hidden behind these seven like revenge, vandalism, grudge, profit, etc.
- *Physical factors:* Generally the physical factors are related to the location of the elements of the infrastructure's hardware, the operation personnel, and the auxiliary services. The availability indicators of the information system can damaged if the physical protection system (buildings, doors, windows, entry-systems, etc.) does not provide proper resistance to an attack or environmental impact (lightning, flood, precipitation, dust, earthquake, etc.).
- *Logical factors:* These factors can greatly endanger the availability level of an information system and the confidentiality, integrity of data handled by it. Via dangers emerging from logical factors can give unauthorized access to the handled information or make its modification or inaccessibility possible, or they may even be lost. The hostile programs take advantage of the logical mistakes (viruses, Trojan programs, etc.) and the factors stemming from bad hardware and software settings and unconsidered system planning can be rated here as well.

As part of information protection we have to attempt to create As far as possible we have to attempt to create linear solid protection systems but without careful planning and selecting there is no guarantee to having the most modern and most expensive technology meet the given infrastructure's requirements. We may say that solutions for adequate information protection can be found only with a complex approach abstracted from mere technology [2]. With regards to the above, when creating a protective strategy it is worth handling the different fields of profession separately [3]:



PERSONAL SECURITY

This model embraces the recognition of the dangers subversive and terrorist acts, the possibilities of restricting the possibility of movement. Personal security can be interpreted from the point of accessing information as well. In other words, classified information can only get into the possession of a person, who has the necessary security clearance and accessing the given classified information is necessary for official reasons. One of the most important procedures of establishing personal security may be national security vetting.

In a broader sense, personal security can be completed with examining other personal and employment circumstances related to the employee. For the security of operation it is inevitable that the employees have the necessary knowledge for which the Human Resource Management has to take care of the continuous training. Also it is necessary to have those having a clearance to access confidential information to be given proper remuneration which significantly helps keep up the working morals and loyalty.

PHYSICAL SECURITY

Physical security is actually the actual obstacles altogether – walls. fences, buildings, entry systems – which prevent the intruders to access the elements of information infrastructure, the documentation of the organization, colleagues and other means to be protected. When configuring it the protective means have to be adapted to the probable threat and life-like and adherent regulations necessary for operation have to be adopted as well. If the protectable and critical system elements are located geographically on a large territory it can affect the efficiency of physical security sub-systems which not only increase expenses but augment the possibilities of intruders.

DOCUMENT SECURITY

It is important to highlight that the protection of information is not only necessary in case of information stored in electronic systems but in case of all forms of appearance as understood in a given infrastructure, thus printed documents, handwritings, audio recordings and films.

All documents have to be protected according to its classification, sensitivity, in other words its security level. Access to documents containing sensitive data – it the way declared in the principles of personal security – have to be restricted to those, for who it is essential to have knowledge of its content. Document security is directly connected to electronic information since all electronic data medium is also a document [4].

Realization of document security is integrally connected to the organizations physical security and the configuration of its document distribution. Physical protection has to adapt to the confidentiality level of the documents. As a part of the document distribution within and outside the organization the protocol necessary for guaranteeing that the documents be accessed by only those authorized (i.e. the problem of confidential documents printed on printers accessible for everyone).

ELECTORNIC INFORMATION SECURITY

The overall regulations applied in telecommunication and informatics and other electronic systems and supporting infrastructures, which protect against the accidental or intentional decrease of the confidentiality, integrity, availability of the produced, processed, stored, forwarded and edited information [5].

Major professional areas:

- *Transmission security:* The result of the overall security regimes which assure the integrity, availability and confidentiality of information on the communication transmission routes, channels and in given cases the authenticity of transmission and the irrefutability of it [6]. Via the gradual incorporation of informatics and communication systems this professional area is more and more handled within network security.
- *Network security:* It means the protection of data connections between computers linked in a network or between computer networks and their services against the decrease of service quality and capacity and against unauthorized access, modification or destruction of information handled in the system. Protection systems of information infrastructures have to provide a great range of flexibility to combat complex threats, hostile and Trojan programs DoS and DDoS attacks, IP source address falsification, spasm, data leakage, etc. The effectiveness of network security can be significantly increased if we strive for homogeneity of the protective systems, in other words we do not try to approximate different technologies of different manufacturers for use at different locations and functions but apply such a solution which is already prepared for integration right at the beginning of the planning stage.
- *Computer security:* Under computer security we usually understand the aggregation of software and hardware security. With regards to the hardware elements to be installed in the computers it is a requirement that they collectively be capable of providing the performance necessary for executing the given service at the appropriate quality besides the required security parameters. With regards to software elements it is expected that they be capable of performing the given function fully and securely. Security can be increased if the operators use software means developed in a target oriented manner for the given task. This was the intruders cannot prepare an attack by using commercial versions, although the cost of this solution may be irrationally high.

- *Ciphering:* Refers to all activities, procedures and regulations which are aimed at converting the protected information to hide its original form from unauthorized intruders. A part of the procedure is the conversion of ciphered data back to the original [7]. Ciphering is perhaps a professional area which greatly depends on the efficiency of other professional fields (personal, physical and document security).
- *Protection against compromising emission:* This professional field means applying active and passive means and measures aimed at preventing obtaining information recoverable via analyzing the conveyed and emitted electromagnetic energy of the secondary emission of the information infrastructure electronic system elements.

SECURITY SERVICE

In many cases security service is not mentioned in the lay-outs of complex information security but still may be an important accessory to the professional areas discussed above which, beyond its basic task, can practically be understood as a kind of checking function. Security service is composed of procedures and methods with the primary goal to identify reconnoitering data-collection activities of intruders directed against the information infrastructure (prevention), to identify the attack itself (detect) and by proceeding in the inner and outer vicinity of the infrastructure to obtain information highlighting possible weaknesses, vulnerabilities, risks and needs for development of each professional area (correction) and to identify potential intruders, their motivation and potentials. So the task of security service, depending on the organizational policies, is to analyze dangers threatening the system, prepare protocols and protective measures to handle risks, eliminate risk sources and decrease feasibility and level of damage.

The effectuation of tasks by oneself which are induced by the above definitions greatly depends on the role of the infrastructure in the life of the given country because in case of a very important –even private property – system police and secret service means may also be used, while in case of a smaller, less important system they can only rely on their own sources and the legal environment may also raise barriers.

CONCLUSION

Establishing a complex information security is an extremely versatile task. When establishing the linear solid system many compromises negatively influencing the planned results have to be made for budgetary, legislative, technological or political reasons. This ends up with an end result different to the ideal safe condition. Generally, the different professional areas of information security are discussed separately but there is such a strong interdependence between them that makes it inevitably necessary to have the professional areas develop protective strategies together step by step, continuously examining and analyzing what effects the steps taken by the professional areas induce in other fields. During the operation of protective systems technological level, personal, physical security and reaction capability in case extraordinary events happen have to be checked to determine whether the system reaches the required level or not, independently from the operators of the given sub systems.

At the same time, in case of certain infrastructures there may be functions or parameters which are not important from the point of operation, thus there is no need to put irrationally large resources into their protection since an attack there will not result in damage or loss of prestige. For example, while in a law enforcement communication system, blocking the connection between the elements result in immediate problems, while in a geological network measuring the movement of continental lamina will not cause hang ups for months.

As a result of analyzing revealed attacks directed at information infrastructures it has been established that generally the intruders have not taken advantage of the weaknesses of one

professional area, but found such security gaps which resulted from the interaction of the weaknesses of several professional areas. This highlights that mutual dependence of the professional areas of a complex information security has to be taken into account when planning and creating a protective strategy.

References:

[1] Schutzbach Mártonné - Az informatikai biztonságot fenyegető tényezők http://portal.zmne.hu/download/konyvtar/digitgy/nek/2003_2/12_schutzbach.pdf, letöltve: 2014. 02. 03.

[2] Horváth László - Az információbiztonság nemcsak informatikai biztonság http://aam.hu/ftp/az_infobizt_nemcsak_2005_oktober_1.pdf, letöltve: 2014. 02. 06.)

[3] Kuris Zoltán - A komplex információvédelem új irányai a nemzeti minősített adatok védelmével összefüggésben (Hadmérnök, V. Évfolyam 4. szám - 2010. december, ISSN 1788-1919, 189. oldal)

[4] Dr. Haig Zsolt - Az információbiztonság komplex értelmezése (Hadmérnök - Robothadviselés 6. Tudományos Szakmai Konferencia - Különszám, 2006. november 22., ISSN 1788-1919)

[5] Dr. Haig Zsolt, Dr. Várhegyi István: Hadviselés az információs hadszíntéren (Zrínyi Kiadó, Budapest 2005., 201. oldal, ISBN 963-327-391-9)

[6] Kerti András - Átviteli út biztonság (Hadmérnök, II. Évfolyam 4. szám - 2007. december, ISSN 1788-1919)

[7] A 43/1994. (III. 29.) számú Kormányrendelet a rejtjeltevékenységről

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Rajki János
rajki.janos@mil.hu

A MH STACIONER HÍRKÖZLŐ HÁLÓZATÁNAK MODERNIZÁLÁSI LEHETŐSÉGE HIBRID KOMMUNIKÁCIÓS RENDSZER ALKALMAZÁSÁVAL

Absztrakt

Cikkemben a MH KCEHH[1] részét képező Stacioner Hírközlő Hálózat továbbfejlesztési lehetőségét vizsgálom meg a jelenleg üzemelő ISDN[2] infrastruktúra felhasználásának továbbfejlesztésével. Tanulmányomban a „hagyományos" távközlés és az informatika szolgáltatások egybeolvadását, fejtem ki, mivel ez a technológiai fejlődés egyenes következménye. Publikációmban a jelenleg uralkodó trenddel szembe menve e konvergenciát nem az informatikai hálózat által nyújtott hangszolgáltatás lehetőségével, hanem a kapcsolóközpontok „informatizálódása" irányából közelítem meg.

In my article, I examine the possibility of further development of Stationary communication network, which is part of MH KCEHH with the use of further develpment of the currently running ISDN infrastructure. This study of traditional telecommunications and information services to the merger will explain this as a direct result of technological progress. In my publication I go against not the prevailing trend of the convergence of non-voice services provided by IT network, but I approach it from the direction of the use of information technology in the switching centres.

Kulcsszavak: *IP, ISDN, VoIP, kommunikációs központ ~ ISDN, IP, VoIP, communication center*

[1] MH KCEHH: Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózata (55/2013. (IX.13.) HM utasítás) - Separated Governmental Communication System of Hungarian Defence Forces
[2] ISDN: Integrated Services Digital Network– Integrált Szolgáltatású Digitális Hálózat

BEVEZETÉS

A tanulmány időszerűségét két tényező határozza meg. Az egyik a technológia rohamos fejlődése, a másik pedig a meglévő távbeszélő központok gyártói támogatásának megszűnése, az eszközök avulása. Az előttünk álló fejlesztés során meg kell találni az optimális megoldást a rohamosan fejlődő csomagkapcsolt IP[3] hálózat és a meglévő időosztásos rendszerek hatékony együttműködésére. Publikációmban alapvetően a fejlesztés irányának egy lehetséges változatát szeretném bemutatni. Koncepcióm lényege, hogy a meglévő és hatékonyan üzemelő távbeszélő hálózat az anyagi erőforrások figyelembevételével több lépcsőben, a már meglévő eszközök, részegységek végkészülékek maximális hasznosításával miként modernizálható, fejleszthető. Cikkemben üzemeltetői szemszögből vizsgálom a témát, konkrét pénzügyi gazdasági összevetésre nincs módom és nem is célom.[1]

A JELENLEG ÜZEMELŐ TÁVKÖZLŐ RENDSZER

A MH Stacioner Hírközlő Hálózat digitalizálása 1998-ban kezdődött, meg amikor a légtér szuverenitási program keretében közbeszerzési eljárásban beszerzésre kerültek az első ISDN kapcsoló központok. Ezután több lépcsőben kerültek lecserélésre hazánkban a stacioner rendszer analóg kapcsoló elemei, melyek után érte el a hálózat jelenlegi állapotát. A MH Stacioner Híradó Hálózatának kialakításakor a tervezés során törekedtek a legnagyobb megbízhatóság elérésére, ezért fő és kerülő irányok is kialakításra kerültek. Topológiáját tekintve gyűrű, de ott ahol a hálózat lehetővé és szükségessé teszi, szövevényes (Mesh) hálózat került kialakításra. Az átviteli utak döntően a MH saját tulajdonú mikrohullámú hálózatára épülnek. Ez a hálózat a Totaltel Kft. által kifejlesztett TDR berendezések alkalmazásával került kialakításra. A hálózat szervezése kezdetben az analóg központok vég-góc rendszerére épült. A 2000-es évek elejétől azonban az ISDN kapcsolóközpont rendszer kiépülésével új igények jelentkeztek a hálózattervezés és kivitelezés során. A szakmai döntéshozatal eredményeként a PCM[4] elvet alkalmazó 4x2, 8x2, 16x2, illetve 34+2Mbps átviteli sávszélességet biztosító TDR berendezések kerültek beszerzésre és telepítésre. Ezen kívül saját tulajdonú optikai kábelhálózat került kiépítésre Budapesten, valamint megtalálhatóak a saját tulajdonú és bérelt réz alapú összeköttetések is. Ott, ahol a mikrohullámú összeköttetés kiépítése nem éri meg vagy nem kivitelezhető, esetleg a redundancia ezt megköveteli, bérelt 2MB/s összeköttetések kerültek kialakításra.

Az átviteli utak fejlesztésekor a távbeszélő hálózat igényei mellett egyre inkább előtérbe került az informatikai rendszerek igényeinek kielégítése is. Kezdetben ezek szigetszerűen működő szervezeti információs[5] rendszerek voltak. A 2000-es évek közepétől a fejlesztés új irányt vett igazodva a NATO és civil trendekhez. A fejlődés a funkcionális informatikai rendszerek[6] kialakítását követelte meg. Ekkor kezdődött meg az MH Transzporthálózat kialakítása. Bevezetésre került az MPLS[7] technológia, ami egyfajta csomagkapcsolt technológia, amellyel különböző VPN[8] szolgáltatásokat biztosít a hálózat felhasználói részére. Az MH országos MPLS gerinchálózat átviteli útjai a mikrohullámú hálózatban rendelkezésre

---

[3] 3 IP: Internet Protokoll

4 PCM: Pulzus Code Modulation – Impulzus Kód Moduláció

5 A szervezeti informatikai rendszer a szervezet információs tevékenységeinek megvalósítását támogató, a szervezet felügyelete alá tartozó, informatikai erőforrások összessége. (Forrás: Prof. Dr Munk Sándor: Alkalmazott Informatika diasor)

6 A funkcionális informatikai rendszer egy adott funkcionális terület információs tevékenységei megvalósítását, támogatását szolgáló, egységes szabályozás hatálya alá tartozó informatikai erőforrások – sok esetben a szervezeti határokon átnyúló – összessége. (Forrás: Prof. Dr Munk Sándor: Alkalmazott Informatika diasor)

7 MPLS: Multiprotocol Label Switching- többprotokollos címkekapcsolás

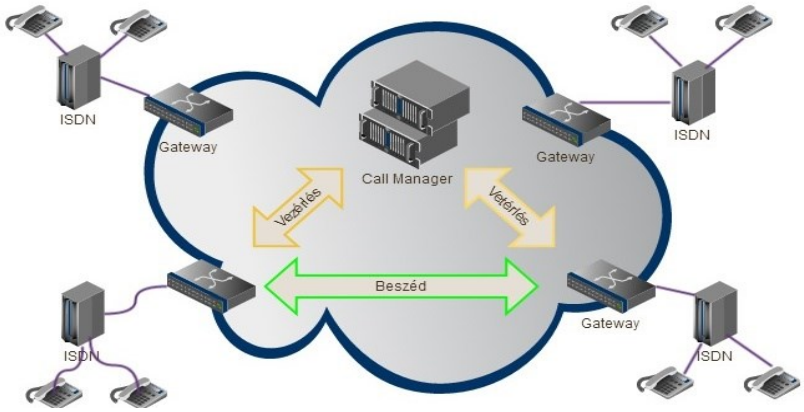
8 VPN: Virtual Private Network- Virtuális Magánhálózat

álló legnagyobb sebességű, jelenleg 34Mbp/s (E3) kapacitású gyűrűjére épülnek, ahol a csomópontokban egy-egy MPLS kapcsoló került telepítésre. A gyűrűtől távol eső katonai szerveztek, alakulatok a meglévő nx2 Mbp/s-os mikrohullámú csatornákon keresztül kapcsolódnak az MPLS hálózathoz. A jobb átvitel érdekében ott, ahol lehetséges Multilink[9] kapcsolatok kerültek kialakításra, amivel több fizikai csatornát összefogva nx2 Mbps-os összeköttetések lettek kialakítva.

A MH Stacioner hírközlő hálózatában jellemzően két technológiai szint együttes alkalmazása a jellemző. Döntően és meghatározó módon a fentebb említett ISDN kapcsoló központok, valamint kisebb mértékben, a csomagkapcsolt IP technológián alapuló beszédkommunikációs rendszer. Fontos még megemlíteni a külső kapcsolati rendszert, mely a bérlet kapcsolatokat (fővonalak, VSAT irányú távhívások, EDR átjárhatóság), az együttműködésre rendelt szervezetek (pl.: Külügyminisztérium, Belügyminisztérium, LRI stb.) irányába kialakított összeköttetéseket jelentik. Ezek a hálózat tervezést jelentősen befolyásolják (pl.: kapacitástervezés, számozási és irányítási terv stb.).

E témakör tárgyalásánál fontosnak tartom megjegyezni, hogy a stacioner hírrendszerhez kapcsolódó MH Tábori Hírrendszere jelenleg még alkalmaz kézi kapcsolású (LB-CB) analóg távbeszélő központokat is. Az ISDN központrendszer sokrétű a missziós és hazai tapasztalatok alapján akár tábori körülmények között is jól használható, megbízható megoldás a távbeszélő igények kielégítésére, azonban adatátviteli lehetőségek tekintetében a technológia jellegéből adódóan korlátozott kapacitás érhető el. Ez gyakorlatban néhányszor 64 Kb/s sebességet jelent. A 2000-es évek elejére az ISDN technológia a polgári távközlésben egyre inkább háttérbe szorult. A (távbeszélő) technikai fejlődés az IP technológiára épülő csomagkapcsolt hálózat beszédcélú felhasználásának irányába mozdult el. A gyártók felismerve ezt a tényt proaktív újításokat hajtottak végre. A MH-ban alkalmazott SIEMENS által gyártott HICOM 300-as kapcsolóközpont utódjaként kifejlesztésre került a HIPath 4000 IP kommunikációs rendszer, ami a HICOM család alapjaira épült, megtartva annak periféria egységeit, de már lehetőséget teremtve az IP technológia által nyújtott előnyök kiaknázásának lehetőségére is.

A Magyar Honvédségben az MPLS hálózat kialakításával lehetőség nyílt a VoIP technológia bevezetésére, ami alapvetően a CISCO által gyártott aktív eszközök alkalmazásával történik. Ezek a rendszerek jelenleg szigetszerűen az ISDN hálózat mellett üzemelnek viszonylag kevés felhasználóval. A rendszer működését tekintve úgy lett kialakítva, hogy a VoIP tranzit hálózatot az ISDN központok egy egységes homogén „felhőnek” látják, amelynek a peremén a közbeiktatott gatewayek fogadják és értelmezik a forgalmat és a jelzéseket, irányítják a hívásokat, kódolják, továbbítják, majd a fogadó oldalon dekódolják a beszédcsatornán érkező jeleket, amit az 1.sz ábra szemléltet.



1.ábra. ISDN és IP rendszer kapcsolódása

9 Multilink: több fizikai vagy átviteli csatorna összefogása

Az ISDN hálózat irányából érkező híváskezdeményezés esetén a beállított tárcsázási minta alapján a legközelebbi ISDN-IP gateway felé történik meg az útválasztás. Az ISDN központ a többit nem vizsgálja, hanem transzparensen továbbítja a jelzéseket. A gateway feladata az analóg vagy digitális távbeszélő jelek fogadása, ezekhez digitális jelfeldolgozók (DSP-k) kapcsolódnak, amelyek a hagyományos és az IP alapú telefonrendszerek közötti jel átalakítást bonyolítják. A hívás felépítését a call manager (hívásvezérlő) végzi. Ez leginkább a hagyományos távbeszélő központokhoz hasonló funkcionalitással bír. Lebonyolítja a kapcsolási folyamatot, valamint az IP végkészülékek menedzselését is ellátja. Központi adatbázisukban tárolják az IP telefon rendszer beállításait. [2]

AZ ISDN ÉS CISCO VOIP RENDSZEREK ÖSSZEHASONLÍTÁSA

Az előző részben ismertettem a MH-ban rendszeresített ISDN és Cisco VOIP rendszereket. Ebben a fejezetben összehasonlítom e rendszerek képességeit, előnyeit, hátrányait valamint külön foglalkozom a hadi használhatóság aspektusaival.

Mindkét esetben alapelv az, hogy, a hanghullámok digitális jellé történő átalakítása a végkészülékben megtörténik. Ezután ez a számmal jellemezhető jelfolyam a kapcsoló eszköz és az átviteli út segítségével az ellenállomás fogadó készülékére kerül, ahol megtörténik az analóg jellé (hang információ) visszaállítása. Az ISDN technológiában egy szabványos hangcsatorna fix 64kbps sebességű adatátviteli csatornát igényel. Ez a sávszélesség igény úgy jön ki, hogy figyelembe véve Shannon mintavételi törvényét, a hang 8000-szer kerül mintavételezésre (2x a legmagasabb 4 khz-es frekvencia) másodpercenként. Ezután történik a kvantálás, majd a kódolás. Ez a nyolc biten megjelenített kódolt jel kerül továbbításra az átviteli közegen. Ezt a metódust a G.711-es szabvány írja le.[10] Előnye a VoIP-al szemben, hogy a hívásfelépítés során lefoglalt útvonal a beszélgetés teljes ideje alatt rendelkezésre áll, tehát nincs ütközés, vagy más olyan veszteség, amely a beszédérthetőséget befolyásolná. Viszont a hátránya is pont ebben rejlik, mert rugalmatlan a sávszélesség kihasználás és a hívásirányítás csak előre definiáltan manuálisan állítható be. A fő és kerülő utak kialakítása komoly szakértelmet és tervezést igényel, míg a VoIP esetén a hang csomagok útvonal választását a beépített QoS alapján a routerek automatikusan elvégzik.

A VoIP esetében éppen a csomagkapcsolt voltából adódóan különböző hátrányokkal kell számolni:

- *Késleltetés:* a késleltetésnek nagy jelentősége van a tömörített hang esetében, mert a hangok csomagokba történő tömörítése időbe telik. Nagy késleltetés esetén visszhangelnyomásra van szükség azért, hogy ne alakulhasson ki zavaró mértékű visszhang. A legtöbb hangcsomagokat előállító berendezés használ valamiféle visszhangtörlési eljárást. A késleltetésnek két fő forrása van a csomag alapú hálózatokban: a jelterjedési késleltetés és a jelfeldolgozási késleltetés. Az első tényező a fény, illetve egyéb hullámok korlátos terjedési sebességével függ össze. Ez elhanyagolhatóan kicsi, ezért egy ilyen kis területi lefedettségű hálózat esetén, mint a MH hálózata, ezt nem érdemes figyelembe venni. A jelfeldolgozási késleltetés már ennél jelentősebb minőség romlást okozhat. A keretek létrehozása időt vesz igénybe, ami kb. 125 ms. Ezek az apró késleltetési idők összeadódnak, úgynevezett sorba állítási késleltetést (serialization delay)/ okoznak, ahogy a keret utazik át a hálózaton.
- *Csomagvesztés:* a beszéd és mozgókép átvitel esetén nincs lehetőség az elveszett csomagok újraküldésére, hiszen nagyon kevés idő áll rendelkezésre a dekódolásra. Az újraküldött csomaggal egyébként sem tudnánk mit kezdeni, ezért maximum 5-10%

10 Léteznek az ISDN esetében is hangtömörítési eljárások a G.723.1 vagy a G.729 szabvány által leírtak, de ezek a MH rendszerében nem használatosak, ellenben a NATO Promina rendszerrel.

csomagvesztés megengedett. A felső határ környékét elérő csomagvesztés már jelentős minőségromlást okozhat a beszédértésben. Véleményem szerint a Vezetés-irányítási rendszerekben ez már nem megengedhető. Tételezzük fel azt a helyzetet, hogy egy magasabb szintű parancsnok utasításakor ez a rövid *nem* szó kimarad a közleményből. Katasztrofális követelményekkel járhat.

- *Bithibák:* Ha a hálózatot „zavarja" valamilyen jel, előfordulhat, hogy az adatfolyamban a bitek értéke megváltozik. Azért szükséges mérni a BER -t (BitError Rate), hogy megtudjuk az egyes codec -ekre milyen hatása van a bithibáknak (mekkora BER érték, amelyet még képesek javítani).
- *Jitter:* hang csomagok időbeni eltolódása az ideálishoz képest.

A VoIP telefonok alkalmazásának vizsgálatakor nem szabad megfeledkezni a tápáram ellátásról sem. Az analóg vagy az ISDN végberendezések esetén a készülékek tápellátását a központ biztosítja. Ebben az esetben elegendő centralizáltan megoldani a szünetmentes tápfeszültség biztosítását. Erre több elterjedt megoldás létezik. Hírközpontok esetén az országos hálózat többirányú betáplálásával duplázható, vagy akár triplázható a nagyfeszültségű hálózat rendelkezésre állása. A másik megoldás a nagyteljesítményű szünetmentes áramellátó berendezések alkalmazása. Ez lehetőséget teremt arra, hogy az országos hálózat teljes kiesése esetén is több óráig a távbeszélő szolgáltatás biztosítható legyen. A harmadik redundancia szint a robbanó motoros aggregátorok alkalmazása, ami akár hosszabb áramkimaradás esetén is képes biztosítani a tápellátást.

Ezzel szemben a VoIP technológia alkalmazása esetén a tápellátást lokálisan kell biztosítani. Ha a készülék PoE [11] képes, akkor lehetőségünk van „távoli" tápellátásra megfelelő hálózati eszközök segítségével. Ez a távolság ugyanakkor a hagyományos távbeszélő szolgáltatás több kilométeréhez képest maximálisan 100 méter. Amennyiben a hálózatban alkalmazott aktív eszközünk nem PoE képes, abban az esetben *minden egyes készülék*et saját tápegységről kell üzemeltetni. Ez a megoldás jelentős plusz áramfelvétellel jár. Mivel biztosítani kell az esetleges segélyhívások lehetőségét is, valamint katonai rendszerekben a magas rendelkezésre állást, ezért akár készülékekről, akár PoE switchekről beszélünk, minden esetben lokálisan kell a szünetmentes áramellátást biztosítani, ami jelentős járulékos költséggel jár. Alkalmazott mellékoldali csatlakozások tekintetében is sokkal érzékenyebb a VoIP telefónia. A végberendezések csatlakoztatása drága CAT-5[12]kábelezést igényel (4 vagy 8 ér felhasználásával, ami a mechanikai sérülések bekövetkezésének lehetőségét növeli) és az Ethernet szabvány figyelembevételével maximum 100 m-re telepíthető a végkészülék. Hagyományos telefónia esetén azonban elég egy nem kategorizált kábel mint például az MH-ban rendszeresített és nagy mennyiségben rendelkezésre álló TKV-100, vagy az eldobó vezeték is. A HICOM rendszer specifikáció alapján 0.6 mm-es PVC szigetelésű réz vezeték alkalmazásával ISDN emeltszintű szolgáltatást nyújtó készülék csatlakoztatható 1000-1500 méteres távolságon is. Analóg készülék akár 6 kilométerre is üzemelhet a telefonközponttól. Létezik megoldás a CISCO IP telefónia esetén is analóg készülék csatlakoztatására úgy mint a VG-22413, ATA-18614 adapter, ám ezek használata a hibalehetőségeket növeli. Tábori alkalmazhatóság szempontjából ezek a tulajdonságok (készüléktáplálás, központtól mért távolság, mechanikai sérülékenység) nem elhanyagolhatóak.

---

11 PoE: Power Over Ethernet- Etherneten keresztüli távtáplálás

12 CAT-5: Az UTP kábel számos hálózatokban használt, 4 érpárból álló réz alapú átviteli közeg leggyakrabban használt fajtája. Az UTP kábeleknek mind a 8 rézvezetéke szigetelőanyaggal van körbevéve. Emellett a vezetékek párosával össze vannak sodorva, így csökkentve az elektromágneses és rádiófrekvenciás interferencia jeltorzító hatását. Az árnyékolatlan érpárok közötti áthallást úgy csökkentik, hogy az egyes párokat eltérő mértékben sodorják. (Forrás: Wikipédia)

13 VG 224: 24 portos analóg telefon gateway

14 ATA 186 : Analóg telefon adapter

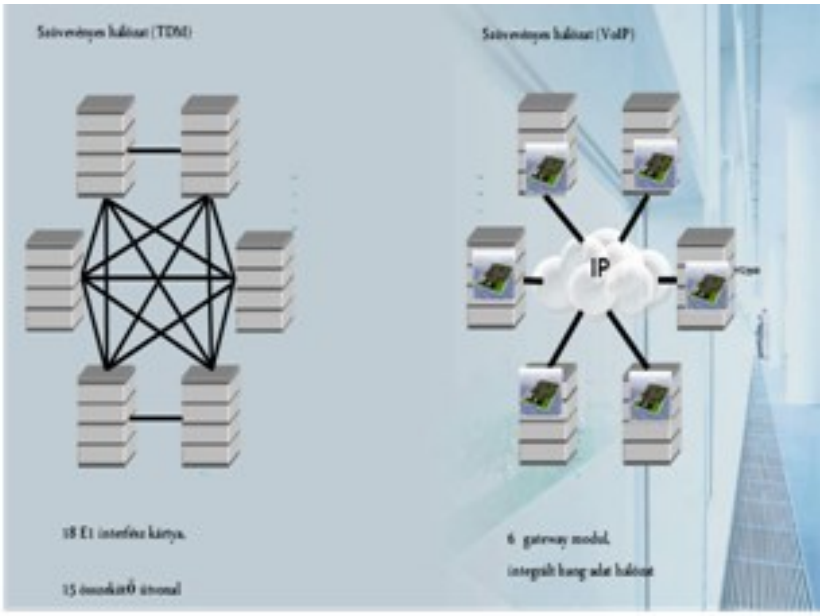
A TÖBBLÉPCSŐS MODERNIZÁCIÓ LEHETSÉGES MEGVALÓSÍTÁSA

A fenti összevetésből megállapítható, hogy mind a két jelenleg az MH-ban alkalmazott technológiának megvannak az előnyei és hátrányai is. Tudomásul kell vennünk azt, hogy az ISDN hiába bizonyította a távbeszélő szolgáltatások nyújtásában létjogosultságát, azonban az adatátviteli lehetőségeinek korlátozott volta miatt a mai felhasználói igényeket nem képes kielégíteni. Másrészről nem vitatható az sem, hogy a VoIP technológia megkerülhetetlen mind a jelen, mind a jövő távbeszélő rendszereiben. A távbeszélő és adatátviteli rendszerek konvergenciája, mint jövőkép már Dr. Fekete Károly 2003-ban készült Ph.D. értekezésében[3] is megjelenik. Felmerül a kérdés, hogy a jelenlegi állapotból kiindulva a meglévő eszközeinket fejlesztve, naprakésszé téve kihasználhatjuk-e mindkét technológia előnyeit?

Azt gondolom, hogy a kérdésre a válasz igen.

A megoldást a hibrid[15] kommunikációs rendszer tulajdonságainak kiaknázásában látom. Mivel egyazon gyártótól egy típuscsaládba tartozó berendezésekről van szó, ezért üzemeltetésük költséghatékonyabban megoldható.

A Hicom majd HIPath központok modernizációjának, IP képessé tételére már a 2000-es évek közepén történtek kezdeményezések, legalábbis teoretikus szinten, ahogy azt Dr. Szöllősi Sándor 2007-ben kelt Ph.D értekezésében is [4] említette. Ez azt jelenti, hogy a HICOM központjaink szoftver és a vezérlő bizonyos (RAM, HDD és MOD) hardver elemeinek cseréjével a HIPath 4000 aktuális verziójára[16] konvertálhatóak, így az IP képességek is elérhetővé válhatnak. Ennek elvi kapcsolódási vázlata a 2. számú ábrán látható. Fontosnak tartom katonai felhasználás esetén a redundanciát úgy, hogy ezt a már meglévő képességeink felhasználásával érjük el. Ezen gondolatmenetem mentén továbbhaladva, figyelembe véve a jelenlegi gazdasági lehetőségeket is, a modernizálást három lépcsőben képzelem el.



2.ábra. ISDN központok IP rendszerbe szervezése (forrás: Siemens)

[15] Hibrid tulajdonság alatt fővonali oldalon az analóg, 2 Mbit/s 30B+D ISDN, IP csatlakozást, mellékoldalon analóg, digitális ISDN, IP mellékek kiszolgálására alkalmasságot értem.

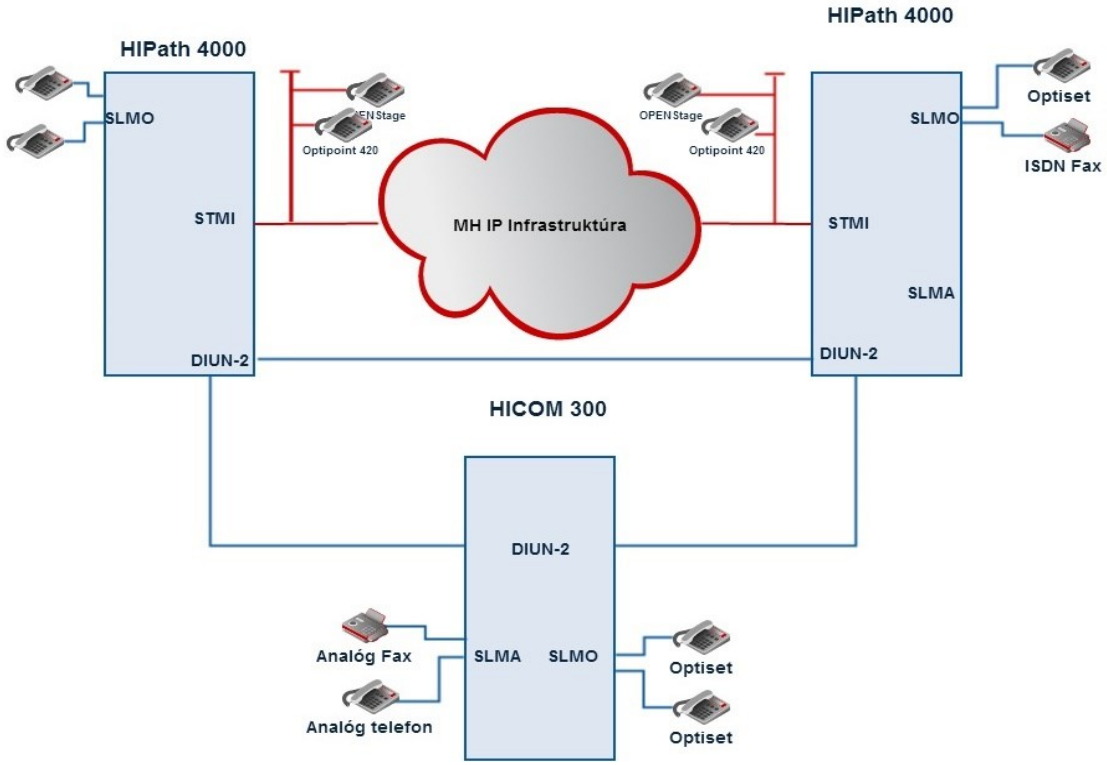
[16] Jelenleg ez a V 7.0

Első lépcső

Első lépésként a Budapesten telepített központokat cserélném le a HIPath aktuálisan elérhető verziójára. Ennek az oka, hogy itt az optikai gyűrű megfelelő sávszélességet (Gigabit) biztosít a központok közötti IP kapcsolat kialakítására, valamint a strukturált alhálózat kiépített, így ezek plusz beruházást nem igényelnek. A hálózatban a többi Hicom központ továbbra is E1 felületen kapcsolódik az új központokhoz, valamint kerülő irányként a jelenleg üzemelő TDM trunk-ok a továbbiakban is használhatóak maradnak. Mellék oldalon a VIP felhasználók részére modern, IP szolgáltatásokat nyújtó készülékek is biztosíthatóak.

1.kép. OPENstage 80 IP távbeszélő készülék (Forrás: Siemens)

A többi felhasználó számára az SLMA, SLMO kártyákon végződtetett analóg és digitális készülékek és fax-ok a továbbiakban is használhatóak, ez sem igényel külön befektetést. Központváltás esetén a lecserélt központokból a szekrény a shelf-ek, a vezérlőkártyák, tápegységek, valamint a felszabaduló készülékek és periféria kártyák tartalék, javító anyagként a többi központban felhasználhatóak.



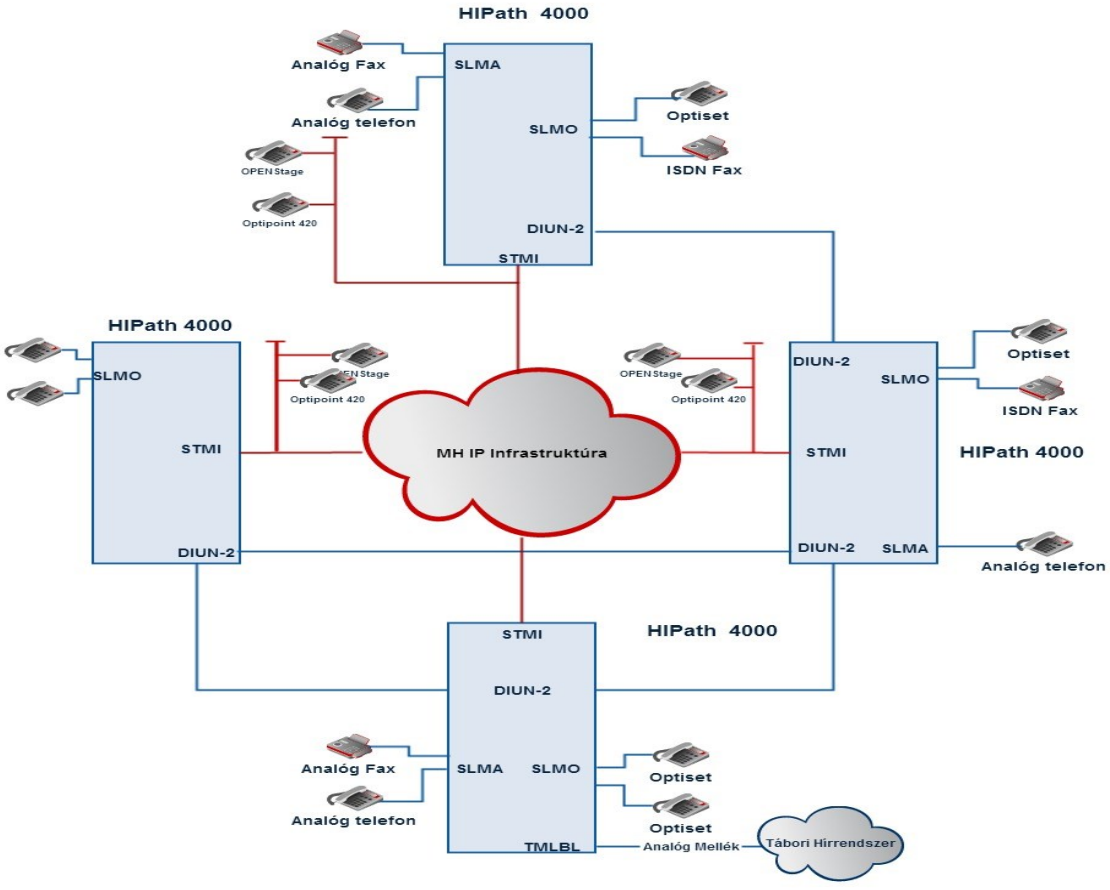
3. ábra. Koncepció a modernizálás 1. lépcsőjére

Az ábrán látható módon a fejlesztés után a két új központ trunk oldalon elsődlegesen az IP hálózatot használja (piros vonal jelzi), de kerülő irányként az E1 felületen kialakított 2 MB/s kapcsolatok is (kék vonallal jelölve) rendelkezésre állnak. Mivel ezek más-más fizikai átviteli módozatokat használnak (optika, mikrohullámú hálózat), így a kapcsolat rendelkezésre állásának növekedésével számolhatunk.

Ez az állapot egy ideig pilot rendszerként üzemelne. Az üzemeltetési adatok gyűjtésével, forgalmi adatok mérésével és elemzésével a további lépcsők tervezéséhez kaphatunk feldolgozható adatokat. A felhasználóktól kapott visszajelzések is fontos, szubjektív információkat tartalmazhatnak a rendszer paraméterezésének tekintetében, gondolok itt pl. VoIP beszéd érthetőség, visszhang, késleltetés, jitter értékek finomhangolására. Ezekkel párhuzamosan a helyi üzemeltető, valamint az országos hálózatfelügyeletet ellátó állomány képzése is végrehajtásra kell, hogy kerüljön.

Második lépcső

Az első lépcső tapasztalatait figyelembe véve a jelenleg rendelkezésre álló 34 Mb/s (100 Mb/s bővítés tervezett) mikrohullámú körgyűrűhöz közvetlenül kapcsolható központok cseréjét javasolnám. Ezek alapvetően olyan helyőrségek, ahol az IP trunk oldali sávszélesség mellett a strukturált alhálózat is jelentős mértékben kiépített.



4.ábra. Koncepció a modernizálás 2. lépcsőjére

Ismételten meg kell vizsgálni az objektív mérések és szubjektív tapasztalások eredményeit az országos rendszer végleges modernizációját megelőzően. Ebben a lépcsőben kell végrehajtani a helyi üzemeltető, a honvédségi szerviz, valamint a regionális felügyeletet ellátó állomány képzését is. Ahogy az a 4. sz. ábrán látható, lehetőség van akár LB üzemmódban is csatlakozni a MH Tábori Hírhálózatához A rendszer komplexitásából adódóan természetesen CB analóg, ISDN vagy az IP csatlakozás lehetősége is biztosítható.

Harmadik lépcső

Ebben a lépcsőben a modernizáció kiterjed az összes stacioner és konténerbe telepített kapcsolóeszközre. Előzetesen meg kell vizsgálni a klasszikusan PCM átvitelre tervezett Totaltel TDR mikrohullámú berendezések alkalmazhatóságát a VoIP kommunikációra (hibaarány, késleltetés). Amennyiben szükséges, ezen átviteli utak modernizációja is elengedhetetlen.

ÖSSZEGZÉS

Jelenleg a Magyar Honvédségben döntően és meghatározó módon az ISDN technológiát alkalmazó távbeszélő központok szolgálják ki a felhasználói igényeket. A központok közötti átviteli utakat biztosító infrastruktúra (alapvetően nx 2MB/s mikrohullámú kapcsolatok) is e technológia kiszolgálására lett kifejlesztve. A VoIP technológia térnyerése a hangkommunikációban az informatikai hálózat fejlesztésével együtt megkezdődött, és bár csak kis számban, de léteznek ilyen megoldások a MH KCEHH-ban. Véleményem szerint a „színtiszta" VoIP technológiára történő áttérés az MH-ban erősen erőforrás igényes. Cikkemben igyekeztem rávilágítani, hogy ez a megoldás nem minden felhasználási szituációban nyújt optimális megoldást. Az általam felvázolt hibrid (IP- ISDN) kommunikációs rendszer alkalmazásával a jelenleg üzemelő ISDN rendszerbe beruházott mind szellemi, mind gazdasági értéket megtartva lehet egy új technológiai szintre átlépni. A homogén hálózati elemek alkalmazásával egy kézben tartható a hálózatmenedzsment, valamint a HPMGR[17] Umbrella Managment[18] képességével az informatikai hálózat eszközei is felügyelhetőek. A tizenöt éves tapasztalattal rendelkező, jól képzett felügyeleti és üzemeltető állomány továbbképzése lényegesen kisebb ráfordítással kivitelezhető, mint egy viszonylag új és az állomány jelentős részének ismeretlen technológia bevezetése.

Felhasznált irodalom

[1] Rajki János: A Magyar Honvédség Stacioner Híradó hálózatának modernizálási lehetősége a jelenlegi infrastruktúra továbbfejlesztésével (Diplomamunka NKE HHK Budapest 2014)

[2] Márkus Szabolcs: Az IP technológián alapuló beszédkommunikáció alkalmazási lehetőségei az MH stacioner hálózatának modernizációja során (Diplomamunka ZMNE BJKMK Híradó Tanszék Budapest 2007)

[3] Dr. Fekete Károly: A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei. Doktori Ph.D. értekezés (ZMNE Budapest 2003)

[4] Dr. Szöllősi Sándor: Konvergáló hálózatok fejlődési trendjei, a technikai alkalmazhatóság kérdései a Magyar Honvédség infokommunikációs rendszerében. Doktori Ph.D. értekezés ZMNE 2007.)

17 HPMGR: HIPath Management Rendszer

18 Umbrella Managment: átfogó, a (rész)hálózati menedzsmenteszközöket összefogó menedzsmenteszköz.

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Szegediné Lengyel Piroska
l.piroska@t-online.hu

INNOVATIVE METHODOLOGIES IN THE CLOUD EDUCATION

Abstract

The article is to describe how different innovative methodologies might support the e-teaching/learning in higher- education. The author has developed a specific CTLM (Competency-based Teaching Learning Model) and 5R Learning Strategy, - which has been effectively and efficiently used at King Sigismund Business School, first of all for Accounting and Taxation courses, for the last five years, and compares it to a similar, but independently elaborated system, called Agile Teaching/Learning Methodology (ATLM). The ATLM has been introduced and used at the City University of Hong Kong. Both teaching/learning models aim at increasing students' motivation to learn, to develop their personalities, their commitments and positive attitudes by compiling and using state-of-the-art interactive teaching materials, acknowledging their results performed, rewarding them, i. e. how to find an enjoying way to the effective learning process. Both CTLM and ATLM can be considered as well applicable for a wide range of teaching/learning subjects, in this way both two models can be applied not only in the field of most common civil sciences, but in specific areas, a. g. the military one – except materials with classified information – as well.

A cikk bemutatja a különböző web-alapú innovatív módszerek oktatást támogató szerepét a felsőoktatásban. A szerző ismerteti a Zsigmond Király Főiskolán 2009. óta hatékonyan alkalmazott saját fejlesztésű Kompetencia-alapú Tanítási tanulási modell és az 5R tanulási stratégia működési elvét, összevetve azt a Hong Kong-i Egyetemen sikeresen bevezetett tanulást támogató „Agile Teaching Learning Methodology" modellel. A bemutatott modellek célkitűzései a tanulók tanulási motivációjának növelése, kommunikációs képességük fejlesztése, a pozitív attitűdök, a személyiség fejlesztése korszerű interaktív tananyagok alkalmazásával, illetve megoldást találni a tanulói teljesítmények elismerésére a modellek által felkínált élvezetes és hatékony tanulási útvonalakon. Mind a két modellnek előnye, hogy nem csak a szokványos tárgyak tanításában/tanulásában alkalmazhatók hatékonyan, hanem a legkülönbözőbb tudományok és szakmák, például a hadtudomány területén is, a nem minősített információk oktatására.

Keywords: *self-learning, learning methodology, teaching methodology, competence-motivation, feedback, adaptive methodology*

INTRODUCTION

The education in virtual environment requires the transformation of the traditional teaching-learning environment, the knowledge and use of the modern information and communication devices. For the sake of the developed world's future, socialization of the "lifelong learning" has become a primary task, i. e. a piece of norms, part of the culture. Under these circumstances, the state-of-the-art e-learning, i. e. distance education – characterized by the learning management, the open learning and the virtual environment of education – has received a specific role.

When highlighting the subject, the "premissa", I have set forth, is that the key dimension of the high quality virtual education is the learning material itself, if it is able to appropriately influence and shape – through a relevant transmission methodology – the further key elements: the student, the teacher and the teaching-learning environment.

On the basis of the above "premissa" I developed the Competence-based Teaching Learning Model (CTLM) and 5R Strategy.

The methodology is being relied on the appropriate aspects of the knowledge management, the learning management, and on the aim at assisting students in finding and developing their own learning style, in order to obtain real knowledge, through a self-relied learning activity. The prerequisite of the successful learning is that the students know "how to learn", and for this goal the learning process is to be continuously learned by them. The methodology strives also for supporting the teachers in developing the learning environment, where all necessary conditions are provided for the continuous development of basic competences of the students. [1]

The Agile Teaching/Learning Methodology (ATLM) of the City University of Hong Kong is a teaching/learning methodology designed for higher-education based on the best-practices and ideas from the field of software engineering and leveraging upon concepts from agile software methodologies. The methodology emphasizes agility, communication, feedback, the teaching/learning process and encourages communication, knowledge sharing and self-learning individuals. [2]

COMPETENCY-BASED TEACHING LEARNING MODEL

The CTLM (Figure No.1) emphasizes: in the teaching and learning the focal persons are the teacher and the student and they contact each other by the learning materials (e-books). The e-books are „knowledge transfers", the substances, tools and methodologies, so it is the tools for presentation of the unity of learning organization.

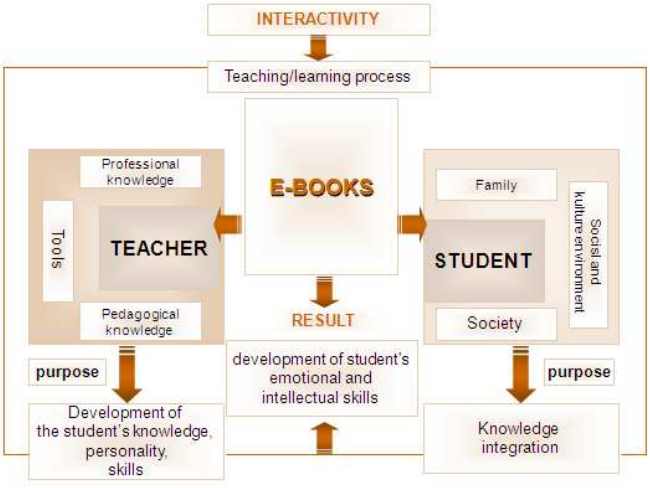


Figure 1. Competence-based Teaching Learning Model [1]

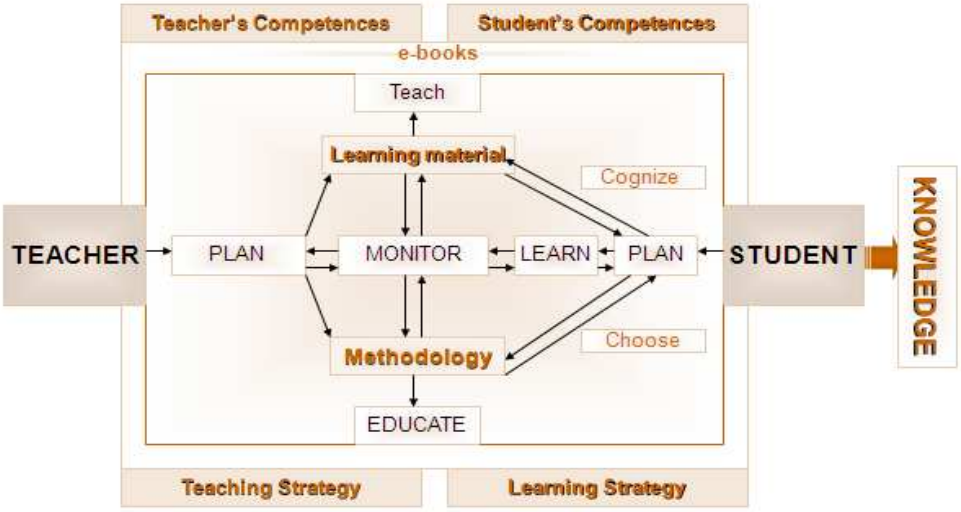


Figure 2. E-Teaching - Learning Process: LLL cycle [1]

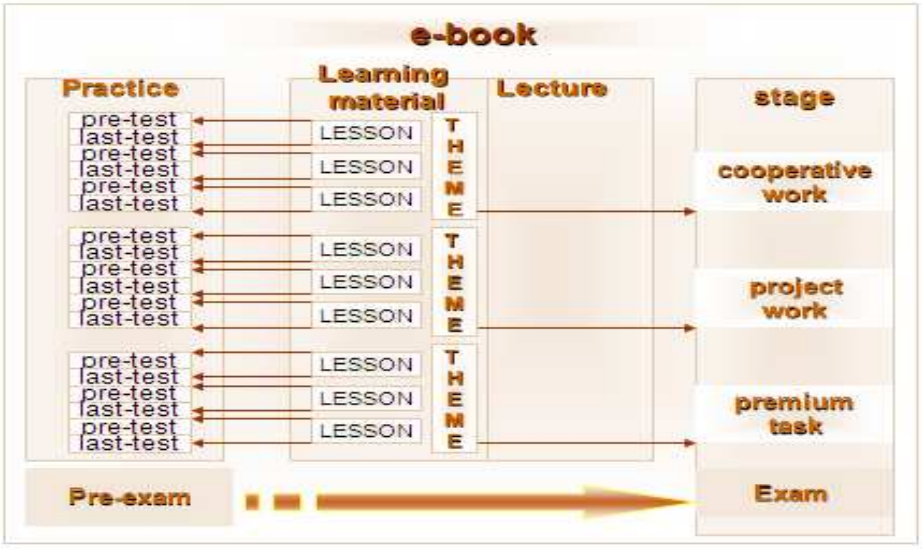


Figure 3. Levels of the learning [1]

The model is an iterative methodology (Figure No.2) to indicate the learning is a never ending process.

The teacher plans the e-learning material and offers it for students. Based on integrated substance and methodological solutions the teacher becomes to get some information now and then (continuously) about the knowledge level and the social-emotional development of the students. The teacher, based on the acquired information, can prepare special and individual development plans for all students to help them to catch-up, to be more confident in course material or to learn independently.

The material needs to cover substances and methods, which facilitate the differentiated education, the personalized development.

For every student, based on preliminary survey on his/her pre-knowledge (the knowledge-level at the beginning of the course), the learner/learning differences, his/her overall strengths and weaknesses, the teacher has to offer the best substances and methods. The student has got freedom of choice; he/she decides what the best is for him/her in the given situation.

In the learning level-system of the e-books (Figure No.3) the model requires to achieve to reveal each and every student's individual values, to get to the maximum interactivity and communication skills within framework of the education.

In the learning level-system, the 5R learning strategy (a 5-level-learning-system), appears to give an offer for the student to create his/her self-learning strategy, as follows:

- Read! - Material
- Reflect! - Lecture
- Recite! - Practice
- Review! - Stage
- Rest! - On each level

In the level-system of the e-books, based on 5R strategy, the competence of the students evolves continuously; their pre-knowledge escalates "from now to then":

The learning "*Material***"** module, which contains the actual level and quantity of information to be acquired, provides opportunity for a self-relied acquisition of the knowledge for each individual student, i.e. learning on his/her own. The module uses passive and active elements, supported by multimedia devices, for presenting the topics, illustrated by pictures, figures. In the closing section of each major chapter of the learning material, project works are inserted, which encourage students to work with others in teams, consequently, to get acquainted with partner students, to emphasize the importance of community-building. Students are invited to measure the level of their knowledge through practical project works, when working together with other partner students, in the framework of on-line sessions. [3]

The structured team works allow students to realize that everybody possesses important and specific intellectual abilities, even though unique ones, through which all individuals may contribute to the successful teamwork.

The participation in the team work requests an intense, self-relied contribution from the students, it integrates the knowledge and the students are responsible for each other's piece of work, in this way and as a result, a relation-net of mutual interdependence will be formed between them. [4]

The most important aspect is that for the successful solution of the team work, it is inevitable to mobilize the students' colourful abilities. The teacher has a possibility and task for "mapping" the individual capacities and capabilities of the students. Also, the teacher's task is to listen, from the background, "behind the curtain", to the students' learning strategy, to control the full learning process, to encourage, to activate the students and to support, if it is needed, the ones with difficulties to keep the team's pace and to well integrate into the team work.

The *"Lectures"* module is the second level of the learning process, the level of deepening the knowledge. The process is eased and supported by interactive elements including a systematic feedback/teacher's cooperation. The lectures are fundamentally being relied on an illustrative-explanatory method. The essence of this method lies in visually presenting, modelling the subject, even playing it, to the extent possible, and commenting and explaining it in a short text. The advantage of the method, that it presents the topic in one shot and in its context, at the same time, while directing the students' attention to the message. Notwithstanding, the very key element of all learning action is the perception, the cognition. For each participant, the progress made on his/her own, the self-relied development, will multiply the efficiency of the learning process.

The *"Practice"* module is to measure the level of acquisition of the knowledge. Both the teacher and the student receive a clear feedback on how and to what extent the latter has managed to acquire the learning material.

It is to be underlined: in order that the assessment can fulfil its motivating function, the teacher – based on the students' performance shown during the works of the Practice module – has to analyse everyone's difficulties in learning, continuously.

This module is to serve for strengthening self-confidence of the students, as well. Out of the works with different difficulty level of the Practices, everyone - in accordance with his/her own assessment regarding the level of knowledge already acquired by himself/herself - may select the appropriate one. The position of having an opportunity of the choice increases the student's autonomy sensation in the learning process. [5]

The opportunity of the choice among the works of different difficulty level increases the probability of the successful problem solving, as well, which influences the competence sensation advantageously, while the successful solution of the works strengthens the student's self-confidence, which is extremely important for both the intellectual health and the learning success, as well.

The "Stage" module is the level for acting and performing. It emphasizes the importance of "the acting school" the view that the "acting" is inevitable both for developing the thinking and for maintaining the interest. It gives an opportunity for the students to prove that they can apply their knowledge in practice. [6]

The student will select a case study out of the works in the "Practice" module, prepare its script, then present it, "play" the story and show the work's possible solutions.

The Stage provides with further experiences of joyful learning, it raises the lower status students' interest, too and increases their autonomy sensation and confidence. The Stage's atmosphere, being characterized by strong cooperation, enhances the inner motivation of the participants and a long lasting impact/endurance of being motivated, which may only be fruitful in such a learning environment, where the single, individual elements, the "players" themselves are strengthening and presupposing each other.

SUMMARIZING CTML'S CHARACTERISTICS

The specialty of the model, the interactive relationship between the teacher and student is created by e-books. As a result, the role of the teacher, the student and the learning material changes dramatically, compared to the traditional education.

The teacher plans and offers the learning materials, learning methods, learning techniques while takes into consideration the cognitive styles, the individual learning differences of the students.

Based on the offer, the teacher gives freedom of choice for the student. The student decides what is the best solution is for him/her in the given situation.

In teaching/learning process, inseparable from each other, the basic competence of the student expands, evolves on the 4+1 levels of the e-books.

The students get the skills to apply their knowledge, experience, personal facilities in the different situations of life. The model can be efficient solely by combined application of the three part-structures.

THE AGILE TEACHING / LEARNING METHODOLOGY (ATLM)

The Agile Teaching/Learning Methodology (ATLM), which has been successfully used at the City University of Hong Kong for a number of years, shows a lot of similarities to the Competence-base Teaching Learning Model (CTLM).

As their names (ATLM, CTLM) show they seek appropriate methodologies for teaching and learning. So the authors emphasize the teaching and the learning should go parallel, the teaching process and the learning process be inseparable from each other, connote and integrate each

other. “Teaching and learning (of course) go hand-in hand. ATML is a balanced methodology that supports both sides of the equation.” [2]

The Agile Teaching/Learning Methodology is an iterative Teaching/Learning Cycle, so the cycles of the methodology are performed over and over again in iteration. In ATLM there are two cycles that operate parallel in each iteration: one for the teacher and one for the student. (Figure 4)

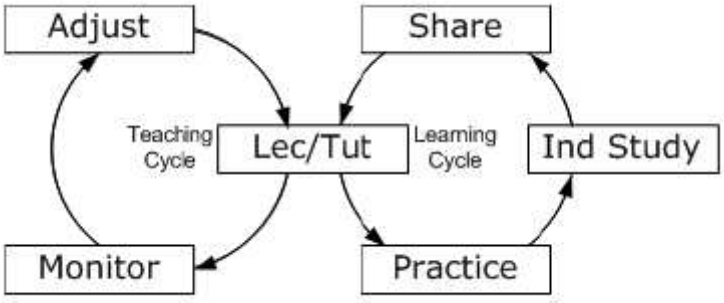


Figure 4. Iterative Teaching/Learning Cycles (ATLM) [2]

The Teaching Cycle is for the teacher to follow the student’s learning process, his/her professional and emotional development while the Learning Cycle is for the student to learn independently, to practice and to measure his/her knowledge continuously, to share his/her acquired knowledge with the teacher and the mates.

Both The Teaching and Learning Cycle share the Lecture/Tutorial task, so the contact is formed between the teacher and the student by the Lecture/Tutorial. In Competence-base Teaching Learning Model the e-book presents this contact, the e-book is „knowledge transfers”. (Figure No.1)

As we can see in Figure 4 the teacher’s one main task is to control the learning process. “The teacher must constantly monitor student progress as well as feedback from students on their own teaching progress/performance.” [2]

The systematic feedback is considered as a key element in both models. The feedback will only be able to promote and help the students in an effective way, if the teacher receives, in respect of the student’s knowledge level, as precise and up-to-date information as possible. Specifically, the ATLM emphasizes the immediate feedback, e.g. providing the students with the opportunity of a simple weakly quiz. As a result of the quiz, every student receives a feedback “in no time” on how and to what extent he/she has managed to acquire the learning material.

In the feedback the most exciting question is the statistics, the results should be anonymous or public. Whether can the weaker performance, the slightly worse result demotivate? Whether can the excellent performance motivate? Whether can the excellent performance increase students’ self-confidence? These questions are too complex and sensitive questions.

In the practice of the Competence-base Teaching Learning Model the quiz is anonymous, however the student can choose the other methods of the self-control, namely the project-work, cooperative-work, so can solve some tests together whit the mates, later can present together on the stage, so in the virtual classroom. In the project work, both the teacher and the partner students are expecting an active participation. They are expecting that everybody takes responsibility for the result of himself/herself and for that of the team, as well. Furthermore, every student will be a competent and equal participant of the learning process. In the course of the team works the students are realizing themselves that everybody possesses important intellectual abilities, even unique ones, through which anyone may contribute to the successful teamwork.

The above features strengthen another important specificity of ATLM: the Iterative Teaching/Learning Cycles, namely the teacher's support/adjust, so the teacher needs to follow the learning process, to intervene, to prepare schedules, learning-plans, to help the students to explore, research, acquire experience (Figure No. 4)

So the teacher needs to ensure students to get into an environment where they can get quality knowledge, and their brain is functioning well.

SUMMARIZING ATML'S CHARACTERISTICS

The key characteristics of the ATLM are the agility, the practice, the feedback, the independent study, the knowledge sharing and the adjustment. These values can operate the model effectively and can provide rich learning experience for the students.

E-LEARNING PLATFORM

The presented innovative methodologies have supported the e-teaching/learning in practice in higher-education institutions for a long time. However, a methodology without modern technology may not be viable. At the same time, the interactivity is a crucial function of e-learning Platform, what be called the spirit of the e-teaching and e-learning. The e-Learning Platform, the hardware and software environment have to be adaptive, namely in feedback, in pathway, in teaching/learning.

Adaptive eLearning is learning and teaching medium that uses an Intelligent Tutoring System to adapt online learning to the student's level of knowledge. Adaptive eLearning provides students with customised educational content and the unique feedback that they need, when they need it.

Adaptive eLearning creates the best possible learning experience for students by emulating the talents of great educators. This is achieved by using technologies that adapt and shape teaching to the needs of the individual student. Each student is unique, has varying levels of knowledge and learns differently. Researchers have found that students' performance improves when online educational content is personalized. The adaptive eLearning allows the teacher to create and teach with rich, interactive, and adaptive educational courseware.

I believe that teachers should have complete control over their students' learning experience, what Adaptive e-Learning Platform can support.

We know the students, when learning, often make mistakes. This is not anything exceptional. Would this happen, teacher has to provide feedback to students and has to guide them back to the right way. Adaptive eLearning systems allow teachers to do the feedback exactly when it is needed.

As emphasized, every student – like any human beeing – is different in many respects. Students have different levels of acquired knowledge; their problem solving approach is also different. Accordingly, teachers need to manage all the students and every student, individually. For example, if a student already knows what the classmates are doing or if a student would like to skip, ahead, to a more challenging task, or if a student has less knowledge in a topic, then teachers should be directed the learning to help to understand the concept and the relationships.

Adaptive eLearning systems lead students via different customized learning path, where the teacher attends, controls, adjusts, comments, where students need to demonstrate the understanding with a set of questions.

A good teacher approaches his/her students, their learning activity in an adaptive way. Teachers regularly adapt homework and assignments according to their students' performance. So, the teacher teaches while continuously learning how to teach better. As teachers are using

course-specific teaching/learning materials, they always need to adjust the teaching/learning environments starting from the online educational content to potential changes in the technological architecture, where they have certainly to work together with programmers and to rely on complex software systems. An Adaptive eLearning system has analytics tools that allow teachers to understand their students' learning and then modify their online lessons accordingly, as well as to improve their contents and teaching easily and continuously.

The CTLM (Competency-based Teaching Learning Model) – which is used at King Sigismund Business School – is supported by Moodle framework and it ensures the interactivity between the teacher and the students. This advanced technology is able to meet the requirements regarding the agility and appropriately sequenced communication.

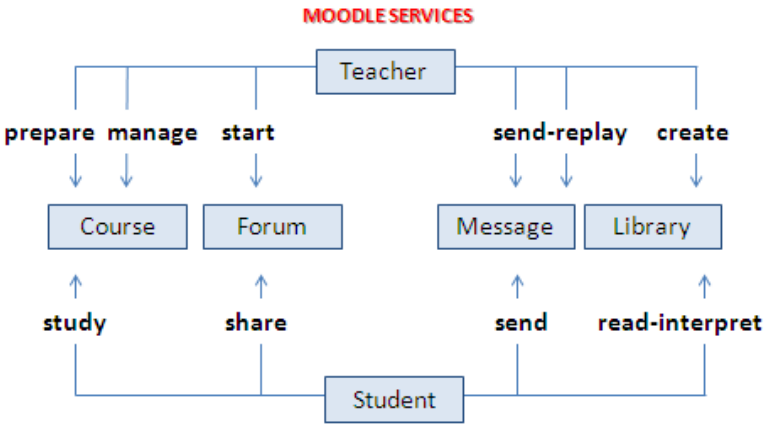


Figure 5. Moodle-services - the serves of the CTLM [1]

One of main features of the Moodle-framework is the WizIQ[1] Virtual Classroom integrated with Moodle to create new capabilities for synchronous learning - all within the LMS environment.

The WizIQ Virtual Classroom can simply be installed on the Moodle servers, then teachers and students can access the classroom seamlessly. All WizIQ functions – scheduling, managing classes, uploading contents, viewing records etc. – are accessible as beeing integrated in Moodle.

By WizIQ Virtual Classroom module, live class sessions can be implemented as Moodle activities and students from around the world can have seamless access to synchronous events within the context of a blended Moodle course.

Teachers can edit the schedule for their upcoming classes and make changes to the uploaded content, again and again directly within Moodle.

WizIQ Virtual Classroom records every time students log in and out. An attendance report is generated by the end of the virtual class-room lessons so the teachers can follow their students' time spent in learning and that may be an essential point of view in assessment of the students' performance.

All classes, all events can be recorded in WizIQ. Teachers can allow students to view the records online and/or to download them that they can use them at any point in time. The system sends reports to the teacher in a regular way (i.e. weekly) to show how often the recordings were viewed and/or downloaded by the students.

"WizIQ Virtual Classroom in Moodle" is a new opportunity to follow the students' learning, to develop the teacher-student, the student-student relationships and communication, when providing an effective and efficient feedback.

1 WizIQ is an online learning and teaching platform that connects educators and students through its WizIQ Virtual Classroom technology

Figure 6. Students can launch a recorded session directly from their Moodle course page WizIQ [7]

Obviously, a high level of sociability in the teaching/learning process is inevitable for the efficient operation of the presented educational models.

In this respect the sociability includes an adequate level of motivation and tolerance. In the teaching/learning process it is usually more difficult to teach how to think than what to think. Students have to be able to think critically and to learn to work – in addition to their individual efforts – together with others and rely on supports emerged by the common/classroom activity.

For an efficient use of WizIQ Virtual Classroom it is advisable for teachers to insert learning-methodology lessons for students-groups in each course held and, in this way, to teach the creative thinking, hard work ethic to give a sense of achievement etc.

The e-learning platform of the Agile Teaching/Learning Methodology (ATLM) provides a variety of collaboration and knowledge sharing technologies such as blogging, commenting, instant messaging, wiki and RSS, which technologies can develop the sociability, the students' adaptability to the community [2]

SUMMARIZING E-LEARNING PLATFORM'S CHARACTERISTICS

The adaptive education in the educational process of differentiation is the version in which the student can choose the different learning paths and goals, capabilities, knowledge correctly, and where there is not a special path between them, which would be more valuable than others. The aim is to align the education of students' individual differences in variable, dynamic and flexible manner in order to create optimal conditions for all students.

Represents on the one hand the student's the adaptation to the existing conditions, on the other hand, that the teacher tries the terms to adapt to the student's needs and their current status, attitude.

The essence of the adaptive learning organization the teachers need to learn how to harmonize their organizational, tutorial and educational activities and the students' basic needs. [8]

Adaptive education uses both computers and different web applications, as interactive teaching and learning devices. These tools adapt the presentation of educational material according to students' learning needs, as indicated by their responses to questions and tasks. Adaptive learning systems endeavor to transform the learner from passive receptor of information to collaborator in the educational process. [9]

In the cloud teaching success of teaching/learning is mainly technology-depending, as the teacher can display his ideas, the teaching-learning purposes, can stimulate the students, to help the lower status students, to develop the excellent students, can organize exams, cooperative-work, project-work, solely by technology. The technology encompasses aspects derived from

various fields of study including computer science, education, psychology and information security. The latter is an important issue for many reasons. The security professionals emphasize need to increase security, to defend the computer networks against the potential attacks as real threats. “Nowadays, computer is used more and more in our everyday life. As the number of computers increases the hazard of attacks against our computers is also growing.” [10]

In each sub-fields of the teaching-learning process, such as the testing, or to convey discipline- specific knowledge (e.g. unrated but sensitive information of the military engineering sciences) is required safe and reliable technique, so choosing the right technology is a priority task.

CONCLUSION

Teaching-Learning environments today are more complex than ever. The main questions are: How to teach? How to learn? Which pathways may be the most effective to teach the students? How to follow the students on the different pathways? What are the methods that we use to obtain information and integrate it within our knowledge base? And how are these methods of learning changing within a technologically connected global society? How to change reliable and safe technology?

At ever-changing teaching-learning environment more and more universities, schools, colleges, learning professionals have to be adapted to the cloud technologies and utilize the opportunities offered by them to better serve their students according to their individual characters, capacities, personalities; need to develop the learning materials, to continue and fine-tune research activities in the field of modern teaching-learning methodologies, to find the best pedagogical practices.

References

[1] Szegediné Lengyel Piroska: Tanulói kompetencia-fejlesztés e-oktatási modelljének korszerűsítése, Doktori értekezés, 2011.

[2] Andy Hon Wai CHUN: The Agile Teaching/learning Methodology and its e-Learning Platform, In Lectures Notes in computer Sciences – Advances in Web-Based Learning Volume 3143/2004, Spring - Verlag Heidelberg, pp.11-18.

[3] Szegediné Lengyel Piroska: An innovative methodology in compiling distance learning materials, Hadmérnök On-line tudományos folyóirat, V. évfolyam, 4. szám. 2010. december ISSN 1788 1919 http://hadmernok.hu/2010_4_szegedine2.php

[4] Falus Iván: Didaktika, Tankönyvkiadó 2003, p. 306; 382-385

[5] Montessori M, 1912. The Montessori Method. In The discovery of the child. Oxford UK, 1991. Clio Press Ltd

[6] Aebli, H. Lélektani didaktika, Budapest, Országos Pedagógiai Intézet, 1984

[7] WizIQ announces plugin for Moodle 2.3. http://lengyelpiroska.hu/moodle26/mod/wiziq/view.php?id=5 Retrieved: 2014. 08.10.

[8] Az adaptív tanulásszervezésről, Dr. Rinse Dijkstra, az APS (Utrecht) munkatársa konferencia-előadásai alapján, http://mag.ofi.hu/adaptiv, Retrieved: 2014. 06.12.

[9] Paramythis and Reisinger: Adaptive Learning Environments and e-Learning Standards, Electronic Journal of eLearning 2004. http://www.ask4research.info/Uploads/Files/Citations/ECEL2003.pdf Retrieved 2014.06.12.

[10] Dr. Kovács László: Az információs terrorizmus eszköztára, Hadmérnök On-line tudományos folyóirat, Különszám. 2006. november ISSN 1788 1919
http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.pdf
Retrieved: 2014. 06.05.

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Török Szilárd
torok.szilard@gmail.com

GOVERNMENTAL LEVEL SOLUTION REGARDING DATA LEAK PROTECTION

Abstract

Information and data being kept by the users carry security risks in themselves due to rapid technological changes. In case of systems with larger networks it is worth examining what approaches and expectations need to be determined against data leakage.
The present publication therefore investigates the security application options of DLP networks from the point of view of the current challenges of cyber security.

A gyors technológiai változás miatt a felhasználóknál tartott információk és adatok önmagukban hordozzák a biztonsági kockázatokat. Nagyobb hálózattal bíró rendszerek esetén érdemes megvizsgálni, hogy milyen adatszivárgás elleni megközelítéseket és elvárásokat szükséges megfogalmazni.
Jelen tanulmány tehát a DLP-k hálózati oldalának biztonsági felhasználási lehetőségeit kutatja a kiberbiztonság aktuális kihívásainak mentén.

Keywords: *data leak prevention or data leak protection (DLP), endpoint protection, network DLP, Centralised Governmental IT System, National Info-Communication Service Provider ~ Adatszivárgást megelőző rendszer vagy Adatszivárgás elleni védelem, Végponti védelem, hálózati DLP, Központi Kormányzati Informatikai Rendszer, Nemzeti Infokommunikációs Szolgáltató Zrt.*

INTRODUCTION

The abbreviation DLP derives from Data Leak Protection or currently Data Loss Prevention. [1] The technological solution itself has a 15 year history. At first it was carried out only by disabling the different ports of the endpoints, later by controlling the incoming and outgoing data and files.

Around 2001-2002 in Hungary a solution was introduced that was developed by Hungarians, which was able to alarm or block based on certain behavioral patterns, then around 2004 it was suitable for more complex analysis such as: clipboard content control, print screen saving as evidence, separate management and regulation of user and desktop computers, the special control of applications and new policies based on collective functioning.

Around 2007 the monitoring, filtering solutions on network side turned up which were able to provide a solution for data leakage prevention during network functioning, along network protocols and according to different directions and content of the network.

The two types of – endpoint and network – DLP clearly pointed into one direction, namely a product that combines both functions.

The generally accepted definitions and their solutions were settled in the past few years, at the same time due to the multiple endpoint and network DLP solutions and the newer and newer special attacks and data leakage several approaches were developed.

Data leak protection however is far not a product, but the issue of real intention and resources on the client side. Even a good choice of solution can cause managing difficulties in the DLP system, eventually the time and energy invested in its introduction will not necessarily pay off.

Due to the related costs and the resource requirements of the process organization it can be clearly concluded that the selection and introduction of any DLP solution needs to be subject to a strategic decision and this is why DLP requirements expectations becomes necessary in government-wide planning.

The goal this publication therefore explore bases and security options of DLP solutions therefore to answer of the current challenges of cyber security.

General introduction of DLP

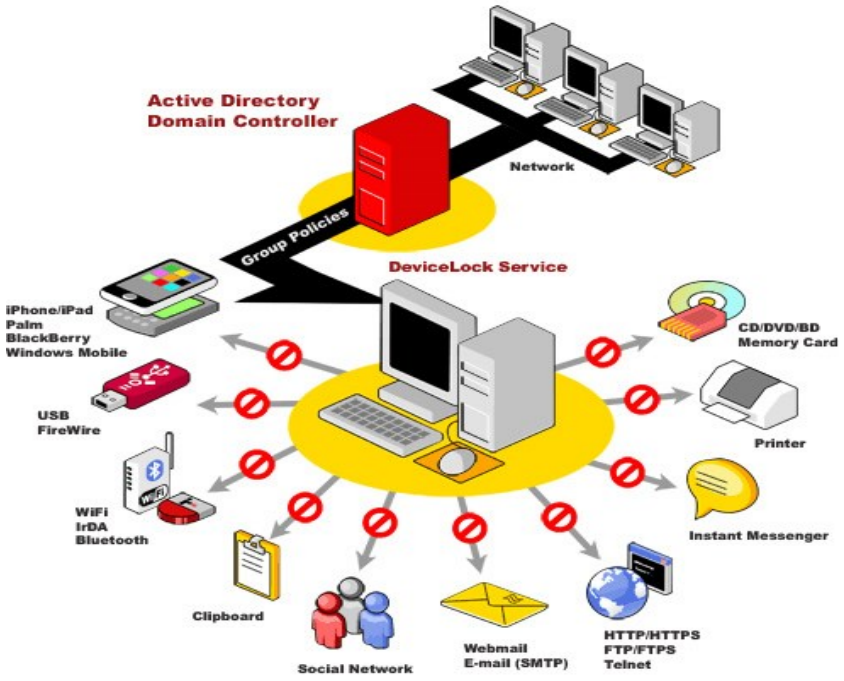
It has to be defined what general goals can be expected from a DLP solution:

- It is an efficient tool against internal threats
- It is a tool for enforcing IT security policies
- It supports the daily work of the security manager
- Built-in security concept, protection profiles
- Risk proportionate IT security can be developed
- Process based, minimum realistic approach
- Detects – incidence, frequency, alignment
- Reaction – approves, logs, disables, blocks, alarms.

A complex DLP solution includes central management, policy establishment, policy enforcement mechanisms that were developed specifically for this purpose.

The real users of the system often do not possess profound technological expertise (this cannot be expected), and are mainly from the fields of work process, data security, business management or law.

It is therefore necessary that the interface and policy generation of the system should be easily comprehendible and operable from a technical point of view even for laic users.



1. Figure. Device protection
http://biztonsagportal.hu/interju-kiterjesztett-adatszivargas-megelozes.html

The system is expected to be centrally manageable: separate interfaces are necessary to determine the data to be protected (eg. HASH), to develop the system of policies, to monitor the data flow, to intervene and to generate reports.

It is furthermore necessary to determine different user levels and authorizations.

2. Figure. The process of insider threat and its possible consequences source:
www.GTBTechnologies.com

Three DLP solution types, or approaches exist which will be described below.

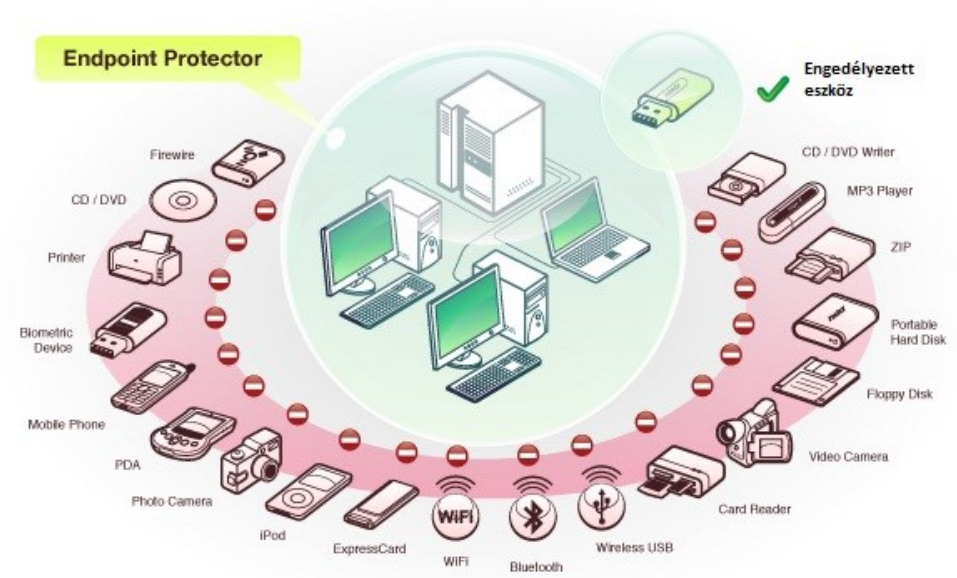
DLP approach: Endpoint DLP protection

The Port Protection approach provides solution almost exclusively for Windows clients, and typically tries to control the external communication channels, ports on desktops.

It derives from the approach itself that most of the solutions are not able to take the source of the data (eg. which directory or server) into consideration during data motion, moreover it does not include process/value generation based regulation.

The technical consequence of endpoint approach or DIU (Data In Use) [2] is that it can only operate with kernel driver level agents. This approach can cause system level clashes in case of compatibility and system updates.

Without proper developments and tests the client might face serious stability problems. An error like this may cause partial or complete Windows based client side breakdown, or it provides access with partial authorization. There were some unfortunate examples like the above in the case of Hungarian developed products, at the same time there was a significant improvement in stability.



3. Figure. Protection of endpoint
www.relnet.hu

DLP approach: Right Management

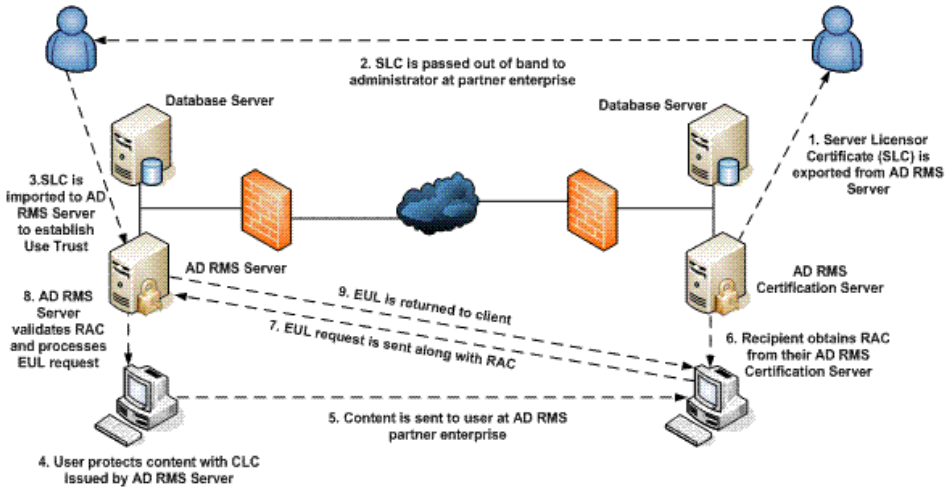
The basis of Microsoft RMS (Right Management Services) [3] is an open source encryption algorithm in which identification and/or encryption is implemented with the usage of two asymmetric keys.

The hindering of the leakage of confidential information is implemented by protection of the content and regulation of content usage. One of the possible leakage methods – among the first ones – is the intentional or unintentional forwarding of e-mails that can generate access to confidential data.

The goal of the RMS solution is not encryption, but the generation of a fingerprint that is typical of the original data. The simplest and most available RMS system is Microsoft RMS. Microsoft integrated this system into all of its current operations systems and its own Office product, and provides these products with the above system.

The RMS system is an XrML based Net web service which possesses a hierarchic and redundant architecture. It generates fingerprints with HASH algorithm.

The RMS clients work through API calls [4], the security calls are executed by a special DLL (Lockbox that manages the private key of the computer). Both, the computer and the user possess an internal certification.



4. Figure. RMS Trusted User Domain
http://technet.microsoft.com/en-us/library/dd983944%28v=ws.10%29.aspx

This RMS system is not compatible with other PKI solutions, not even with Microsoft's own PKI solution. Reason of this is that oddly their own asymmetric key system is operated to maintain dynamic operation. The utilised algorithms are similar to the PKI (RSA, AES), the certifications are in XML formats, and for the SSL web service an X.509v3 certification is necessary.

The vital attributes, advantages of RMS concerning data leak protection:

- Limited content access (Outside the RMS system it is not possible to read the document).
- Modification and printing can be limited
- Encrypted e-mail that can be only read by the recipients.
- The readability of the e-mail is limited in time.
- Control of Drag and Drop
- Copy/Paste blocking in case of copying from a protected document.
- Print Screen control
- It can be integrated with SharePoint, it automatically protects the content according to the user authorisations.

The disadvantages of the solution are worth mentioning – during the testing and usage of RMS the following deficiencies could be revealed:

- The optional templates are of limited availability: eg. maximum 20 templates are indicated, despite the fact that more templates have been defined in the system.
- Version control does not operate properly in case of MOSS 2007 integration
- Besides protected Office documents it is only possible to extend the range of RMS to (some) other types only with complementary (not Microsoft) products. In this case the risks concerning file filter drivers can increase, it is recommended to set up an independent file server with the activation of RMS extensions for the specifically protected documents.
- In some cases the clipboard operations are completely shut down when opening a protected document, which at the same time makes it impossible to use the copy/paste functions within the document.

DLP Approach: Content Filtering

The SANS Institute defines the DLP [5] in the following way: „Products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use, through deep content analysis."

Thorough content analysis, central policy system and the ability to manage the content on more platforms and locations have to be emphasized in the definition. If we choose this solution, the DLP system not only protects the sensitive data, but helps adjusting the policies and the technical policy system generated from them to the actual data flow.

Nowadays the primary goal of the introduction of a data leak prevention software is the detection, monitoring of data leakage in the web traffic and e-mail traffic of certain organisations and partners. In case of IT operation in public administration the recon of sensitive data on the central SharePoint server has to be emphasized.

Content recognition

According to the Content Filtering approach the task of the DLP solution is the precise recognition of content. Taking into consideration the fact that information flows in an unstructured way in many cases, the recognition of the context is of key importance (to whom, from who, when, in what form, with what other information) which not only increases the accuracy of recognition, but decreases the frequency of false alarms.

Moreover, the knowledge of numerous file formats is necessary in order to analyse the content. Analysis typically means fingerprint recognition, policy based recognition, document or document section recognition or statistical analysis.

Architecture

A good DLP solution is able to recognise the data at rest (on work stations and file servers), during motion (at any point in the network at gateways or near them) and during usage (copying, printing, e-mail sending), and is able to interfere in its usage if it is necessary.

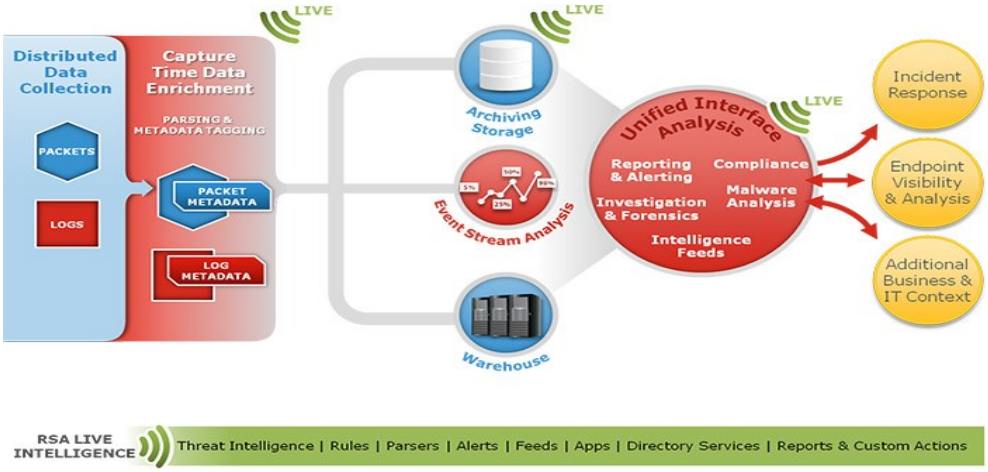
Regarding architecture the network DLP solution has a network sensor (in bridge or monitoring mode), gateway protection (e-mail and web-gateways, print-and file server modules can be accessed), and an endpoint application. Thus the protected information can be managed at any point. With the integration of PKI solutions of third party manufacturers the system is even able to recognise encrypted data contents.

Another vital ability lies in HASHING, namely in intense language analysis which is able to recognise confidential information in an intelligent way regardless of the language. For structured data formats (eg. credit-card number, bank account number, personal identification number, ID card number, etc.) separate definitions can be developed, furthermore these are mostly predefined in the system. The outstanding content recognition abilities are the core of these solutions which can operate equally on multiple levels of the IT infrastructure (network, gateways, end point).

Regarding data protection those data needs to be monitored that on the one hand can be defined with the help of keywords and regular expressions, on the other hand they are stored in highly protected systems.

In order to be able to monitor traffic towards the internet a sensor device needs to be set up. The sensor primarily analyses the communication on SMTP, HTTP protocol according to their data content, but the device is able recon and analyse data content in other protocols (eg. FTP, Telnet, POP3, IMAP, AIM, MSN).

As a matter of fact the sensor works like and IDS, therefore the traffic to be analysed needs to be monitored through one SPAN port of the central Switch.



5. Figure. RSA Data Loss Prevention Network
http://www.emc.com/security/rsa-security-analytics/images/chart-sa-marketecture-700px.jpg

With this solution it can be completely excluded that it would impact the procedure continuity due to malfunction of the device or due to a incorrect configuration. That traffic needs to be mirrored to the SPAN port, through which the outgoing (leaving the organisation) traffic of the appointed organisations can be monitored. Certain traffics can be distinguished by defining IP addresses and address ranges.

In order to be able to distinguish certain people and organisation units the DLP system can be implemented by connecting to a central address storage system. This way the monitoring policies can be directly assigned to people and organisational units.

In case of content monitoring policies data surveys need to be conducted at the involved organisations in order to be able to determine those data categories which will be monitored by the DLP system.

It is necessary to create a classification pattern or the default profile of the DLP system needs to be used.

As a result of policy system planning two types of sets of policies can be developed:

- Set of policies which determine what classification a file/document should be assigned. Based on these designations the user of the system can decide the relevance of certain incidents.
- Set of policies which determine the management of designated files, namely which user operations are allowed and which are not in the given data category (whether e-mail sending is allowed).

REVIEW OF CENTRAL GOVERMENTAL IT

The goal of the Digital Renewal Action Plan [6] 2010-2014 – as a tool of the national info-communication development strategy formulated in the New Széchenyi Plan [7] - is the utilisation of modern information and communication technology in order to ensure transparent, more secure, cheaper and more efficient operation of the state.

Central Governmental IT System

In accordance with the directives of the European Union and the central goal of the Hungarian Government to improve the efficiency of public administration, the implementation of a Centralised Governmental IT System (KKIR) was finished in October 2013. [8]

The project is the organic continuation of the Standardised (IT) Infrastructure Programme (EIP) launched in 2008 then suspended in May 2010. In the framework of EIP the integration

of IT systems, IT networks and applications used by the institutions has been launched in certain institutions of central public administration.

The primary goal of the KKIR project was to replace the non-branch specific IT elements operating in certain institutions by centralised services, thus unjustified parallel developments and unnecessary operational expenditures can be avoided. This way the advantages of basic and advanced level infrastructural and network data transfer services can be utilised by the employees in public administration.

The extremely important fundamental principle of an efficient and unified governmental IT is a central architecture that is able to serve the institutions in a centralised and standardised way.

The Government Decree of 1314/2010. (XII.27.) named the Centralised Governmental IT System Development project [9] as an accentuated project, and the National Info-communication Service Provider Ltd. (NISZ) was assigned with the implementation of the project.

The company as the operator of the governmental info-communication infrastructure primarily provides governmental IT solutions (through the National Telecommunication Core Network – NTG).

309/2011. (XII.23.) Government decree [10] the category of centralised IT and electronic communication services that are provided by NISZ, and defines the category of those organisations which are obliged or entitled to use these services.

The results of NISZ in central operation

In the framework of KKIR such a complex system was developed that makes it possible to operate a secure, high quality and cost efficient info-communication infrastructure and basic service in the central government.

By the end of the KKIR project the Standardised Infrastructure will provide services to the Ministries. The direct target group of the project will be the institutions of central government (abbreviations: NFM, EMMI, NGM, VM, KIM, BM and the Prime Minister's Office) the employees and associates of these institutions.

Throughout the project the central address storage was standardised (domain-consolidation), obsolete work stations (2640 pcs PC, 350 pcs notebook) were replaced by modern devices and theye were installed with a standard environment in order to be able to operate the newly introduced management systems efficiently operated by NISZ. [11]

Identical, modern platform was installed at the new desktop environment, and OPEN Doc Format (ODF) was set as default.

As a result of the new management systems now a standardised system supervision and software management operate within the Standardised Infrastructure. Within the framework of the project, group work applications were installed where remote access is provided as well. Regarding technical content a shift to Windows 2008R2, Exchange 2010, SQL Server 2008, SharePoint Server 2010 systems was implemented.

In the framework of KKIR project NISZ Ltd. developed a mutually substitutive (geo redundant) server environment – 46 pcs new server, 1 pcs new computer room, 2 pcs redundant storage, 2 pcs redundant devices for e-mail archiving were procured and put into operation. With these devices the availability time of the extended EI system can increase, and the quality of the service is improved with the operation and IT security solutions.

In order to modernise the network infrastructure the firewall system was improved, the institutional internal backbone networks were made redundant, and the external station connections were extended so that each station would operate with standardised, redundant network connection.

NISZ IT Security

The reorganisation of NISZ started in February 2012 with the appointment of the new CEO and reorganisation of the management which accelerated the reorganisation process. The management's mission was that NISZ would provide high quality, cost efficient and reliable electronic services to its users – public sphere, residents and businesses – which help their clients manage their everyday activity easier, faster, environmentally responsibly and securely.

In May 2012 an independent IT Security Directorate started to operate at NISZ Ltd. Its goal was to develop a standardised, transparent, controllable and homogeneous IT security system and policies in the field of IT security and regulation that operate according to effective laws, standards and professional recommendations.

In 2013 the staff of IT security directorate was significantly extended in accordance with new tasks and projects.

DLP IN GOVERNMENT

Selecting DLP type

The proper DLP solution needs to include the following type of solutions by SANS Institute [12]:

DIM (Data In Motion): The DLP network component should continuously monitor and track network traffics:

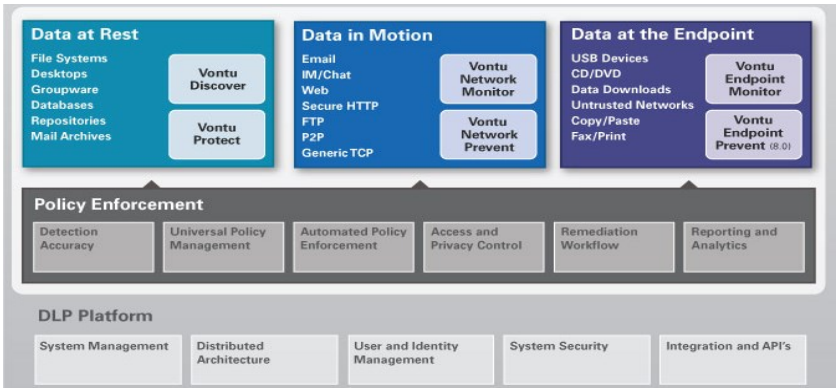
- Make sensitive information exiting the system measurable on a risk level.
- It should monitor and log (should be able to block) the unauthorised forwarding attempts of sensitive data in real time.

DAR (Data At Rest): It should protect the data stored on network resources (file servers, databases, etc.) from unauthorised actions.

- The system should be scalable
- It should reveal the sensitivity of the data available in file sharing, SAN/NAS systems, databases and other records.

DIU (Data In Use): The endpoint protection component should continuously monitor and track sensitive information stored in work stations and user activities, and prevent data leakage incidents:

- It should seek and protect sensitive information on desktops and mobile computers
- It should provide real time protection



6. Figure. DAR, DIM and DIU in Vontu solution
http://www.emagined.com/vontu_data_loss_prevention.php

Based on these types and taking the Centralised Governmental IT System into consideration basically the network DLP solution type can result in an efficient IT security solution.

The usage of network DLP in Governmental IT

The network DLP solution can be applied in the standardised IT system of the Government, and its advantage is that its usage does not require substantive user contribution, the operation of the system does not influence their activity.

The goal is to control data motion and hinder the exit of data from protected environment through communication channels.

It depends on the manufacturer how many communication channels the product is able to control, but the basic goal of the product is to control FTP, HTTP channels, e-mail and instant messaging channels and encrypted channels.

Cloud based communication might be integrated into the abilities of the systems, this is important because a cloud solution was developed on governmental level (Governmental Cloud, abbreviations: Gov-Cloud or KOF [13]).

Depending on the choice of solution the communication channels either need to be filtered natively or using an external supplier's product.

The internet traffic can be analysed with the usage of some kind of a proxy server, electronic mails are in many cases controlled through e-mail filtering applications. It is of great advantage if the DLP system can cooperate with as many products of external suppliers as possible.

Besides the control of communication towards the external world, the control of internal network traffic can be also the task of DLP.

Besides the usage of proxy servers the ability of monitoring the network is a useful and important attribute. Generally the systems can monitor (eg. on a Switch SPAN port) the traffic with some kind of a mirroring method, but other methods can be applied as well in case they do not weaken the performance of the system and the malfunction of the device does not jeopardise normal task management.

Internet network management

The traffic can be mirrored by the system or can be monitored other way. The normal management cannot be affected by monitoring, at the same time each port needs to be monitored.

Intervention/modification in traffic: the DLP solution monitors the traffic, and if necessary, it can intervene. This can take place natively (intervention in TCP session) or with a third party software (web proxy, e-mail filter).

The network component of the DLP system should be able to recon sensitive data transmitted through the network, to monitor traffic and block traffic:

- In case of monitoring the network the system should support the following protocols and systems: HTTP/HTTPS, FTP, SMTP, POP3, IMAP, AOL, IM, Google IM, MSN IM, Yahoo IM, Telnet.
- An incident should be generated if a policy breaching data transmission takes place.
- In case of blocking network actions the analysis of SMTP, HTTP, HTTPS, FTP, ActiveSync should be supported among network protocols. The system can execute the following actions with the data breaching the policy system: logging, blocking, in case of a policy breach on SMTP protocol in addition to the above quarantine and encryption can be executed.
- The system should support the monitoring of data traffic between e-mail boxes in internal e-mail systems (Microsoft Exchange).
- The system can execute the following actions with the data breaching the policy system: logging and blocking.

E-mail filter integration
Electronic mail is one of the most important channels, the filtering of this is of key significance.

It is expected that the DLP system can be integrated to a third party email filter application. It has to know Microsoft Exchange and Lotus Notes from the email sending systems minimally.

Proxy integration
Assuming a centralised internet exit, a web proxy server needs to run the complete internet traffic.

The task of web proxy applications is content filtering, thus they can analyse the incoming and outgoing packages which is expected.

It should be able to look into the SSL connection with the help of a proxy or with an own solution.

Internal network
DLP systems are typical installed concerning border protection, but the monitoring of internal network traffic might be expected.

Managing mobile devices: it should be able filter the traffic directed towards the mobile devices. Managing clouds: it should be able to filter the internal traffic directed to the Gov-Cloud.

Managing virtual devices: the simple cloning method of virtual devices pose multiple risks from a data leakage point of view, thus this problem should be tackled by the DLP system. As a result, complete functionality can be expected in case of virtual devices.

Endpoint protection in the Government

Endpoint usage: the components installed on the desktop and mobile work stations need to continuously monitor the end users' activity in real time, and if necessary it needs to be able to intervene as well.
The following general functional expectations can be formulated:

- Printing: The system does not allow the transfer of sensitive data to the printer.
- Clipboard management, print screen saving: In case of a file containing sensitive data, the disabling of print screen and clipboard restricts the potential channels of data leakage. If a sensitive document needs to be made available to a larger category, then this ability can be especially useful.
- Mobile devices: On mobile devices it is possible to take out great amount of data from the organisation in a short period of time, thus avoiding border protection. It is important to be able to control the physically connected mobile devices at each endpoint: USB key, mobile wreck, CD, DVD, etc.
- Disabling applications on using sensitive data: It should be limited through which application should be the file containing sensitive data accessed. The file level access management can be adjusted by proper authorisation management of the applications.

DLP answers to incidents

- Incidents can be reacted by several actions depending on the fact what is the level of the incident. The scale can range from reporting to deleting the file (or database) containing the sensitive data.
- Reporting: The incident will be recorded. The record can be retrieved if it is necessary or it can be included in a regular report. This is a detective control, it is not able to hinder the leakage of sensitive data.

- Explaining the incident: It requires an explanation from the user before any action that can jeopardise sensitive data. If the user cannot explain the action, the action will not be executed. This a detective control too, it is not able to hinder intentional data leakage. However, it is able to reduce unintentional data leakage.
- Quarantine: The file containing sensitive data needs to be placed in a quarantine. The file placed in quarantine can be only accessed by the authorised users. It is a preventive control, leakage of sensitive data can be hindered with it.
- Encryption: The system encrypts the object containing sensitive data. It is a usual function when sending an email. It is good for reducing unintentional data leakage, but it does not protect against hostile activities.
- Deletion: The object containing sensitive data is deleted. The usage of this function is not recommended, or just with very reasoned settings and control – given the fact that it can result in serious data loss.

Recon on data storages

In order to hinder data leakage it is important to know what kind of sensitive information is contained in the data assets of the organisation and where they are located. The mapping of this is important task of the DLP system.

The attribute of a professional DLP system is that it can manage several types of data storages and mapping does not cause problems in performance.

According to new data storage practices, it is important to be able to manage virtualised storages and data stored in Gov-Cloud.

As a result of the mapping, it can be seen where the data is located in the data asset that meets the predefined criteria, furthermore it can make a Hash from the database or file that are considered important. During future searches these hashes can be monitored in other databases, files or communication channels, thus hindering the leakage of these files or databases.

- Managing scanned files, databases: A report should be made based on a search according to the defined policies. It is useful if the system sends feedback about certain assigned files or databases. It is expected that the object containing sensitive data can be transferred to quarantine, can be encrypted or deleted.

SharePoint, Linux and Windows file servers, SAN and NAS

It should be able to map the data assets and search in it with the above described analysing techniques. Usage is significantly easier if only a certain part of the directories can be controlled.

In case of file server sharing the control of CIFS, NFS and WebDAV based sharing is expected, furthermore it should recognise and list encrypted files as well.

Oracle, MSSQL, IBM DB2 and other optional databases: Mapping data assets with the above described analysing techniques. The time and method of mapping can be configured.

- Fingerprinting: The system can efficiently generate fingerprints of great amount of data. The fingerprint generation should be configurable and schedulable.
- Pattern search: The sample search (fingerprints, regular expressions, dictionaries, etc.) on the devices under monitoring should be executed as efficient as possible.

The system should be able to do split search and scheduled search. The endpoints and servers should participate in the search through the installed Agents.

Managing user interfaces and users

The status of external components of the system should be easily accessed, if possible from one location. It should contain the version of the component, the date of the latest updates and information on what sample search it executes. The management of the components should be executed from the central interface.

Reports, alarms or status reports of components should be indicated on the home page in a customised way.

The system should be connectable to AD (Active Directory). The registration of new users and identification should be done through the AD. The system should be able to generate cues. These cues should be assigned to AD groups.

It is more advantageous if it can manage the given DLP system with the better known Identity Management systems.

Incident management

In case of breaching the policy system the solution needs to provide a review into the incidents (arranged into incidents), set a notification and provide manual remedy or request a notification about the solution.

The filtering and arranging aspects of the incidents should be able to process identification number, date, type (network, datacentre, endpoint) severity, status, validity, the person/group assigned to the incident, policy breaching user, protocol or action, breached policy and action taken by the policy.

Status and person/group need to be set as search terms in a given time interval, furthermore it has to provide filtering terms for the search or exception management and the search itself could be saved (in a modifiable way).

The system automatically assigns the following to the incidents:

- identification (assigning to person or group)
- details of the incident (who committed a breach in the policy, when, with what, and what kind of policy).
- what was the reaction of the system
- severity level
- validity setting
- investigation (to whom the incident can escalate) of responsible (person or group)
- investigation of deadline
- status
- possibility to comment
- sending email notifications

All the aspects can be searched among the incidents, and besides a search can be executed according to the organisation of the perpetrator and deadlines.

Certain phases of investigation of incidents can be commented. The status of the investigations can be followed by the authorised staff. The incidents should be exportable into generally used formats.

Reporting possibilities

The system should have its own built-in report compilations. These on the one hand help prepare for audits (eg. PCI DSS), on the other hand they serve as a sample for preparing own reports.

The reports should be embraceable and comprehensible for those who come from the field of business.

The system should make it possible to generate summary reports according to the following aspects:

- according to organisation
- according to incident type
- according to breached policy
- according to data definition
- according to severity
- according to status
- fulfilment/compliance summary

The system should be able to generate trend indicator reports according to the following aspects:

- according to organisation
- according to device type
- according to incident type
- according to breached policy
- according to severity
- incident remedy trend indicator

Data center component

The data centre component of the DLP system should be able to recon the sensitive data in the systems below:

- File server sharing
- Database servers
- Data storages

In case of file server sharing the analysis of CIFS, NFS and WebDAV based sharing can be expected.

Based on the policy system the following actions are indispensable regarding the files: logging, deletion, modification of file authorisation, moving to dedicated directory, quarantine, authorisation, execution of automated counter actions (based on policies).

Throughout the analysis of database servers Oracle, Microsoft SQL and IBM DB2 database management systems are supported.

Throughout the analysis of data storages Microsoft SharePoint, Microsoft SharePoint Online (Office 365), Lotus Domino and Microsoft Exchange Server should be supported.

SUMMARY

In order to prevent governmental level data leakages, basically the introduction of a network type DLP solution is recommended in the centralised governmental IT system.

Based on the review of DLP solutions, my previous publications about governmental cyber-attacks [14][15][16][17], and analysis of possible requirements the following most important requirements can be formulated:

- Filtering network traffic
- Analysis of file sharing on network storage
- Control of endpoint activity
- Indexing of file or database content, recognising coherent data
- Recognition of encrypted files

- Recognition regular expression based data
- Management of previously built-in policies based on international standards
- Integration of Active Directory
- Preservation of original files, emails as proof in case of alarms
- Management of built-in alarm and incident management work processes
- Automatic severity classification of alarms
- Supporting analysis of alarm, comprehensive report generation and filtering
- Adjusting to logging and analysis systems

In case of a governmental level introduction the DLP solution might need to be extended with a system managing mobile devices (Mobile Device Management – MDM).

It has to closely cooperate with the logging and analysis systems of NISZ and with the operated specific systems, furthermore a customised access needs to be developed for the Governmental Incident Management Centre (Gov-CERT) to implement special queries and searches.

References

[1] *Data Loss Prevention* in Wikipedia (12 march 2014), The Free Encyclopedia, downloaded: 5 May 2014, source: http://hu.wikipedia.org/w/index.php?title=Data_Loss_Prevention&oldid=13290439

[2] *Data In Use* in Wikipedia (12 march 2014), The Free Encyclopedia, downloaded: 5 May 2014, source: http://en.wikipedia.org/w/index.php?title=Data_in_Use&oldid=599357970

[3] *What is Microsoft Dynamics Retail Management System (RMS)?* Microsoft, downloaded: 5 May 2014, source: http://www.microsoft.com/dynamics/dynamicsrms/retail-management-system.aspx?pageID=1

[4] *Application Programing Interface* in Wikipedia (10 Jun 2014), The Free Encyclopedia, downloaded: 11 Jun 2014, source: http://en.wikipedia.org/w/index.php?title=Application_programming_interface&oldid=612421786

[5] *Understanding and Selecting a Data Loss Prevention Solution,* SANS Institute, 2007, downloaded: 12 May 2014, source: https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf

[6] *Digital Renewal Action,* Hungarian Government, 2011, downloaded: 12 May 2014, source: www.nih.gov.hu/download.php?docID=24683

[7] *New Széchenyi Plan,* Hungarian Government, 2011, downloaded: 12 May 2014, source: http://palyazat.gov.hu/uj_szechenyi_terv1

[8] *Realize of Modernized the Centralised Governmental IT System (KKIR),* Hungarian Government, 2011, downloaded: 12 May 2014, source: http://www.nisz.hu/node/110

[9] 1314/2010. (VII.27.) Government decree about Centralized Governmental IT System Development Project

[10] 309/2011. (XII. 23.) Government decree about services of the Centralized Information Technology and electronic newscasts

[11] *Close up EKOP KKIR project at National Info-communication Service Provider,* NISZ Ltd., 12 Dec 2013, downloaded: 12 May 2014, source: http://www.nisz.hu/node/209

[12] *Data Loss Prevention,* SANS Institute, 2007, downloaded: 12 May 2014, source: https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf

[13] Governmental Cloud System, Hungarian Government, source: http://kof.hu/informaciok

[14] Török Szilárd: „Some Aspects of cyber attacks in 2011", Hadmérnök, VI. Évfolyam 2. szám; http://www.hadmernok.hu/2011_2_torok.pdf

[15] Török Szilárd: „Hungarian experiences in the light of cyber attacks in 2011", Hadmérnök, VII. Évfolyam 2. szám; http://hadmernok.hu/2012_2_torok.pdf

[16] Török Szilárd: „Anonymous in the World and Hungary", Felderítő Szemle, 2013. XVII. 3-4. ISSN 1417-7293, page 228-243.

[17] Török Szilárd: „Hungary's cyber defense readiness from the perspective of international recommendations", Hadmérnök, IX. Évfolyam 1. szám; http://hadmernok.hu/141_20_krasznaycs.pdf

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

DIAMANT PÉTER KAMILLÓ - FEKETE LÁSZLÓ - NAGYGYÖRGY ÁDÁM - ZENTAI ÁGNES
r@zmne.hu

EXTRACORPORALIS LÖKÉSHULLÁM KEZELÉSSEL SZERZETT ELSŐ TAPASZTALATAINK DIABÉTESZES LÁB KEZELÉSÉBEN (ESETISMERTETÉS)

Absztrakt

A diabéteszes láb szindróma (diabetic foot ulceration /DFU) a cukorbetegségben szenvedők populációjának 4-10 százalékát érintő súlyos szövődmény, amely egyben ezen betegek kórházi kezelésének egyik leggyakoribb indikációját is képezi. A számos preventios és therapiás protokoll használatának dacára a cukorbetegeknél az alsó végtag-amputáció gyakorisága tizenötször nagyobb, mint a nem cukorbetegek körében. Jelen esetünkben az 58 éves, 23 éve II.típusú diabéteszben szenvedő férfibeteg mindkét lábát érintő, nagyméretű talpi fekélyek kezelését extracorporalis lökéshullám (RSWT) kezeléssel egészítettük ki. A sebgyógyulás aktuális fázisához adaptált kötszerek használata mellett az extracorporalis lökéshullám kezelést hetente kétszer alkalmaztuk. Az általunk beállított kezelési eljárás mellett a talpakat érintő elváltozások begyógyultak, a beteg jelenleg is panaszmentes.

The diabetic foot ulceration (DFU) is a severe complication which affects the 4 – 10 percent of those who suffer in diabetes. This makes also one of the most common indications for hospitalization. Despite the several preventive and therapic protocols the lower limb amputations are fifteen times more frequent among those who suffer in diabetes compered to the heathy populations. In this case our patient was 58 year old, suffering in type II diabetes for 23 years. Both of his legs was affected with DFU. Beside the usages of bandages adapted to the phaese of wound healing, the extracorporal shockwave therapy (RSWT) was used twice a week. Our therapic method led to the full recovery of the lesions affecting both soles. The patient is asymptomatic still today.

Kulcsszavak: *diabéteszes láb szindróma, radiális extracorporalis lökéshullám, adaptált kötszer választás ~ diabetic foot ulceration syndrom, radial extracorporal wave therapy, adaptic wound bandage*

BEVEZETÉS:

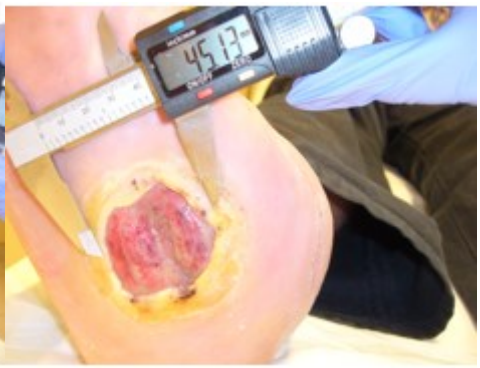
A diabéteszes láb szindróma a cukorbetegség jellegzetes, mindamellett szélsőséges megjelenési formákkal bíró tünetegyüttese. Alapját heterogén patológiai elváltozások – úgymint a neuropathia, a micro- és macroangiopathia, -a következményes statikai eltéréseket okozó csont-, valamint ízületi elváltozások képezik.(1) A tünetegyüttes legsúlyosabb szövődménye a seb kialakulása, ami a betegek mintegy 10-15%-nál jelentkezik. Az irodalomban fellelhető adatok szerint a seb gyógyulását követő első évben a seb 40-80%-ban kiújul.(2) A kialakult sebek teljes gyógyulása leggyakrabban meghaladja a 12 hetet, még a leggondosabb, legkörültekintőbb kezelés ellenére is. Napjainkra kialakult modern sebkezelés fogalma a modern kötszerek, valamint az individualizált sebkezelési módszerek egységét jelenti. A sebgyógyulás mechanizmusában a gyulladást sejtmigratio, sejtnövekedés, angiogenesis, extracellularis matrix-synthesintesis és remodelling, végül epithelisatio követi. Ezen folyamatok szabályozásában jelentős szerep jut a különböző növekedési faktoroknak. A mesterségesen előállított faktorok közös jellemzője a hőlabilitás.(3) Jelenlegi tapasztalataink szerint az extracorporalis lökéshullám elősegíti a különböző növekedési faktorok lokális felszabadulását, következményesen stimulálja az angiogenesist, így támogatja az erek növekedését, a sejtproliferatiot.

ESETISMERTETÉS:

Az 58 éves férfibeteg távoli anamnaesisében 1993-óta kezelt hypertonia, 2002-ben diagnosztizált, -évek óta insulin therapiaval kezelt- II típusú diabetesz szerepel. 2008-ban lumbalis microdiscectomia történt a betegnél. A folyamatos diabetologiai gondozás mellett 2005-ben a bal, majd 2011-ben a jobb talpon is nagy kiterjedésű fekély alakult ki, amelyek az alkalmazott kezelés mellett sem mutattak jelentős gyógyhajlamot.

2012 áprilisában a lökéshullám kezelés megkezdése előtt a betegnél rögzítettük a fekélyek statusat.*(1. és 2. ábra)*

1. ábra.



2. ábra.

A bal talpi felszínen 7,5 x 2,8 cm-es, a jobb talpi felszínen 4,3 x 4,5 cm-es hyperkeratoticus udvarral övezett fekély volt látható, következményes phlegmone nélkül. A sebek a Texas Wound Classification system (4) ajánlását figyelembe véve grade II. C-D stádiumúak voltak. Az angiológiai szakvizsgálat az artériás és vénás oldalon sem írt le jelentős kóros eltérést. A beteg mindkét lábán a gravis osteoarthropathia diabetica (5) jelei voltak láthatóak a röntgen felvételeken.

A beteg fekélyeinek RSWT kezelését hetente két alkalommal végeztük, kiegészítve ezáltal az addigi therapiaját. A kezeléseket az alábbi módon végeztük:

- A kötés eltávolítása után szabályos sebtisztítás, szükség szerint necrectomia, keratotomia történt.
- Steril fedőfóliával fedtük a sebeket, a sebszéleken 5 cm-rel túlérően.
- Steril kontakt gélt helyeztünk fel a fóliára.
- A seb nagyságának megfelelően cm^2-ként1000 impulzust közöltünk a sebbel, 0,08mJ/mm^2 energiasűrűség mellett. A sebszélek nem kaptak kezelést.
- A kontakt gél, valamint a védőfólia eltávolítása után steril fiziológiás sóoldattal öblítettük le az elváltozásokat.
- A sebek aktuális állapotának megfelelő kötszert választottuk a sebek kötözéséhez.

A RSWT kezelés megkezdését követő negyedik héten a sebek méretei megkisebbedtek. *(3. és 4. ábra)*

3. ábra.

4. ábra.

A beteget 4 hónapig kezeltük. Ezen időszak alatt a protokolltól nem tértünk el, a kezelések gyakoriságát nem csökkentettük. 16. hétre a fekélyek begyógyultak. A beteg azóta is tünet és panaszmentes.*(5.ábra)*

5. ábra.

MEGBESZÉLÉS

2006-ban történt felmérés azzal kapcsolatban, hogy hány regisztrált cukorbeteg él hazánkban. Akkor 507 ezer (20-69 év közötti) felnőtt emberről szólt az adat. Szakértők állítása szerint napjainkra ez a szám 10%-kal nőhetett, azaz közel 568 ezer főre tehető azok száma, akik ebben a kórformában szenvednek. Viszont az is tény, hogy megközelítőleg azonos azon csoport nagysága akik nem regisztráltak, mert nem is tudnak a betegségükről. Valamint ugyanennyire teszik azok számát, akiknél kialakulóban van a betegség.

A diabéteszes láb szindróma (diabetic foot ulceration /DFU) a cukorbetegségben szenvedők populációjának 4-10 százalékát érintő súlyos szövődmény, amely egyben ezen betegek kórházi kezelésének egyik leggyakoribb indikációját is képezi. A számos prevenciós és terápiás protokoll használatának dacára a cukorbetegeknél az alsó végtag-amputáció gyakorisága tizenötször nagyobb, mint a nem cukorbetegek körében, továbbá a statisztikai adatok szerint ezen amputáltak mintegy felénél négy éven belül szükségessé válik a másik végtag valamilyen szintű amputatioja. Hazánkban ez évi 3-4000 amputatiot jelent. (2) Az emberi veszteségen túl a gazdasági költségek is igen magasak, a major amputatiok után az átlagos ápolási idő közel 40 nap még a fejlett társadalmakban is. (7)

A diabeteszes láb szindróma összefoglaló neve a cukorbetegek lábán kialakuló, összetett pathomechanismusú tünetegyüttesnek, amelynek egyik legsúlyosabb szövődménye az alkalmazott therapia ellenére sem gyógyuló krónikus seb (8,9) kialakulása a talpi felszínen. Ez a kórforma a diabeteszes betegek 15-20%-nál jelentkezik.

A DFU az esetek mintegy 75%-ban neuropathias, 25%-ban neuroischemias eredettel bír.(10) A kórlefolyást jelentősen súlyosbítja a talpi fekély kialakulása, megteremtve az infectio lehetőségét, így szinte megbecsülhetetlenné téve a prognózist. Az autonóm idegrendszeri károsodás, a következményes vasomotoros blockból eredő microcirculatios zavarok révén tovább rontja a lokális oxygenisatiot, továbbá a sudomotor zavar okozta bőrszárazság szintén az inflammatio irányába hat. (1)

A diabeteszes láb szindróma kezelésében számos diszciplina érintett kell legyen a megfelelő eredmény reményében. A kezelés legtöbbször hosszadalmas, a súlyosabb formák. felülfertőződött esetek többnyire hospitalisatiot tesznek szükségessé.

A kezelés részben gyógyszeres, részben sebészi. A gyógyszeres therapia elsődlegesen az optimális anyagcsere állapotot célozza. Bakteriálisan felülfertőzött esetekben lehetőség szerint célzott antibiotikumokra van szükség prolongált szekvenciális therapiaban. Kiegészítendő ezen gyógyszeres paletta a microcirculatiot fokozó pentoxyphillin, esetleg prosztanoid tartalmú szerekkel.

Manifeszt hyperaesthesiaval, paraesthesiaval, fájdalommal kísért neuropathias kórformák esetén az oki therapia jegyében alpha-liponsav, tüneti kezelésként gabapentin, duloxetin adható.(11)

Az endothelfunctiora ható sulodexid therapia bevezetése hazánkban napjainkban zajlik.

A sebészi kezelés természetszerűleg – dominánsan macroangiopathias esetekben- a reconstructios beavatkozásokat, és a kollateralis keringést javító sympathectomiat jelenti.

A következményesen felülfertőződótt sebek keratotomiat, sebtoilettet, necrectomiat, időnként drainage-t igényelnek. A sebek kötözéséhez hazánkban is un. intelligens kötszerek széles tárháza áll rendelkezésre, megteremtve a lehetőségét a seb állapotától függő kötszerválasztásnak.

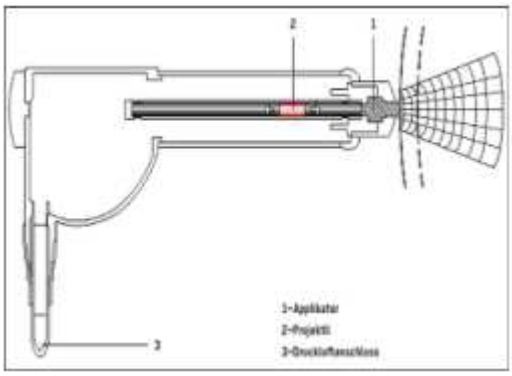
A diabeteszes láb szindróma kezelésében mind szélesebb teret kapnak a therapiat kiegészítő-vákuumasszisztált sebkezelés, a hyperbaricus oxygentherapia, valamint a lokális növekedési faktorok alkalmazása, továbbá a sejttherapia.

Diabeteszes láb szindróma esetén kimutatható a magas matrixmetalloproteáz aktivitás. Ezen enzimek lebontják a növekedési faktorokat, valamint egyéb extracellularis matrix elemeket is mint a citokinek, kollagén, fibronectin, stb.(12) Voltaképp a localis növekedési faktorok képződésének, felszabadulásának elősegítése révén kapcsolható az extracorporalis lökéshullámtherapia ezen szindrómában szenvedő betegek kezelésébe.(13)

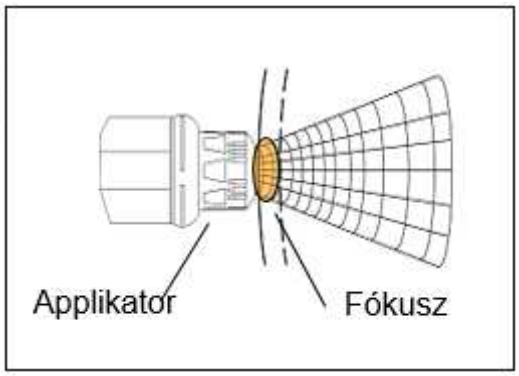
Megjegyzendő, hogy napjainkban a medicina több diszciplínája is eredményesen alkalmazza a lökéshullámot. A teljesség igénye nélkül: az urológia vesekőzúzásra, az orthopaedia ízületi calcificatiok kezelésére, myalgias triggerpontok ingerlésére (14,15)

Experimentalis, majd klinikai vizsgálatok eredményei azt mutatták, hogy a radiális testen kívüli lökéshullámok közvetlenül alkalmazhatóak akut és krónikus sebek gyógyítására steril

körülmények között kontakt gél használatával. A lökéshullám olyan akusztikus hullám, melyet magas energiával rendelkező csúcsnyomás, rövid időintervallum, továbbá alacsony utónyomás jellemez. Nyílt térben ezen hullámforma terjedése térben és időben szabályos. Abban az esetben, amikor a terjedést egy parabolával szabályozzuk, a kialakuló lökéshullám energiái egy pontban összegeződnek, a térben terjedő lökéshullához képest nagyságrendekkel nagyobb energiát hordozva. Az élő szövetben is hasonlóan viselkedik a hullám, a lágy-részeken minden károsító hatás nélkül áthalad, energiáit egy pontban összegezve *(6. és 7.ábra)*



6. ábra.



7. ábra.

Esetünkben a Swiss DolorClast® készüléket alkalmaztuk a seb kezelésére. Ezen készüléknél a radiális testen kívüli lökéshullámok jellemzője a több mint 10 MPa értéket elérő magas nyomású pozitív csúcs, a kb. 1ms időtartamú gyors kezdeti nyomásemelkedés, az alacsony, kb. 5 MPa értékű kibocsátási amplitúdó, és egy rövid, kb. 20µs tartamú ciklus. (16) *(8.ábra)*

8. ábra.

A radiális extracorporalis lökéshullám (RSWT) alkalmazása akut és krónikus sebek gyógyítására 75% sikerességi arányt mutat, mind fekvő, mind járóbeteg ellátásban.(17) Könnyen elvégezhető, egy-egy kezelési alkalom 5-15 percet vesz igénybe. Ez a terápia kiegészítő lehetőséget kínál a modern sebkezelés területén.

Az irodalomban fellelhető kísérletes, valamint klinikai vizsgálatok adatai, és saját eredményeink alapján úgy gondoljuk, hogy az *extracorporalis lökéshullám elősegíti a növekedési faktorok, és valószínűleg más immunmodulatorok felszabadulását, továbbá stimulálja az angiogenesist – kapcsolódóan a növekedési faktor felszabadulásához, s így támogatja az erek növekedését, elősegíti a sejtproliferatiot.*

ÖSSZEFOGLALÁS

A bemutatott eset adataiból, valamint az említett elméleti megfontolásokból levonható az a következtetés, hogy a diabetesben szenvedő betegek végtagot fenyegető diabeteszes láb szindróma eseteiben a végtag-megőrző therapias beavatkozásokat az extracorporalis radialis lökéshullám kezelés pozitívan támogatja. Fontos megjegyezni azt a tényt, hogy a kezelt betegek csupán 5%-a számol be lokális fájdalomról kezelés során, s mintegy 15%-uk említ kezelés közben fejfájást.

Nyilvánvalóan az előrehaladott artériás elégtelenségben a kezelés nem tudja tartósan helyettesíteni a revasacularisatios beavatkozások effektusát. Az ér- rekonstrukciós beavatkozások a standard therapias protokollnak megfelelően elsődlegesen elvégzendők az adjuváns beavatkozások megindítása előtt.

Tényként rögzíthető, hogy ezen betegcsoport kezelésében is kiemelt helyet kell, hogy kapjon a multidiszciplináris gondozás és kezelés.

A jelen cikkben ismertetett esetet követően további 30 betegnél értünk el teljes gyógyulást.

Felhasznált irodalom

[1] *Jermendy György:* Diabeteses láb szindróma: patomechanizmus, klinikai kép, korszerű terápia, megelőzés. LAM 2012:22 (4) pp. 249-256

[2] *Daróczy Judit, Rédling Marianna:* Diabéteszes lábon kialakult bőrgyógyászati szövődmények. HIPPOKRATESZ 2012/2 pp. 51-55

[3] *Vivas, A.,Choundhary, S.,Escandon, J.:*New therapies for treatment of diabetic foot ulcers: a review of current clinical trials.Surg. Technol. Int., 2010 pp. 20 83-96

[4] *Lavery LA, Amstrong DG, Harkless LB.* Classification of diabetic foot ulcerations J. Foot Ankle Surg. 1996; 35 pp. 528-31

[5] *Fráter Loránd:* Radiológia Medicina Könyvkiadó Zrt. Budapest 2008.

[6] *MostRS, Sinnock P.:* The epidemiology of lower extremity amputations in diabetic individuals. Diabetes Care 1983 pp. 6 87-91

[7] *Van Houtum WH, Lavery LA, Harkless LB:* The costs of diabetic-related lower extremity amputations in the Netherlands. Diabetic Med. 1995 pp. 12:777-781

[8] *David G. Amrmstrong, Andrew J. Meyr:* Clinical assessment of wounds. 2013. UpToDate

[9] *Hunyadi János, Salczerné Hok Mária, Sugár István:* A krónikus és nehezen gyógyuló seb fogalma, okai, kritériumai kezelésének alapelvei a nemzetközi és hazai konszenzusok tükrében. Sebkezelés-Sebgyógyulás 2008/2 pp. 4-8

[10] *Tomlinson DR, Gardiner NJ:* Diabetic neuropathies: components of ethiology. J Periph Nerv Syst 2008, 13 pp. 112-21

[11] *Kempler P, Putz Zs, Istenes I, Németh N, Keresztes K, Körei AE, et al:* A diabeteszes neuropathia klinikai jelentősége, és újabb kezelési lehetőségei. Orvosképzés 2010, 85 pp. 155-62

[12] *Field, F. K., Kernstein, M. D.:* Overwiew of wound healing in a moist environment. Am. J. Surg., 1994, 167 2S-6S

[13] *Wang CJ., Kuo YR., Wu RW., Liu RT,. Hsu CS., Wang FS., Yang KD.:*Extracorporeal shockwave for diabetic foot ulcers. J. Surg. Res. 2009, 152 pp. 96-103

[14] *Seibert W., Buch M.:*Extracorporeal shock waves in orthopaedics. Springer Verlag Berlin 1997 pp. 1-245

[15] *Roehring GJ., Baumhauer J, DiGiovanni BF, Flemister AS.:* The role of extracorporeal shock wave on plantar fascitis. Foot Ankle Clin 2005, 10 (4) pp. 699-712

[16] *Gerdesmeyer, L., Maier, M., Haake, M., Schmitz, C.:* Physical-technical principles of extracorporeal shockwave therapy (ESWT). Orthopäde 2002, 31 pp. 610-617

[17] *Vasas Judit, Dr.Meszes Angéla, Dr.Nagy Nikoletta, Sánta Csilla, Prof. Dr.Kemény Lajos, Dr. Szabad Gábor:* Lökéshullám-terápia hatása a sebgyógyulásra. Sebkezelés-sebgyógyulás 2012,1 pp. 4-9

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Gávay György - Dr. Kende György
gavay.gyorgy@uni-nek.hu – kende.gyorgy@uni-nke.hu

A HADFELSZERELÉS ÉLETCIKLUSÁVAL KAPCSOLATOS FOGALMAK ELEMZÉSE A FONTOSABB MAGYAR ÉS ANGOL NYELVŰ KIFEJEZÉSEK MEGFELELTETÉSE

Absztrakt

A 2013/14-es tanévben két félévben is felvették Erasmus hallgatók a „Research, Development and Military Industry„ megnevezésű 20 órás tantárgyat. Az órák tervezésénél számos új kérdés is felmerült, amelyek egyik lényege az, hogy a külföldi hallgatók az általánosan elfogadott szabályzók és eljárások mellett a fontosabb magyar vonatkozásokkal is megismerkedjenek. Ezek közül jelen publikáció a tárgyhoz kapcsolódó egyes magyar és angol kifejezések megfeleltetésének kérdéseit vizsgálja. A vizsgálat módszere a hadfelszerelés életciklusának a magyar és más NATO nemzetek felfogásának összehasonlítása abból a célból, hogy az egyes fázisok megnevezése és tartalma összevethető és megfeleltethető legyen. A kutatás aktuális, egyrészt azért, mert Erasmus hallgatókat várhatóan a jövőben is fogunk oktatni, másrészt azért, mert hozzájárulhat a terminológiai kérdések megválaszolásához.

Erasmus students have applied for the 20-hour subject called „Research, Development and Military Industry" in two semesters during the 2013/2014 academic year. When designing the lectures numerous new questions have come up, their main point being that the foreign students should also get acquainted with the most important Hungarian regulations and processes beside the universally accepted ones. This publication examines the question of finding the corresponding Hungarian and English expressions concerning the subject. The method of the examination is the comparison of the Hungarian, NATO and other NATO nations' understanding of the armament lifecycle, the aim of which is to be able to study and find the corresponding terms of the certain phases. The research is well-timed, since we will most likely be teaching Erasmus students also in the future, and also since it can help in answering the questions of terminology.

Kulcsszavak: *hadfelszerelés, beszerzés, rendszerbe állítás, életciklus modell, terminológia ~ armament, acquisition, deployment, life cycle modell, terminology*

BEVEZETÉS

A hadfelszerelés életciklusának folyamata, szakaszokra osztása a Magyar Honvédségben nem egyezik meg teljes mértében a különböző NATO dokumentumokban leírtakkal. A hosszú évek alatt kialakult, rendszerek eltérése kommunikációs problémákhoz vezethet. A két rendszer fogalomköre nagymértékben hasonló, de szó szerinti fordítást nem minden esetben tesz lehetővé, továbbá a korábban megjelent fordítások közül is lehet találni pontatlanságokat. Jelentősen nehezíti a fogalmak megfeleltetését, hogy számos esetben a magyar jogi szabályzók sem fogalmaznak egységesen. A témában járatos szakemberek számára egyértelműek a szinonimák jelentései, de a témával ismerkedőket könnyen elbizonytalaníthatja a sok esetben hasonló csengésű szavak értelmezésének problémája.

Az absztraktban szereplő okok szükségessé tesznek egy olyan kutatást, amely egymás mellé helyezi a hasonló fogalomkörök elemeit, rávilágít a különbségekre és a hasonlóságokra.

A HADFELSZERELÉS FOGALMA

A hadfelszerelés[1] olyan eszköz és anyag, amelyet a Magyar Honvédség alaprendeltetéséből eredő feladatainak végrehajtása során alkalmaz vagy felhasznál, illetve[2] a honvédelmi szervezetek tevékenységéhez szükséges valamennyi anyag és technikai eszköz, amelyet az ipar és a kereskedelem katonai célokra gyárt és szállít. Hadfelszerelés kereskedelmi forgalomba nem, vagy csak külön engedéllyel kerülhet. A hadfelszerelés fogalomköre további két alrendszerre bontható: hadianyagokra és haditechnikai eszközökre. Ezek elfogadott angol nyelvű megfelelője az „armament" szó és a „military equipment"[3].

A hadianyagok[4] a hadfelszerelés alrendszerét képező azon anyagok és termékek összessége, amelyeket a katonai szervezetek a fegyveres küzdelemben és a különböző műveletek végrehajtása során az ellenség élőerejének és haditechnikai eszközeinek pusztítására, építményeinek rombolása céljából felhasználnak. A hadianyagokat a felhasználás célja alapján harcanyagokra, fenntartási anyagokra és ellátási anyagokra osztják. A „war material" kifejezés[5] ritkábban használt megfeleltetése a magyar hadianyag szónak.

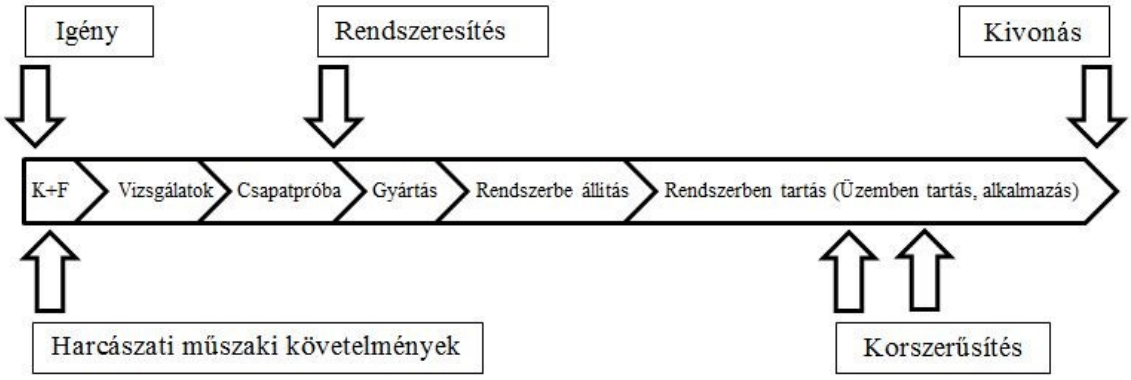
A haditechnikai eszköz[6] a hadfelszerelés részét képező azon eszközök összessége, amelyek a katonai szervezetek alaprendeltetés szerinti működtetéséhez, a béke és háborús feladatok megoldásához szükségesek. Másik meghatározás[7] szerint a honvédelmi szervezet állománytáblájában szükségletként előírt katonai rendeltetésű eszköz, amely a felkészítéshez, kiképzéshez, a katonai műveletek végrehajtásához, támogatásához, kiszolgálásához szükséges. A haditechnikai eszközöket a működtetés célja alapján harceszközökre, harcbiztosító eszközökre és kiszolgáló eszközökre osztjuk. A haditechnikai eszköz a Haditechnikai Lexikon megfogalmazása alapján a hadfelszerelésnek azon része, melyre jellemző a huzamosabb ideig tartó alkalmazás, használat, üzemfenntartás. A lexikon szerint az ajánlott fordítás a „military technical means". A „military device" bár katonai eszközt jelent, legtöbb esetben elektronikai eszközöket takar. A Magyar Honvédség haditechnikai eszközeit további csoportokra lehet osztani felhasználási területük szerint, de ezt a felosztást csak tartalmilag követi az angol nyelvű fogalomrendszer.

[1] Dr. Kende György, Dr. Seres György: Haditechnikai Kutatás – Fejlesztés. ZMNE egyetemi jegyzet Budapest. 2004. 53.p.
[2] 9/2010. (I.22.) HM utasítás 2.§ c)
[3] Haditudományi Lexikon, Magyar Hadtudományi Társaság, Budapest, 1995. I. kötet 445.p.
[4] Fazekas József: Szakmai szabályismeret. Budapest ZMNE főiskolai jegyzet, 2001. 5.p.
[5] Haditudományi Lexikon, Magyar Hadtudományi Társaság, Budapest, 1995. I. kötet 447.p.
[6] Fazekas József, Szakmai szabályismeret, főiskolai jegyzet Budapest ZMNE 2001.5.p.
[7] 1/2009 HM rendelet 2.§ i)

Egyszerű példa, hogy a fegyverzettechnikai eszközök között van „weapon”, azaz fegyver, illetve a már előbb említett „military device” ami lehet például egy távcső is. Az optikai eszközök a Magyar Honvédségben fegyverzettechnikai eszközök.

A HADFELSZERELÉS ÉLETCIKLUSÁNAK BEMUTATÁSA A MAGYAR HONVÉDSÉGBEN

A Magyar Honvédség hadfelszerelése jól szabályozott, hosszú és részletes folyamat során kerül alkalmazásra. Abban az esetben, ha a szervezet feladatrendszere új elemmel bővül, a legtöbb esetben új eszközökre van szükség a feladatok eredményes végrehajtásához. A hadfelszerelések[8] életciklusát a 9/2010 HM utasítás foglalja keretbe. Az életciklust az 1. ábra mutatja be részletesen. Az egyes időszakaszok ábrázolása nem időarányos, és a pontos időtartamok az eszközök jellegétől függően minden esetben különböznek. Aktuális példaként említhető a BTR 80 SKJ[9] sebesültkihordó jármű, amelynek a várható rendszerben tartási ideje 20 év.



1. ábra. Haditechnikai eszköz életciklusa a Magyar Honvédségben[10]

Az új feladatok kapcsán felmerülő igény kielégítésére vagy egy már meglévő eszköznek a saját követelményeinkhez illesztése, vagy egy új eszköz kifejlesztése a megoldás. Mindkét esetben beszélhetünk kutatás - fejlesztési tevékenységről.[11] A kutatás - fejlesztés olyan előre tervezett átfogó műszaki, gazdasági, tudományos tevékenység, amely a célul kitűzött - általában hadfelszerelés, technológia és szellemi termék kifejlesztése, korszerűsítése, illetve az ezeket megalapozó kutatási - feladat megoldására irányul. Ebben az időszakban kell megfogalmazni és pontosítani a Harcászati Műszaki Követelményeket[12], mely a hadfelszerelés alkalmazási szintű komplex műszaki követelménye. A Haditechnikai Lexikon megfogalmazása szerint[13] „Mindazok a katonai, technikai követelmények, melyeket a katonai vezetők a haditechnikai műszaki fejlesztők közreműködésével egy-egy haditechnikai eszközzel szemben támasztanak, s amelyek kielégítése lehetővé teszi a harcban való hatékony alkalmazásukat vagy sajátos feladatok megoldását. A Harcászait Műszaki Követelmények a tervezés, a haditechnikai fejlesztés alapokmányát képezik.” A kifejlesztett eszköz mintáját (prototípusát) a várható igénybevételeknek megfelelően laboratóriumi, üzemi, és egyéb vizsgálatoknak vetik alá a csapatpróbára bocsátást megelőzően.

---

[8] 9/2010. (I.22) HM utasítás - A hadfelszerelés rendszeresítéséről és rendszerből történő kivonásának rendjéről-Honvédelmi Közlöny CXXXVII. szám; 326-332.pp.

[9] A Honvédelmi Miniszter a 82/2005 (HK 17) utasításában meghatározta 10-15 darab páncélozott sebesült kiürítő jármű kifejlesztését, melyet a BTR-80 típusú páncélozott szállító harcjármű bázisán kell kialakítani, úgy, hogy maximálisan érvényesüljön az egészségügyi jelleg.

[10] Dr. Kende György, Dr. Seres György: Haditechnikai Kutatás – Fejlesztés. ZMNE egyetemi jegyzet, 2004. Budapest, 52.p. 18. sz. ábra alapján szerkesztve

[11] uo. 52.p.

[12] uo.53.p.

[13] Haditudományi Lexikon, Magyar Hadtudományi Társaság, Budapest, 1995. I. kötet 502.p.

A csapatpróba[14] olyan széles spektrumú vizsgálatot, vizsgálatsorozatot jelent, amely annak megállapítására irányul, hogy a rendszeresítés előtt álló hadfelszerelési anyag megfelel-e a tervezett feladatok ellátásához kapcsolódó alkalmazási követelményeknek. A csapatpróba során szerzett tapasztalatok alapján lehetőség van a Harcászait Műszaki Követelmények módosítására, továbbá a rendszerben tartás feltételeinek megfogalmazására. A csapatpróba fogalma angol nyelven szintén nem egyértelmű, mivel a tesztelés (testing) a bemutatás (demonstration), és a folyamatos értékelések (assesment) együttesen fedi le azt. A gyártás feltételeinek megteremtése után minden lehetőség adottá válik a hadfelszerelés rendszeresítésére.

A rendszeresítés[15] valójában egy „döntés olyan új, illetve jelentős mértékben modernizált hadfelszerelésnek a Magyar Honvédség rendszerébe való felvételére, amely a Magyar Honvédség egészére vagy haderőnemeire hatással van. Emellett hazai fejlesztésből vagy hazai polgári termelésből származik, illetve olyan külföldi beszerzés, amely addig még nem volt rendszeresítve." A rendszeresítés másik megfogalmazása[16] is helytálló, de bővebben fogalmaz: „az új haditechnikai eszközöknek a fegyveres erők rendszerébe történő felvételével kapcsolatos elosztási folyamatok, infrastrukturális beruházások, szakmai felkészítések és egyéb eljárások összessége. A rendszeresítés a legmagasabb szintű logisztikai szolgálat feladata. Célja a haditechnikai eszközök üzemeltetési feltételeinek kialakítása, továbbá biztosítani a rendeltetésszerű üzemeltetés, a tárolás, az állagmegóvás, a technikai kiszolgálás és a helyreállítás személyi, tárgyi és anyagi feltételeit." A vonatkozó HM rendelet a fogalom meghatározás tekintetében viszont igen szűkszavú:

- A rendszeresítés az MH állománytábláiban felszerelési jegyzékeiben, normajegyzékeiben meghatározott szükségletek kielégítésére beszerzett hadfelszerelés felvétele a Magyar Honvédség rendszerébe. (9/2010. (I.22.) HM utasítás 2.§ a),
- Olyan szabályozott eljárás, amelynek eredményeként a munkaeszköz, hadfelszerelési anyag, katonai védőeszköz felvételre kerül az MH rendszerébe. (1/2009. (I.30.) HM rendelet 2.§ o).

A rendszeresítés a Rendszeresítési Bizottság javaslatára a Honvédelmi Miniszter által kiadott rendszeresítési határozat, vagy a HM Honvéd Vezérkar főnöke által kiadott alkalmazásbavételi határozat alapján történik.

A katonai alakulatokhoz a rendszerbe állítás[17] folyamán kerül a hadfelszerelés. A rendszerbe állítás az a tervezett folyamat, amely során – a fent említett dokumentumok alapján – a hadfelszerelés ténylegesen bekerül a Magyar Honvédség rendszerébe. Ennek eredményeként az alakulatok, csapatok megkezdhetik - haditechnikai eszköz esetében - annak rendszerben tartását, azon belül annak rendeltetésszerű alkalmazását. Hadianyag esetében ettől a mozzanattól kezdve van lehetőség azok rendeltetésszerű felhasználására. Fogalmára a Hadtudományi Lexikon pontos megfogalmazást nem ad, a rendszerbe állítás fogalmát a rendszeresítés fogalomkörével együtt tárgyalja. Angol fordításként a „systematizing" szót ajánlja, mely valójában nem helyes. A rendszerbeállítás tulajdonképpen a hadrendbe állítás fogalmával egyenértékű, így a „deployment" kifejezést látjuk helytállónak.

A rendszerben tarás - alkalmazás időszaka - a rendszerből történő kivonással végződik. Ez idő alatt üzembentartják az eszközöket. Ezt az időszakot lehet az „in-service" fogalommal lefedni.

---

[14] 1/2009. (I.30.) HM rendelet 2.§ d)

[15] Dr. Kende György, Dr. Seres György: Haditechnikai Kutatás – Fejlesztés. ZMNE egyetemi jegyzet, 2004. Budapest, 53.p.

[16] Fazekas József, Szakmai szabályismeret, főiskolai jegyzet Budapest ZMNE 2001 megjegyzés: A „standardization" szó nem megfelelő fordítás.

[17] Dr. Kende György, Dr. Seres György: Haditechnikai Kutatás – Fejlesztés. ZMNE egyetemi jegyzet, 2004. Budapest, 54.p.

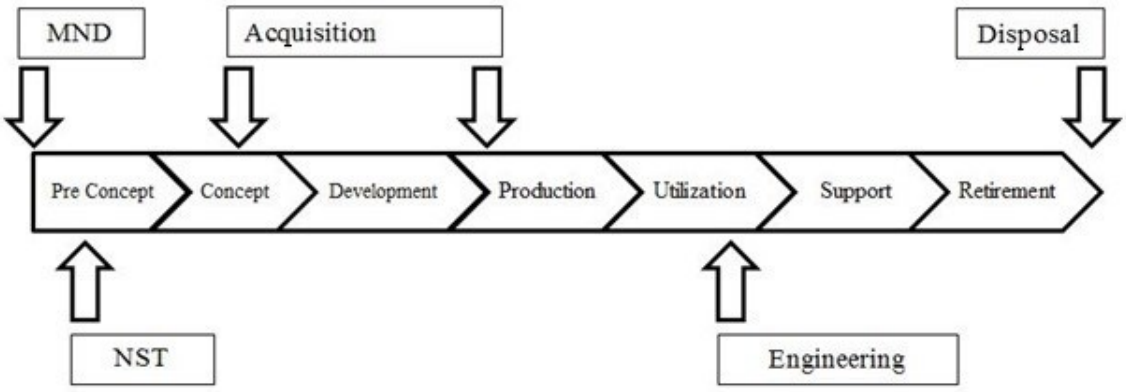
A rendszerből történő kivonás a haditechnikai eszközök életciklusának utolsó fázisa, melyet legfelső szintű haditechnikai vezetés szervez meg. A rendszerből történő kivonás[18] tartalma a rendszeresített hadfelszerelés és a hozzá tartozó anyagok törlése a Magyar Honvédség állománytábláiból, felszerelési jegyzékeiből, normajegyzékéből. Ez a fázis teremti meg az adott eszköz, eszközcsoport további alkalmazásának (értékesítésének, tartalékolásának, megsemmisítésének, újrahasznosításának) feltételeit. A rendszerből történő kivonással befejeződik az adott eszköz, eszközcsoport életciklusa a haderőben. Az eszközt akkor is ki kell vonni, ha műveleti területen meg nem térülő veszteséggé válik. A „out of system evacuation" kifejezés[19] nem biztos, hogy megfelelő fordítás, a 05-57 Def Stanag[20] szerint „disposal" illetve „retirement" szavak megfelelőbbnek tűnnek.

PAPS (PHASED ARMAMENTS PROGRAMMING SYSTEM) ÉS CMP (CONFIGURATION MANAGEMENT PLAN)

A NATO 1988-ban hagyta jóvá a Hagyományos Fegyverzet Tervezési Rendszert (CAPS, Conventional Armaments Planning System), mivel szükségessé vált a Szövetség védelemtervezési alapjainak összehangolása. Feladatai között szerepelt az iránymutatás a nemzeti programok számára, arra nézve, hogy hogyan tudják a Szövetség kollektív katonai érdekeit a legjobban teljesíteni. A fegyverzet szó helyett, véleményünk szerint a hadfelszerelés fogalma helyesebb, mivel szélesebb tartalommal bír.[21]

A CAPS -t 1989-ben felváltotta a PAPS (Szakaszolt Fegyverzeti Program Rendszer). Ez a keretrendszer a hadfelszerelés életciklusának szakaszait határozza meg. A rendszert az AAP-48 (Allied Administrative Publication, azaz Szövetséges Adminisztrációs Kiadvány) 2007 NATO dokumentum mutatja be. A tagoláshoz mérföldköveket (milestones), és szakaszokat (stages) használnak.

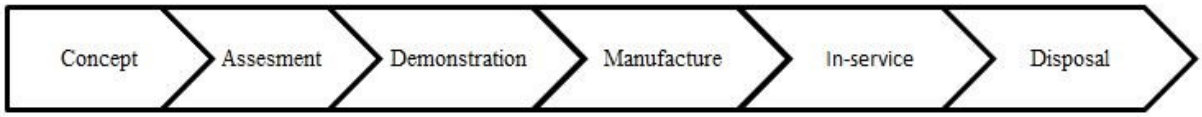
A PAPS második generációját a 2010-ben kiadott dokumentum, az AAP-20 mutatja be, továbbá a PAPS edition 1 és edition 2 közötti átmenetet definiálja, amely valójában a Concept fázis két részre bontásából áll. A második kiadásban Pre-Concept és Concept szakaszok szerepelnek. A Nato Logisztikai Kézikönyv és az AAP-20 edition 2 több szinonimát használ, de ezek tartalma valójában nem különbözik.



2. ábra. PAPS (edition 2) a beszerzés folyamatával kiegészítve[22] (rövidítések kifejtése a szövegben)

[18] 9/2010. (I.22.) HM utasítás 2.§ b)
[19] Fazekas József: Szakmai szabályismeret. Budapest ZMNE főiskolai jegyzet, 2001. 5.p.
[20] Configuration Management of Defence Materiel, Ministry of Defence UK; Defence Standard 05-57
[21] A NATO Logisztikai Kézikönyv fordítása nehezen érthető, a szövegek pontos megértéséhez ismerni kell a kifejezések, rövidítések jelentését, hátterét.
[22] AAP-20 (3-118) Appendix 1, Disposal Process Throughout the System Lifecycle című ábra alapján szerkesztve. (MND - Mission Need Document; NST - NATO Staff Target)

Az eszközök életciklusának másik megközelítését a 2000-ben kiadott Configuration Management of Defence Materiel[23] dokumentum részletezi. Ez a dokumentum a védelmi eszközök beszerzésére ad útmutatást.



3. ábra. Configuration Management Plan (CMP) egyszerűsített folyamata[24]

Amikor egy ország, vagy a NATO Katonai Hatósága megállapít egy katonai feladatra való igényt, megszületik a Feladat Szükségleti Dokumentum (MND - Mission Need Document). Magyar vonatkozásban ezt tekinthetjük az igény megfogalmazásának. Ezt követi időrendben a NATO törzs célok megfogalmazása (NST - NATO Staff Target).

1. táblázat. Fogalompontosítások összesítő táblázata

Magyar fogalom	Angol fogalom	Megjegyzés, forrás
Hadfelszerelés	Armament Military Equipment	Hadtudományi Lexikon [2] Certain Acquisition Procedures of Armament and Military Equipment [11]
Hadianyag	War Material	Hadtudományi Lexikon
Igény (Az igényt megfogalmazó dokumentum)	Mission Need Document	Nato Logisztikai Kézikönyv[25] [6]
Értékelés (a koncepciót, illetve a hadfelszerelést)	Assesment	Def Stanag 05-57 [5]
Bemutatás (csapatpróba alatt, előtt)	Demonstration	Def Stanag 05-57
Koncepció (elképzelés)	Concept	AAP-48 (ed. 1) [9]
Gyártás	Manufacture, Production	Def Stanag 05-57 AAP-20 [10]
Fejlesztés	Development	AAP-48 AAP-20
Rendszerbe állítás	Deployment	How DOD Acquires Weapon Systems and Recent Efforts to Reform the Process [12]
Igénybevétel (használat)	Utilization	AAP-48 AAP-20
Támogatás Anyagi támogatás	Support Material Support	AAP-48 Szakmai szabályzatismeret jegyzet [4]
Kivonás, Rendszerből történő kivinás	Retirement, Disposal	AAP-48, AAP-20 Def Stanag 05-57
Rendszeresítés	Acquisition	A beszerzés döntését nem lehet megfeleltetni a magyar fogalomnak, a szerzők javaslata az „Acceptens for future acquisition”
Rendszerben tartás	In-service	Def Stanag 05-57
Üzemfenntartás	Maintenance	AAP-6 alapján Nato Logisztikai doktrína [6]
Korszerűsítés, Modernizáció	Modernization	értelemszerű, általánosan használt megfogalmazás

[23] Ministry of Defence; Defence Standard 05-57

[24] Configuration Management of Defence Materiel, Ministry of Defence UK; Defence Standard 05-57. 25. p. 2.ábra alapján szerkesztve

[25] Nato Logisztikai Kézikönyv 170-173.o

ÖSSZEGZÉS

A Magyar Honvédség és a NATO fogalomrendszerének párhuzamba állításával elérhető egy olyan elméleti, és a gyakorlatban jól alkalmazható eredmény, mely a fogalmi egyezések és különbségek esetében a szó szerinti fordításból adódó hibák és félreértések megelőzésére irányul. A magyar kifejezések elemzésével, valamint a haditechnikai eszközök beszerzésével, azok életciklusnak meghatározásával foglalkozó angol nyelvű publikációk vizsgálatával lehetőség nyílik a helyes fordításra, illetve fogalomértelmezésre. Mindez jól segíti – többek között – a témában tartott angol nyelvű (Erasmus) előadások megtartását.

Felhasznált irodalom

[1] Dr. Kende György, Dr. Seres György: Haditechnikai Kutatás - Fejlesztés ZMNE egyetemi jegyzet, Budapest, 2004. 51-54.pp.

[2] Hadtudományi Lexikon, Magyar Hadtudományi Társaság, Budapest, 1995. I-II. kötet 445-1198.pp. ISBN 963 04 5228 6

[3] 9/2010. (I.22) HM utasítás, A hadfelszerelés rendszeresítéséről és rendszerből történő kivonásának rendjéről, Honvédelmi Közlöny CXXXVII. szám; 326-332.pp.

[4] Fazekas József: Szakmai szabályismeret, főiskolai jegyzet Budapest ZMNE 2001. 5.p.

[5] Configuration Management of Defence Materiel, Ministry of Defence UK; Defence Standard 05-57

[6] Nato Logisztikai Kézikönyv, A HVK Logisztikai Csoportfőnökség kiadványa, 1998. 171-173.pp.

[7] Szövetséges Összhaderőnemi Logisztikai Doktrína, A HVK Logisztikai Csoportfőnökség kiadványa, 1999. 263.pp.

[8] 1/2009. (I.30.) HM rendelet, A Magyar Honvédségre, illetve katonai nemzetbiztonsági szolgálatokra vonatkozóeltérő munkavédelmi követelményekről, eljárási szabályokról. http://hm.hatosagihivatal.kormany.hu/download/4/3c/40000/1_2009_hm_rend.pdf (Letöltve: 2014.04.10.)

[9] AAP – 48 NATO System Life Cycle Stages and Processes, 2007. Edition 1. http://www2.fhi.nl/plot2012/archief/2010/images/aap-48e.pdf (Letöltve: 2014.04.10.)

[10] AAP – 20 edition 2 Phased Armaments Programming System, 2010. http://www.msb.gov.tr/birimler/tekhiz/doc/ac327/AAP-20%282%29Ec1.pdf (Letöltve: 2014. 04.14.)

[11] Prof dr. Wlodzimierz Mszalski: Certain Acquisition Procedures of Armament and Military Equipment (RTO-MP-SAS-080)

[12] Moshe Schwartz, Defense Acquisitions: How DOD Acquires Weapon Systems and Recent Efforts to Reform the Process, 2013. https://www.fas.org/sgp/crs/natsec/RL34026.pdf (Letöltve: 2014.03.20.)

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Harald Pöcher

MONEY, MONEY AND MONEY AGAIN
THE DEFENCE EXPENDITURE IN THE EVE OF WORLD WAR ONE

Abstract

Most of the scientific studies about World War One focused on historical events, diplomacy, conferences but only a small number of books were written about the financial base and potentiality of great powers and their defence spending before the war. Furthermore only a handful of scientist wrote some books and papers about war economy of World War One. In this article the author gives some implicit answers about the course of the war, especially why the "Central powers" already lost the war before they begun it in 1914.

A legtöbb első világháborúról szóló tanulmány elsősorban a történelmi eseményeket, diplomáciai tárgyalásokat vizsgálja meg, és csak kevés könyv ír az eseményhez köthető pénzügyekről valamint a háború előtti védelmi kiadásokról. Csak csekély számú kutató írt cikkeket, könyveket a háború gazdasági vonatkozásairól. Jelen cikkben a szerző válaszokat próbál adni a háború folyamatáról, valamint arról, hogy a Központi Hatalmak miért vesztették el már azelőtt a háborút, hogy 1914-ben elkezdték volna.

Keywords: *military economy, World War One; defence spending ~ katonai gazdaságtan, első világháború, védelmi kiadások*

INTRODUCTION

Nearly all scientific works about World War One and the decade before focused on historical events, diplomatic activities, conferences as well as wars and battles but only a small number of books were written about the financial base and potentiality of great powers and their defence spending before the war. Furthermore only a handfull of scientist wrote some books and papers about war economy of World War One[i]. The reason for this scientific gap is multifarious and an accusation to single scientific disciplines is not very helpful to shut the gap. The author simply assumes that extensive research work on defence expenditure in the eve of World War One was not a priority field of research work of defence economists or historians in the past.

In 2014, the year of reminiscence of 100 years after the beginning of World War One, publishing an essay about "defence expenditure in the eve of World War One" is a real challenge for a defence economist. The following essay is only a single essay under numerous essays published in 2014 to remember the events of World War One, but it gives some implicit answers about the course of the war, especially why the "Central powers/Mittelmächte/Központi hatalmak" (The Central Powers were one of the two warring factions in World War One, composed of the German Empire, the Austro-Hungarian Empire/Österreichisch-Ungarische Monarchie/Osztrák–Magyar Monarchia, the Ottoman Empire, and the Kingdom of Bulgaria) already lost the war before they begun it in 1914. Having analyzed the figures and data in detail it is more or less a miracle that the Central powers were able to fight nearly five years against the "Triple Entente/Entente/Antant" (The Triple Entente was the name given to the alliance among France, Great Britain, and Russia) which was in financial terms vastly superior.

The situation in the fateful summer days of 1914 also showed that all leading politicians, emperors and kings of Central powers didn't have a clear sight about the importance of financial base on warfare and about the importance of national economic conditions on operational readiness of armed forces and the possibility to sustain a longer war. In times of need for absolute secrecy it also could be possible that countries published manipulated data to deceive other countries.

100 years after the World War One it is not easy to collect all the data about the financial situation of all European countries without great effort. To collect all the data it is necessary to make research work in the war archives of all countries of Europe or in the libraries of the parliaments because most of the defence budgets had to pass the parlaments to become a budget act.

On the way searching for traces the author found the peridocials "Army Almanac (Armee-Almanach)" which were published at the beginning of 20 Century by the Austrian-Hungarian army colonel Alois Veltzé[ii]. The Army Almanac was a kind of forerunner of today`s "The Military Balance" or the SIPRI´s Yearbooks. Colonel Veltzé was the head of the publication division of war archive in Vienna and a prolific writer of his time writing more than 122 historical important volumes as an author or co-author. During the times of the First World War he founded the so-called "literary group of war archive" which produced books and articles to motivate the soldiers on the front. Veltzè was one of the officers of k.u.k army whose achievements besides to be a soldier were remarkable. The k.u.k army was full of such talented officers, i.e. one of them was the later Major general Theodor Edler von Lerch who introduced skiing in Japan during his official stay in Japan 1911/12 to study the Japanese army which won the war against mighty Russia in 1904/05 and was considered to be one of the best armies of its day.

Remarks on the sources of data of military spending

The quality of economic data changed within the last 100 year because economics as a science discipline made great steps forward in developing its scientific tools. But now and then the principle "Don`t trust statistics you didn't create (fake) yourself" is valid. Besides statistical inaccuracies military secrecy was another important factor why it is not easy to get right data related to military affairs.

To verify the quality of the data published by Veltzé in his Almanacs the author found some recently published book containing financial data of armed forces of selected countries. Two real impressive analyzes of the period before the World War Two transmit the books "Armaments and the Coming of War-Europe 1904-1914"[iii] written by the historian David Stevenson and "The Arming of Europe and the Making of the First World War"[iv] written by David G. Hermann. The book of Hermann is also a treasure chest to find easily primary sources due to a detailed bibliography enclosed.

Studying and comparing all these sources the author is able to qualify the value of Veltzé`s Army Almanac. Comparing the data presented by Veltzé with the results of author's research work lead us to the conclusion that in Veltzè's Army Almanac are some inaccuracies in the publication of defence spending data but it was not possible to clear up these existing differences due to the lack of footnotes in Veltzè's books.

The essay is more or less an essay on macroeconomic level using aggregate economic terms but the author gives also some attention to microeconomic level in the fourth part by discussing the value of the work of officers using payment as a yardstick. The following essay is divided into five parts. In the first part, the author analyzes the burden of military spending on national economy in selected countries in Europe. Hereafter in two parts the author reflects upon military expenditure as a whole and military spending of selected countries broken down in spending for army and naval forces between 1906 and 1913. In the fourth part the author analyzes the labor value of officers in selected countries using payment as a yardstick. Final remarks conclude the essay.

The burden of military spending on national economy

An important question in every country is to what extent the state is able to burden its national economy with military spending because now and then a country is able to spend its disposable money only once and it had to find a well balance relation between expenditure for education, health and security to satisfy all the needs of all social groups in the best possible way to guarantee social freedom and justice in a society. Table one shows different forms of expression of the burden of military spending on national economy. In the second column from the left the burden is shown in percent of public expenditure and in the third column from the left in percent of net national product. As the left column shows, Germany and the Ottoman Empire burdened their public expenditure more than other countries with military expenditure. In this view the Austrian-Hungarian Monarchy burdened its public expenditure only moderate with military expenditure. Using the net national product as a yardstick to show the burden of military spending on national economy we obtain results between 2.6 and 4.5 percent which can be assumed as not really high compared with data of European countries which were measured during times of the Cold War after the Second World War until the collapse of Soviet Union in 1990/91. In this view the Austro-Hungarian Empire burdened his economy less than other great powers of Europe. Therefore it is not surprising that armed forces of Austro-Hungarian Empire was not developed as well as armed forces of other great powers in Europe.

Country	Burden in percent of public expenditure	Burden in percent of Net National Product	Remarks
Germany	50	4.2	War participant since 1914
France	29	4.1	War participant since 1914
Great Britain	29	3.9	War participant since 1914
Italy	25	2.9	War participant since 1915
Ottoman Empire	45	no figures available.	War participant since 1914
Austria-Hungary	13	2.6	War participant since 1914
Russia	25	4.5	War participant since 1914

Table 1: Average burden of National Economies with military spending in selected countries in the eve of World War One, Source: Stevenson, page 6

An analyze of military expenditure between 1906 and 1913

Armed forces are complex system, which are not able to set up between nightfall and daybreak. This fact has various reasons which could not be discussed in this essay in detail because of the available space. Only as much is said: the process of establishing efficient and powerful armed forces needs time, at least five up to ten years, to reach a high grade of operational readiness. The author realizes that money is not the only key factor to gain a high operation readiness of armed forces but money plays an important role financing housing and arming of armed forces and to pay the soldiers and civilian who work for armed forces.

To show how much money, expressed in Austrian-Hungarian Kronen (A-H K), was spent between 1906 and 1913, the author added up the defence budgets of European countries, published in Veltzès army-almanac, and formed a total sum for Central Powers and Triple Entente. The calculation yielded to 40.000 million A-H K for Triple Entente and not more than 19.000 million A-H K for Central Powers which is not more than half of the sum for Triple Entente. See for more detail figure 1 (Defence expenditure between 1906 and 1913 of European and outside of Europe).

Defence spending for Army and Navy of selected Countries between 1906-1913

In the period under consideration (1906 to 1913) every great power in Europe operated an army and naval forces. During the eve of World War One, the establishment of an independent air force was in the early stages of development, and the pilots operated their planes as a part of army or navy. Table 2 shows military expenditure for Army and Naval Forces of selected Countries between 1906 and 1913. All the expenditure are expressed in British pounds and therefore it is easy to compare the figures cross border.

A quick look at the figures for every country leads to the conclusion that military spending continuously raised between 1906 and 1913. Stevenson calculated the raise of military expenditure from 19 billion UD $ in 1908 to 30 billion US $ in 1913 worldwide.

Country Year	Great Britain		France		Russia		Italy		Germany		Austro-Hungarian Empire	
	Army	Navy	Army	Navy	Army	Navy	Army	Navy	Army	Navy	Army	Navy
1906	27,8	31,4	34,2	12,2	41,5	12,3	10,1	4,8	41,5	12,7	17,4	2,9
1907	27,1	31,1	32,7	12,6	42,9	9,3	10,3	5,8	46	14,9	18,5	2,6
1908	26,8	32,2	33,3	13,2	54,4	9,9	10,9	5,9	47	17	21,1	3,1
1909	27,2	35,8	34,7	13,9	57,0	9,8	12	6,6	49	20,6	27,4	4,2
1910	27,4	40,4	36,4	14,5	56,6	11,9	13,5	6,3	47,3	21,3	24,2	4,2
1911	27,6	42,9	40,5	20,7	58,1	12,8	14,7	8,2	46,9	22,1	22,4	5
1912	28,1	44,4	43,4	17,1	67,6	18,6	18,7	11,2	52,1	22,7	25,4	7,1
1913	28,3	48,4	44	19	75,8	25,9	25,3	14,4	78,3	23,5	34,4	8,7
Sum	526,9		422,3		566,4		178,7		562,9		228,3	

Table 2: Military spending for Army and Navy of selected Countries between 1906 and 1913 in million British pounds, Source: Stevenson, page 7

Remarks: The exchange rate between the British Pounds and Austro-Hungarian (A-H) Kronen (£ 1 = 24 A-H K)

As table 2 shows, it is obvious that before World War One, Great Britain maintained a blue water navy which operated in a separate league and the slogan "Rule, Britania! Britania rule the waves! Britons never will be slaves" was filled with life. To name concrete data, between 1906 and 1913 Great Britain took more large warships (battleships/dreadnoughts, battle cruisers and pre-dreadnoughts) into service than other great powers as the following comparative figures in brackets show[v]: Great Britain (50), Germany (30), France (19), Russia (11) Italy (10) und Austria-Hungary (10).

The column "Army" in every countries column further shows the importance of land forces for continental European powers which spent more of their money to equip their armies in the best possible way than sea going nations to pursue their continental interests.

The military spending of Austro-Hungarian Empire needs some explanation. The Austro-Hungarian Monarchy has been a dualistic monarchy since the reconciliation (Österreich-Ungarischer Ausgleich / osztrák-magyar kiegyezés) of 1867. The reconciliation had far reaching implications for both countries including effects on security and defence policy of the Monarchy. Since 1867 the defence of the country has been organized as follows: Both countries operated a common army and navy. The common forces were led by the war ministry which was located in Vienna. Moreover, both countries operated their own armed forces, in Hungary this army was called "Honved" and in Austria "Landwehr". Both territorial armies were lead by separate ministries of defence which were located in Vienna and Budapest. The reconciliation also played an important role for the preparation of defence budget in the Austro-Hungarian Empire. Both countries prepared their own budget independently. Therefore Austria and Hungary prepared a budget for the common forces and for their own territorial forces. For example, the defence budget for 1913 looks as follows[vi]: Austria's contribution to the common army and navy was 648 million Kronen and for the territorial-army 121 million Kronen and Hungary contribution was 315 million Kronen for the common army and navy and 105 million Kronen for the Honved. In sum, 1913 Austria-Hungary spent 1.186 million Kronen for its armed forces.

The duplication in the Austro-Hungarian Empire resulted in many negative effects, especially inefficiency in the use of scarce financial resources for armed forces due to splitting of the monarchy into two de facto separate acting states. Ultimately this situation lead to duplicities and a low operational readiness of armed forces and was one of the main reason that Austro-Hungarian Empire lost the first battles in the World War One accompanied with high losses of younger officers.This enormous loss of high qualified young officers could never be replaced during the wartime.

The value of officer's work in selected countries

In every country's chapter, Veltzé presented the payment of officers in armed forces but there are no footnotes added to check the correctness of the data. To verify the data of payment, the author found some other sources which mentioned payment rules in armed forces. For example, in his book "Der k.(u.) k. Offizier (The k.(u.) k. Officer)"[vii], István Deák mentioned that low ranking officers of Austrian-Hungarian armed forces were less paid than officers in France and Germany and in "The March to the Marne, The French Army"[viii], Douglas Porch gives an overview of the payment and pension claims of officers in selected countries.

A comparison of the data in table 3 shows that in Austro-Hungarian Empire besides the ranks of Generals all other ranks got less payment than officers of the same rank in France, Germany and Italy. The author was not able to find an explanation about the inequalities between the wages of Generals and other ranks in armed forces of Austro-Hungarian Empire and also about the inequalities of the payments of lower ranks in Austro-Hungarian Empire, France, Germany and Italy. One explanation for the concrete situation in Austro-Hungarian Empire could be the fact that most of the high ranking generals were members of the nobility and during the times

of Austro-Hungarian Empire the nobility had a great influence to set things right themselves and the nobility was indifferent to the standard of life of other social groups. The low payment of officers in Austrian Hungarian armed forces lead to chronically indebtness of younger officers. Therefore in Austrian Hungarian Monarchy circulated the slogan "He has debts like a staff officer". Many military officers in Austrian Hungarian Empire had debts during their whole life because many of them reached only the rank of a major.

	Highest ranks of Generals	**Major General**	**Colonel**	**Captain I.Class**	**Lieutenant**	**Remarks**
Austria-Hungary	24.000	11.400	7.200	3.000	1.680	In addition to regular payment special allowances were paid
Germany (D)	14.160	10.620	9.204	4.800	2.900	In addition to regular payment special allowances were paid
France (F)	k.A.	17.955	7.729	4.753	2.836	In addition to regular payment special allowances were paid
Great Britain	5.760	2.160	1.440	417	189	In addition to regular payment special allowances were paid
Italy	14.250	8.550	6.650	3.230	2.280	In addition to regular payment special allowances were paid
Russia	5.334	3.710	3.048	2.286	1.828	In addition to regular payment special allowances were paid
Ottoman Empire	1.720	k.A.	430	86	54	The payments not regularly take place. In addition to payment officers were also paid in kind

Table 3: Payment of officers in selected countries 1908/09 in Austrian-Hungarian Kronen
Source: Veltzés Armeealmanach 1909, Porch: The March to the Marne, page 89

The data of pension claims of officers in selected countries offer nearly the same picture as the data of payment of active officers. Table 4 shows that generals in France less pension claims than generals in Germany and in Austro-Hungarian Empire.

	Major General	**Colonel**
Germany (Pension claim after a duty of 30 years)	12.000	7.000
France (Pension claim after a duty of 30 years)	5.800	3.300
Great Britain (Pension claim after a duty of 30 years)	17.000	9.000
Austro-Hungarian Empire (Pension claim after a duty of 40 years)	11.400	7.200

Table 4: Pension claims of Major Generals and Colonels in selected countries
Source: Veltzés Armeealmanach 1909, Porch: The March to the Marne, page 89

Concluding remarks

To ensure the highest possible grade of operational readiness, armed forces need money, money and money again, a slogan which is credited Raimondo, Count of Montecúccoli.

The study about military spending in the eve of World War One showed that the Central Powers spent considerable less money to develop their armed forces than the Triple Entente. To analyze if this fact was responsible for the loss of the war by Central Powers was not an object of the study.

References

[1] [i] See Hardach Gerd: The First World War, 1914-1918, University of California Press 1977 and Pöcher Harald: Kriegswirtschaften im Ersten Weltkrieg in ÖMZ 1/2003

[2] [ii] Broucek Peter and Peball Kurt: Geschichte der österreichischen Militärhistographie, Böhlau, Köln 2000, pages 638-641

[3] [iii] Stevenson David: Armaments and the Coming War-Europe 1904-1914, Oxford University Press 1996

[4] [iv] Hermann David: The Arming of Europe and the Making of the First World War, Prineton University Press 1997

[5] [v] Conway's all the World's Fighting Ships, 1906-1921, US Naval Institute Press, Annapolis 1984

[6] [vi] See Veltze's Armee-Almanach 1906, C.W. Stern-Verlag Wien und Leipzig 1906, page 324

[7] [vii] Deák István: Der k.(u.)k. Offizier, Böhlau, Wien 1995

[8] [viii] Porch Douglas: The March to the Marne, Cambridge University Press 2003, see also Clayton Anthony: The British Officer-Leading the Army from 1660 to the present, Pearson, Edinburgh 2007

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Koronváry Péter
koronvary.peter@uni-nke.hu

TQM A KÖZSZFÉRÁBAN? VESZÉLYEK ÉS LEHETŐSÉGEK

Absztrakt

A cikk a modern vezetéstudomány történetének új felismerései alapján újraértékeli a TQM (total quality management, minőségelvű menedzsment) alkalmazásának egyes nehézségeit. A taylorizmus elterjedésével jelentkező alkalmazási problémák mintául szolgálhatnak a TQM alkalmazói számára a kockázatok előrejelzésénél. További alkalmat ad az előre gondolkodáshoz a TQM kialakulásának és elterjedésének saját története. A fő problémát az TQM elvrendszerének, ill. a hagyományos vezetési kultúrának és a fennálló szervezeti felépítésnek ütközésében jelöli meg a szerző. A megoldás része lehet a TQM elveinek össztársadalmi terjesztése az oktatási rendszeren keresztül.

The article summarises some of the possible difficulties of the introduction of total quality management (TQM) in public organisations foreseeable using new insights in the history of management thinking and practice. The history of Taylorism, the story of its adaptation may serve well in forecasting expectable difficulties and misunderstandings. A further source may be the story of TQM itself. The core of problem seem to be discrepancies between the ideas of the new management philosophy and the management culture/style and structural schemes of the adapting organisations. A part of the solution may be a nation-wide dissemination of TQM philosophy through education.

***Kulcsszavak**: menedzsment, taylorizmus, tudományos vezetés, közigazgatási vezetés, vezetéstudomány, minőségmenedzsment, teljes körű minőségalapú vezetés ~ management, Taylorism, scientific management, public management, management theory, quality management, TQM*

Ne gondolj, mondj vagy csinálj olyat, ami árthat a minőségnek. Építs olyan szervezetet, amely képes tagjait megakadályozni ebben.

A TAYLORIZMUS MINT A TQM ELŐFUTÁRA

Az ezredforduló környékén fellendülő tudománytörténeti kutatások a vezetéstudomány történetének első fél évszázadáról a vezetőképzés tankönyveiben szokásos sablontól erősen eltérő képet rajzolnak fel. A változások átrajzolják többek között az első vezetéstudományi „iskolák" és irányzatok megítélését is [1].

A 20. század elején kialakul, rögzül és letisztul az új gondolatok elterjedésének, intézményesülésének folyamata, elnyerik ebben helyüket a modern tudomány új intézményei, az egyetemek, tudományos szervezetek, a vállalatok, a szaklapok, a tudományos vita és annak modern terepei stb. Érzékelhetően elválik egymástól az új elmélet kialakulása, irányzattá válása, institucionalizálódása és globális elterjedése.

Ezen a folyamaton már a taylorizmus, a „tudományos menedzsment" módszertana is szinte mintaszerűen végighaladt. A taylorizmus egyre intenzívebben kutatott története nem csak a „valódi" taylori tanok kialakulásának és elterjedésének sikertörténetét tárja elénk, hanem a taylori tanok továbbfejlődésének sokszínű és sokirányú voltára is rávilágít: arra a komplex, multilineáris fejlődésre, mely tanítványok (pl. a Gilbreth-házaspár vagy Emerson) gondolkodásának, elveinek, kutatásainak és eredményeinek nyomán kialakuló potenciális új irányzatcsírák levárását megakadályozta és (az utókor szemében legalábbis) „belül tartotta" ezeket a taylorizmus keretein, ugyanakkor pl. a hawthorne-i kísérletek nyomán kibontakozó „emberi kapcsolatok" iskolájának hagyományos elkülönülését lehetővé tette. A taylorizmus történetének tanulmányozása új fényben mutatta meg azt a dialektikus viszonyt, mely a „tudományos menedzsment" kutatóinak gyakorlata és eredményei, valamint a módszereiket leginkább az elmélet megértése, elfogadása és internalizálása nélkül alkalmazni próbáló vulgár-taylorizmus félsikerei és félkudarcai között feszült. Taylor közel sem volt „munkásfaló", még kevésbé „kizsákmányoló", nem vádolható azzal sem, hogy hajszolta volna a munkásait, sőt, korának viszonyaihoz képest kifejezetten humánus, emberorientált elveket vallott [2]. A hatékony és eredményes termelésnek az a módszertana, amelyet ő és tanítványai kifejlesztettek, amelyet ma a tankönyvek a „tudományos menedzsment" iskolaként emlegetnek, kifejezetten védi a munkást a túlhajszolástól. A folyamatszervezési módszereik gyors elterjedése azonban nem jelentette, hogy az eszmeiségük, a munkás megbecsülése, képzése, partnerként kezelése, tisztességes fizetséggel és jutalmakkal való motiválása, a felelősség vezetői felvállalása stb. is elterjedt volna. A „vulgár-taylorizmus" szép példája annak, hogy *modern módszereket is lehet elavult módon használni és így kárt okozni*. A taylorizmus tankönyvi kritikáiban néha még mindig emlegetett társadalmi-szociális következmények épphogy nem Taylornak, hanem az őt meg nem értő, de a folyamatszervezés új, tudományos módszereit lelkesen és gátlástalanul alkalmazó kortársainak róhatók fel [3].

A 20. század első felének vezetéstudományi fejleményeinek közelebbi tanulmányozása rámutat arra is, hogy maga a „vezetéstudományi iskola" túl mereven értelmezett koncepciója jelentős félreértési lehetőségeket rejtett magában. A szokásos, a különbségeket hangsúlyozó-ütköztető tárgyalással szemben a történelmi tények vizsgálata felfedi, hogy a menedzsment gyakorlatának és elméletének fejlődésében milyen fontos szerepe volt bizonyos vállalatoknak és mérnök-menedzsereiknek. Az „emberi kapcsolatok iskolájaként" ismert csoport, amellett, hogy jelentős szerepet kaptak a híres hawthorne-i kutatásokban a Harvard Business School ipari pszi-

chológia tanszékének tanárai élükön az ikonografikus alakká vált Elton Mayoval, legalább annyit köszönhetett a Western Electric vállalatnak, amelynek a Chicago melletti Ciceroban (IL) létesült gyárában, a Hawthorne Works-ben ezek a kutatások folytak, illetve azoknak a mérnököknek, akik a kutatásokban aktívan részt is vettek. Roethlisberger és Dickson példája érzékeltetheti, hogy az „emberi kapcsolatok mozgalom" nem a taylorizmus mérnök-menedzser-kutatóival szemben jött létre a munkapszichológia hatására, épp ellenkezőleg: *a taylorizmus továbbfejlődésének egy állomásaként, annak valódi szellemiségének teljesen megfelelően* kutatták a teljesítménynövelés lehetőségeit. Az, hogy – megint csak a taylori szándékoknak megfelelően – a kutatás, elemzés és magyarázat érdekében felhasználták az akkortájt színre lépő ipari pszichológia képviselőit és tudásukat, mutatja, hogy a vezetéstudomány már gyökereiben is *interdiszciplináris alkalmazott tudomány* volt, mely a cél – a folyamatok hatékonyabb működtetése – érdekében minden elérhető, megtanulható és kitalálható eszközt hajlandó felhasználni. Ugyancsak megfelel a taylori gondolatnak a hawthorne-i kísérleteknek az a tanulsága, melynek sulykolására a tankönyvek annak történetét felhasználják, nevezetesen, hogy a szupportív (emberorientált) vezetők munkacsoportjai általában jobban teljesítenek, mint feladatorientált társaikéi, ill. hogy az emberorientált vezetés elsajátítható. Mindez természetesen nem csökkenti az emberi kapcsolatok iskolájának fontosságát – de fontos látnunk, hogy nem valamiféle, a tudományunk fejlődésében bekövetkező „ingamozgás" jelenik meg benne, amely a folyamatszervezésről az emberekre irányítja a figyelmet, hanem a Taylorral és kortársaival induló menedzsment-gondolkodás szerves továbbfejlődése, mely továbbra is aktívan és energikusan a taylorizmus alapkérdésére (t.i.: hogyan lehet a munkavégzés hatékonyságát a lehető legeredményesebben biztosítani?) a legjobb válaszokat, felhasználva mindent és mindenkit, ami és aki útjába kerül. Eredményeik sem korlátozzák a taylorizmus érvényét, hanem részletezik, kifejtik és modernizálják azt [4].

A fejlődés szerves volta mellett szól az a tény is, hogy a hawthorne-i kísérletekkel párhuzamosan zajlanak továbbra is a tudományos menedzsment jegyében értelmezhető kutatások és vezetési gyakorlat a kor olyan ipari centrumaiban, mint az említett Western Electric vagy a Bell Laboratories. Ráadásul ugyanebben az időszakban és ugyanezeken a helyszíneken tűnnek fel először azok az emberek, akiket ötven-hatvan év múltán a TQM kapcsán fogunk tisztelni: az előfutár-mester Shewhart és tanítványa, Deming, valamint Juran a taylorista módszerek és hagyományok örökösei, folytatói és továbbfejlesztői.

Walter A. Shewhart (1891-1967) élete és vezetési gyakorlata legalább két fontos momentummal gazdagíthatja a korról alkotott képünket. Nem csupán azért tarthatjuk a taylorizmus egyik továbbvivőjének, mert mind a Western Electric-nél, mind a Bell Telephone Laboratories-nél dolgozott – a problémamegoldáshoz való hozzáállása volt a szó legnemesebb értelmében taylorista. Ő volt az, aki a matematikai megközelítésekre mindig is nyitott tudományos menedzsmentet végképp összekötötte a statisztikával [5]. Statisztikai módszereivel és a munkafolyamatok menedzsmentjében alkalmazott négylépéses eljárásrendjével („tervezd meg, csináld, ellenőrizd, javítsd") nem csak a taylorizmus eszköztárát fejlesztette, de egyúttal előfutára lett a TQM-nek is. Fontos felismerése, miszerint a hibát jobb megelőzni, mint kiszűrni, a demingi gondolkodás sarokköve lesz. A gyakorlatban is a hangsúlyt a folyamattervezésre és -javításra helyezte. Innen már csak egy lépés a TQM egyik (igazi taylorista) alapelve, miszerint statisztikai adatgyűjtés és -értékelés, sőt igazából minden ellenőrzési (*controlling*) módszer, folyamat és rendszer értelme a folyamatok hatékonyságának és eredményességének javítása, nem a dolgozók ellenőrzése. Ő és fiatalabb kortársai, többek között Deming és Juran is ilyen és hasonló eszközökkel segítették a 2. világháború alatt a hadigazdaság hatékony működését. A TQM megszületését és elterjedését azonban ő már nem érhette meg.

MI AZ A TQM – VALÓJÁBAN?

A TQM [6], ahogy láthattuk, szerves folytatása a taylorizmusnak. Szigorúan véve a „*Total Quality Management*" kifejezés bevezetése azonban jóval későbbi – az irányzat hivatalos „keresztelőjét" csak a 80-as években tartották meg. Japánban, ahol kibontakozott, nem így nevezték, úgy tűnik nem is volt egyetlen, mindenki által elfogadott elnevezése. A legelterjedtebb talán a CWQC („*Company-Wide Quality Control*") elnevezés arra a módszertanra és vezetői gondolkodásra, amelyet Deming, Juran és számos más amerikai társuk hozzájárulásával a japánok az ipari gyakorlatban kialakítottak. Az, hogy a 2. világháború után ilyen kiváló szakemberek segítették a modern japán közigazgatási szervezet és az ipar újjáépítését, óriási szerencse volt. Az eredetileg állami megbízásból és feladattal Japánba érkező Deming például mintegy mellékesen kezd el előadásokat tartani a statisztikáról és a folyamatjavításról a japán menedzsereknek. Ezeknek azonban akkora hatása volt, hogy 1950-re a helyi menedzserek gyakorlatilag felvállalták az előadásokban és vitákban kibontakozó vezetési rendszert. Két évtized alatt meg is hozta az eredményét – a hetvenes években már ők jártak az Államokba előadásokat tartani az iparszervezés új módszertanáról, segítve ezzel az amerikai ipar megújítását. Új nevét azonban csak akkor kapta meg, amikor az amerikai haditengerészet 1984-ben a Deming-féle elvrendszert választotta a saját szervezeti reformjának filozófiájául [7].

A TQM VEZETÉSI KONCEPCIÓJA

A demingi koncepció [8] sarokköve, hogy a megfelelő vezetési elvek alkalmazása mellett lehet csak a minőséget javítani és élvezni ennek mellékhatásait, pl. a költségek csökkenését azáltal, hogy csökken a pazarlás, a selejt, a lemorzsolódás, a munkaügyi perek száma stb., vagy az ügyfelek elégedettsége és elkötelezettsége nő. Hibás szemlélet mellett mindez nem működik. A hibás vezetői szemlélet forrása, hogy a vezetők nem érzékelik kellőképp a társadalmi-gazdasági-technológiai haladást, a világ – és bennük a szervezetek és a munkaerő – változását. Míg Taylor korában, az akkori feltételek mellett a természetes kihívás a menedzserek előtt igenis lehetett a költségcsökkentés, hiszen a körülményeik sajátosságai (tanulatlan, sokszor a nyelvet nem beszélő, kiképzetlen, felkészületlen, motiválatlan dolgozók tömege, hagyományos és esetleges munkavégzési és munkaszervezési szokások, nem megfelelő, célirányos eszközök és munkakörülmények stb.) szinte predesztinálták a termelést a selejtre és pazarlásra. Az a világ azonban már rég eltűnt. Az új korszakban, ahol az általános iskolázottsági szint jóval magasabb, ahol a munkaerő tipikusan képzett és motivált szakember, a költségek csökkentésére koncentráló vezetés pont az ő motivációjukat csökkenti, együttműködési készségüket és szakismereteik alkotó felhasználását téve lehetetlenné.

*A TQM bevezetését a vezetőkön kell kezden*i. Olyan vezetői kultúrát, olyan vezetői mentalitást kell kialakítani, amely természetessé teszi a vezetői önvizsgálatot és önátalakítást. Meg kell őrizni, sőt fejleszteni kell a vezetők nyitottságát az új világ más körülményei iránt. Csak az ilyen vezető tudják alkalmazni azokat az ismereteket, melyeket nap mint nap használniuk kell. A vezetői ismereteknek dinamikus egységben kell tudni tükrözni (1) a vezetett folyamatok, folyamatrendszerek működésének és sajátosságainak alapos megértését; (2) a tervezettől való eltérések ismeretét, beleértve annak különböző fajtáit és sajátosságaikat, okait, mértékét és mérésük lehetőségeit, ill. ezek korlátait; (3) a kapcsolódó elmélet nyújtotta magyarázatokat és azok korlátait; valamint (4) az emberi természetet, a lélektant.

Ebben a szellemben fogalmazta meg Deming a maga vezetési elveit. Ezek egy része a klaszszikus fayoli, emersoni stb. elvek megerősítése, a többi viszont már az új kor szellemiségét tükrözi. Mi kell tehát – Deming szellemében – a TQM bevezetéséhez?

1. *Egységes szervezeti szándék* és elkötelezettség a közös célok mellett. Olyan céloknak például, mint a minőség, a versenyképesség, a vállalat életben tartása, a munkahelyek megtartása minden résztvevő fél számára fontosnak kell, hogy legyenek. Ha nincs mellettük erős és egyértelmű *közös* elkötelezettség, a TQM bevezetése nem lesz, nem is lehet sikeres.
2. Az új kor *új gondolkodást*, új „filozófiát", új koncepciókat követel. Nem lehet olyan elvekre és megoldásokra építeni, melyek lényege a képzetlen és motiválatlan tömegek mozgatása. Internalizálnunk kell azokat a gondolatokat, melyek segítik megértenünk: már nem a motiválatlan segédmunkás betanítása, majd szakmunkássá képzése a kihívás, sőt nem is a képzett és motivált szakmunkások hatékony és eredményes munkáltatása, hanem valami teljesen más: magasan képzett, belsőleg motivált emberek munkájának menedzselése. Ha ezt nem sajátítjuk el, mit fogunk tenni egy olyan világban, ahol a munkafeladatok már annyira összetettek és speciálisak, hogy a vezető (különböző körülmények folytán) már nem is ismerheti azokat kellő mélységben? *Hogyan fogunk vezetni olyan dolgozókat, akik a munkájukhoz nálunk sokkalta jobban értenek?*
3. Az ellenőrzés maga *nem* vezet minőséghez – a minőség a termék tulajdonsága, azt a munkás „építi bele". Ebben viszont az ellenőrzés éppen hogy megakadályozhatja. Philip Crosby (1926-2001) megfogalmazásában: a minőség *előre* felállított követelményeknek való megfelelés, ahol a követelményeket a felhasználói elvárások alapján határozzák meg. Innentől kezdve *a minőséget nem az értékelés, hanem a megelőzés állítja elő – a minőségellenőrzés adatai nem a minőség mutatói, csupán a követelményektől való eltéréseket, pontosabban ezek árát érzékeltetik* [9].
4. Ne az egyes beszerzések költségét kell leszorítani, hanem a *hosszú távú összköltséget* azzal, hogy stratégiai távon, megbízhatóan, minőséget szállító partnerekkel működünk együtt.
5. A termelési-szolgáltatási rendszer, a minőség és a termelékenység *folyamatos* javítása, fejlesztése biztosítja a költségek csökkenését.
6. A *munkahelyi szakképzés* az emberi erőforrások folyamatos fejlesztésének legfontosabb eszköze. Ez biztosítja, hogy aki a munkát végzi, az a lehető legjobban értsen hozzá. Ha pedig ő ért a munkájához a legjobban, egyre inkább a dolgozó lesz az, aki a maga munkafolyamatának javításához hozzájárulni.
7. *Támogató* vezetésre (*leadership*) van szükség. A cél *nem* az ellenőrzés, hanem a dolgozók segítése abban, hogy jobban, eredményesebben végezhessék a munkájukat. Ehhez azonban új típusú vezetési szemlélet és gyakorlat kell, melynek ellenőrzését éppúgy új alapokra kell helyezni, mint a munkásokét.
8. *Bizalmat* kell teremteni – a megélhetésükért rettegő dolgozók képtelenek a hatékony és eredményes munkára. A hibákat a rendszer okozza, nem az alkalmazottak.
9. Olyan *modern szervezeti felépítési formát* kell alkalmazni, ahol a közös dolgon munkálkodók egy teambe tartozhatnak akkor is, ha más-más szakterületet képviselnek. A hagyományos funkcionális szervezeti felépítés erre nem elég.
10. *Meg kell szüntetni a semmitmondó vagy túlzó szlogenekre épülő propagandát*, mert ezek ellenségességet szülnek. Nem várható hibátlan munkavégzés vagy új termelékenységi szintek megugrása, ha ezek feltételeit (melyek egyébként jórészt kívül állnak a dolgozók hatáskörén!) nem biztosítjuk. El kell törölni a kvantitatív ellenőrzési eszközöket, mert csökkentik a dolgozók motiváltságát. A képességek fejlesztése viszont erősíti azt, sőt jó közérzetet teremt.
11. *Ne alkalmazzunk numerikusan rögzített célokat* a teljesítménytervezésben. Ha a számosított célokat a dolgozó eléri, az elégedettsége kérészéletű lesz, mert ott fog mocorogni az ő és a vezetője fejében egyaránt a gondolat, hogy túl alacsonyra volt téve a léc; ha viszont nem éri el, az csalódást okoz akkor is, ha egyébként a korábbinál jobban

teljesít. A nem megfelelően alkalmazott ellenőrzési eszközök inkább akadályozzák, semmint segítik a minőség előállítását, ezért használatuk káros. *Meg kell adni a lehetőséget arra, hogy a dolgozó büszke lehessen a munkája eredményére.*

12. Ugyanez a jog a saját munkájukra való büszkeségre meg kell illesse a vezetőket, menedzsereket és mérnököket is. A tervezés és ellenőrzés rögzített számai az ő esetükben éppúgy inkább demotiválnak, mint motiválnak. Nem versenyeztetni kell, hanem folyamatos, érdekes, élvezetes, motivált és *folyamatosan eredményes* munkára kell lehetőséget biztosítani, melyben a teljesítmény javulásának alapja a belső motiváció és az önmagunkkal szemben támasztott teljesítményigény.
13. A munkahelyi szakmai képzés mellett szükség van egy olyan, erőteljes *oktatási, képzési, önképzési programokra* is, mely a szervezet tagjainak szellemi fejlődését, horizontjuk tágulását, regenerálódását stb., szakmailag releváns vagy akár a munkájukhoz kevéssé kapcsolódó területeken való fejlődésüket egyaránt serkenti.
14. *Az átalakulásba mindenkit be kell vonni.* A TQM bevezetése, az új, minőségalapú szervezeti gondolkodás és kultúra elterjesztése mindenki feladata és felelőssége kell, hogy legyen [10].

Deming hangsúlyozza, hogy *az átalakulás elsődleges feltétele a rögzült, elavult, hibás gondolkodási képletek és hagyományok megtörése*. Az ehhez szükséges bátorságot bele kell nevelni az emberekbe, amihez erőteljes átképzés, sőt átnevelés szükséges. Ennek a tanulási folyamatnak a része minden egyes olyan feladat új szemléletű elemzése és végrehajtása is, amit a munkatársak a maguk munkakörében egyébként is ellátnak.

Ahhoz, hogy az új kor új lehetőségeit, konkrétan a jól képzett dolgozók kreativitását és jobbítási törekvéseit ki lehessen használni, a Shewhart-kör, a „tervezd, végezd, ellenőrizd, fejleszd/javítsd” ciklus már nem csak vezetői munkamódszer kell, hogy legyen – ugyanígy kell a képzett dolgozónak is hozzáállnia saját munkájához. Ez biztosítja, hogy felnőttként viselkedhessen és kibontakoztathassa a benne lévő potenciált, hiszen nem irányítják, mint valami kezdőt, hanem érett, felelősségteljes és döntésképes személyiségként kezelik, akinek természetes joga és elvárása, hogy hatással lehessen a munkájára és ezen keresztül a saját (és a szervezet) jövőjére. A beosztott innentől kezdve válhat partnerré. Ezt a Taylor tanaiból egyébként levezethető gondolatot Kaoru Ishikawa (1915-1989) tette a minőségmenedzsment gyakorlatának egyik alapkövévé [11].

A TQM vezetési elveit kiegészíthetjük az „alapító atyák” további meglátásaival is. Joseph M. Juran (1904-2008), aki hasonló karrierutat járt be, mint Deming, hisz dolgozott a Western Electricnél, majd Japánban is, saját, Demingtől függetlenül kialakított gondolati rendszerében kitér arra, hogy – mint ahogy maga a folyamatszervezés is – a minőségmenedzsment nem csupán a termelés területén alkalmazható és alkalmazandó, hanem *a szervezet gyakorlatilag bármely funkcionális területén* [12]. Az, hogy a szükséges gondolkodás szervezeti kultúrába integrálása a japán tapasztalat szerint legalább két évtizedet és a szervezet csúcsán kezdődő és lefelé haladó képzéssorozatot igényel, Juran számára kulcsfontosságúvá teszi a vezetőképzést és a minőségmenedzsment emberi, kulturális oldalát. Megtapasztalhatta, hogy a japánoktól eltérően mekkora ellenkezést váltott ki az amerikai vállalatoknál az a gondolat, hogy a felső- és középvezetőknek alá kell vetniük magukat újabb és újabb képzéseknek. Ő hozta be a vezetői gondolkodásba a Pareto-arányt is annak hangsúlyozására, hogy a kevesebb, de kritikus hatású ügy kezelése ugyan a túlélés, a gyors fejlődés, a siker záloga lehet, de azért a mindennapokban a többi tényezőről sem szabad megfeledkezni. [13]

Juran módszere szerint a minőségmenedzsment előkészítési folyamata a tervezés, ellenőrzés és javítás három lépéséből áll: (1) a tervezésnél tisztázni kell, ki az ügyfél, mire van szüksége, mit jelent ez a szolgáltató számára, milyennek kell lennie a megfelelő terméknek, és hogyan lehet azt az ügyfél igényeihez igazítani; (2) a javítások sorozatán keresztül ki kell alakítani azt az optimális folyamatot, mely a tervezett terméket állítja elő; végül (3) az ellenőrzés fázisában

bizonyítani kell, hogy a folyamat az adott működési feltételek között, minimális ellenőrzés mellett a kívánt terméket képes előállítani. Ha ez sikerült, a folyamatot át kell helyezni végső helyére, termékelőállítás esetén az illetékes gyártási részleghez.

Végül egy utolsó gondolat a TQM klasszikusaitól. Genichi Taguchi (1924-2012) hangsúlyozta, hogy a minőség (vagyis a felhasználó szükségletei szerint tervezett termék) előállításának a költségei alacsonyabbak, mint amennyit költenünk kell tervektől való eltérés esetén. *Az ilyenkor jelentkező extra költségek nem csupán a gyártót, hanem a társadalmat is feleslegesen terhelik* [14]. A nem minőségelvű gazdasági szervezetek az egész társadalom erőforrásait pazarolják feleslegesen. A pazarlás fogalma lesz a minőség után a következő „hívószó", amely a japán menedzsment-gondolkodás egy újabb szakaszát fogja jellemezni: a *lean management* (a „karcsú", vagy inkább „szikár", „takarékos" menedzsment) korszakát.

MILYEN ELŐFELTÉTELEI VANNAK A TQM BEVEZETÉSÉNEK A KÖZSZFÉRA SZERVEZETEIBEN?

Az eddigiek alapján azonnal feltűnik, hogy a közszervezetekben a TQM bevezetésének a feltételei nehezen tekinthetők a lehető legteljesebb mértékben adottnak. Vegyük sorra az akadályokat.

15. *Idő nélkül nem megy.* Ha csak jelképesen elfogadjuk a japán minta relevanciáját, durván két évtizeden át kellene „tanulnunk", gyakorolnunk a TQM gondolkodását ahhoz, hogy az átjárhassa a szervezeti kultúrát. Ilyen távú politikai vagy szakmai elhatározásra racionálisan ma nem számíthatunk. Reményre annyiban láthatunk okot, hogy a TQM alapértékeinek egy része a ma Magyarországon talán jobban elterjedt, mint az ötvenes évek Japánjában. Ha a társadalom más területein ez a fajta vezetői gondolkodás meggyökeresedik, a közszervezeteknél is könnyebb lesz a helyzet. Ha a vezetőképzés legkülönbözőbb szintjein és oktatási formáiban képviseltetve lesznek a TQM gondolkodási képletrendszerei és metodológiája, a „tanulási idő" is rövidülhet.
16. *Az elvek internalizálása nélkül nem megy.* A szervezetek átitatása az új gondolkodással a felső- és középvezetés folyamatos továbbképzésével (is) jár a japán minta szerint. Ennek elmaradása – látjuk a TQM az amerikai történetének példáján is – torzítja az eredményt. Ugyanakkor kérdés, hogy az ehhez szükséges elszánás és erőforrások rendelkezésre állnának-e akár egyéni, akár szervezeti oldalon. Rövid távon súlyos kiesést jelent minden közszervezet számára, ha kulcsemberei rendszeresen képzéseken vesznek részt. A jó hír, hogy az új oktatási technológiák, az internet, a távoktatás, a munkahelyi képzés és az önképzés még kihasználatlan lehetőségei enyhíthetnek a kiesésen. A folyamatos vezetői önfejlesztés iránti belső igényt társadalmi szinten egy varázsütésre kiépíteni ha nem is lehet, terjedését elősegíteni talán igen.
17. *Decentralizáció nélkül nem megy*. A TQM gyakorlata centralizált, funkcionális, lineáris szervezetekben nem működtethető úgy, hogy hosszabb távon ne torzuljanak maguk a folyamatok. A közszervezetek felépítését és működését azonban többnyire központosítva, törvények útján szabályozzák, ami a vertikális decentralizáció ellen hat. Csak olyan közszervezetnél lehetséges tehát a TQM alkalmazása, amelynek megvan a törvényes lehetősége saját belső működési rendszerének megfelelő átalakításához.
18. *A munkatársak nélkül nem megy.* A TQM erősen épít arra, hogy mindenki a maga munkájában a Shewhart-ciklus szerint működik. Ez viszont feltételezi, hogy a munkatársak a maguk munkájának nem egyszerűen szakemberei, de *szakértői* – mind képzettségük, mind tudásuk, mind gyakorlatuk, mind szervezetbeli megítélésük szempontjából. A szervezeti munkafolyamatokat tehát úgy kell felépíteni, hogy a munkaterhelésébe mindegyiküknek bele is férjen annak elemzése és javítása. A minőséget az

ő munkájuk építi be a szervezet termékeibe, szolgáltatásaiba – a vezetés fő feladata, hogy biztosítsa ehhez a feltételeket.

19. *Tervezés nélkül nem megy*. A minőség lényege, hogy a Shewhart-ciklus lépéseit betartva még az előkészítési szakaszban kiszűrjük, kijavítjuk a lehetséges hibákat, aztán vezetjük be az új folyamatot. Minél alaposabb az előkészítés, annál több ráfordítást takarítunk meg szervezeti és társadalmi szinten egyaránt (pl. károk, javítási költségek, időveszteség stb.).
20. *Bizalom nélkül nem megy.* Az ellenőrzés és tervezés hagyományos megoldásai lehet, hogy szükségesnek látszanak a vezetők szemében, ugyanakkor legtöbbször akadályozzák a minőségi munkát. Ilyen esetben mindig az alapszabálynak kell érvényesülnie: ne gondolj, mondj és tégy semmit, ami árthat a minőségnek, és másnak se engedd. Olyan ellenőrzési (*controlling*) rendszert kell működtetni, amely nem vesz el időt a munkától, nem rombolja a motivációt, és nem a dolgozók ellen irányul. *Az ellenőrzés egyetlen célja, hogy segítsünk mindenkit abban, hogy a maga munkáját egyre jobban, hatékonyabban, eredményesebben és elégedettebben végezhesse.*

Végül, Deming szellemében: nyitottnak kell lenni az új gondolatok, modern problémák és modern megoldások előtt. Lehet, hogy megfontolandó lenne a közszférában is a TQM-ből kinőtt, azt folytató szervezésmódszertan, *lean* menedzsment alkalmazási lehetőségeiről is gondolkodni.

Felhasznált Irodalom

[1] Morgen Witzel: *A History of Management Thought* (Routledge, 2012) a szemléletbeli átalakulást az utóbbi időben talán legjobban érzékeltető munka.

[2] Dobák Miklós és Antal Zsuzsanna: *Vezetés és szervezés* (Akadémiai Kiadó, 2013) p. 340. Vö.: Stephen P. Robbins és Mary Coulter: *Management* (Prentice Hall, 20121[1ed]) pp. 29-30 és 270-271, Mauro F. Guillén: „Scientific Management's Lost Aesthetic: Architecture, Organization, and the Taylorized Beauty of the Mechanical", *Administrative Science Quarterly* 42 (1997) pp. 682-715, továbbá S. Wagner-Tsukamoto: „ An Institutional Economic Reconstruction of Scientific Management: On the Lost Theoretical Logic of Taylorism", *Academy of Management Review* (2007 január) pp. 105-117.

[3] Witzel (2012), pp. 321ff.

[4] Witzel (2012), p. 152.

[5] Walter Shewhart: *Economic Control of Quality of Manufactured Product* (D. Van Nostrand Co. Inc., 1931) és uő: *Statistical Method from the Viewpoint of Quality Control* (Washington, The Graduate School, The Dept. of Agriculture, 1939); Lloyd S. Nelson: „The Shewhart control chart-tests for special causes" *Journal of Quality Technology* (16(4), pp. 237-239.

[6] Arthur R. Tenner és Irving J. DeToro: *Teljeskörű minőségmenedzsment* (Műszaki Könyvkiadó, 1996) illetve Thomas Pyzdek és Paul Keller: *Handbook for Quality Management* (McGraw Hill, 2013[2ed])

[7] Poorinma M Charantimath: *Total Quality Management* (Pearson, 2011[2ed.]) p. 59.

[8] William Edwards Deming: *Out of the Crisis* (MIT Center for Advanced Engineering Study, 1986) és uő: *The New Economics for Industry, Government, Education* (MIT Center for Advanced Engineering Study, 1993).

[9] Philip Crosby: *Quality is Free* (McGraw-Hill, 1979) és Bill Creech: *The Five Pillars of TQM* (Truman Talley, 1995) p. 478.

[10] Mark A. Vonderembse és Gregory P. White: *Operations Management* (West, 1996[3ed]) pp. 83f.

[11] Kaoru Ishikawa: *What Is Total Quality Control the Japanese Way?* (Prentice Hall, 1985)

[12] Joseph M. Juran és A. Blanton Godfrey: *Juran's Quality Handbook* (McGraw-Hill, 1999[5ed])

[13] A TQM filozófiájának kifejtéséhez l. Kövesi János és Topár József (szerkk.): *A minőségmenedzsment alapjai* (Typotex, 2006) 4. fejezet, pp. 55ff.

[14] Genichi Taguchi: *Introduction to Quality Engineering: Designing Quality into Products and Processes* (Quality Resources, 1986)

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Koronváry Péter
koronvary.peter@uni-nke.hu

KICSODA A VEZETŐ? GONDOLATOK A VEZETŐI FELELŐSSÉGRŐL

Absztrakt

A cikk a vezető tankönyvi meghatározásaiból kiindulva segít végiggondolni néhány szokatlan gondolatot a vezető szerepével és identitásával kapcsolatban. Rávilágít arra, hogy a vezető önmagában nem létezik, kell a beosztottak elfogadása ahhoz, hogy a vezetői szerep érvényesüljön. Ennek megnyeréséhez a pozicionális hatalom mellett más autoritásformák is szükségesek: pl. a szakmai hozzáértésből, vagy az erőforrásokhoz való hozzáférésből származó autoritás. Az utóbbi kiemelkedően fontos, ha olyan helyzetben kell vezetni, amikor magunk nem értünk az elvégzendő tevékenységhez. A vezető szokványos meghatározásaihoz a cikk a felelősség kiemelése és a szokványosnál tágabb értelmezése mellett két ritkább fogalmat rendel hozzá: az elfogadást és az elkötelezett, kutató érdeklődést a szervezet, a beosztottak, a munka és a vezetői tevékenység iránt.

The article, starting with some textbook definitions of management, aims to think over some less common ideas concerning the role and identity of the manager. It pinpoints the fact that no leadership may exist without the acceptance of the followers. To acquire acceptance, modern managers need other types of authority beside positional power: either professional knowledge or the personal access to necessary resources may serve as such. Beside the emphasis on a wider than usual interpretation of responsibility, the article adds two rarely considered concept to the definition of the leader: the idea of acceptance and the open-minded, committed interest in a deeper understanding of management, leadership, organisations, follower behaviour and the world of work.

Kulcsszavak: *vezetés, vezető, követői magatartás, szervezet, kutatás, facilitálálás, felelősség ~ management, leadership, organisation, followership, research, facilitation, responsibility.*

„A vezetés feladata, hogy képessé tegye az embereket a közös teljesítményre, hatásossá tegye erősségeiket, és jelentéktelenné gyengeségeiket.”
(Peter Drucker)

EGY ÖRÖKKÉ RELEVÁNS KÉRDÉS

Ki is az a vezető? Ezzel a kérdéssel foglalkozni első látásra már-már kellemetlen. Elvégre mindenki tudja. Vagy mégsem? Az *Encyclopedia of Management* például sem a *leader*, sem a *manager* szavakat nem tartja érdemesnek egy-egy szócikkre, megelégszik a *management*, illetve a *leadership* tárgyalásával [1]. Ezek szerint a vezető az lenne, aki vezet … a gyakorlatból azonban tudjuk, hogy ez nem feltétlen van így. Nem mindenki szakács, aki képes egy rántottát elkészíteni.

Márpedig vezető van mindenhol, függetlenül attól, hogy kis csoportban keressük vagy nagyban, a családban vagy az osztályteremben, a vállalatokban vagy nonprofit szférában, állandó szervezetekben vagy ideiglenesekben, művészeti vagy politikai csoportosulásokban, populáris vagy elegáns helyeken. Akkor hát mi alapján ismerjük fel őket?

Nem mindig olyan a vezető, amilyennek képzeljük. Nincsenek könnyen azonosítható testi vagy viselkedésjegyeik. Nem mindig az a vezető, aki annak látszik, sőt, nem is látszik mindig vezetőnek, aki pedig az. Nincsenek kőbe vésett szabályok a vezető felismerésére – a névtábla az irodaajtón vagy a vizitkártya, bár jól eligazít, mégsem mindig tévedhetetlen. Mindenkiből lehet vezető, ha olyan vezetési helyzet alakul ki, amely őt „löki” ebbe a pozícióba, és mindenkiből lehet jó vezető, ha képességei és tulajdonságai, személyisége és tudása az adott helyzet sajátosságainak megfelelőek, illetve a hiányzóakat képes kellő gyorsasággal megtanulni, elsajátítani, kifejleszteni. A lehetőség és a képesség azonban nem kötődik automatikusan egymáshoz, még akkor sem, ha a motiváltság és a képesség a vezetésre ki tudja alakítani a kellő helyzetet.

A vezetéstudomány bevezető tankönyvei, ami a definiálást illeti, már kevésbé önmegtartóztatóak, mint a vezetéstudományi enciklopédia – a kínált meghatározások, még ha többször inkább körülírások is, meglehetősen sokfélék. Idézzünk fel itt három, meglehetősen különböző példát, hogy láthassuk, mekkora ez a sokféleség:

- *A vezető az a személy, aki csoportja tagjainak munkateljesítményéért felelős.* [2] Csak olyanok vannak, melyek levezethetők a teljesítményért való felelősségből? Csak a beosztottjai munkateljesítményéért? A csoporttagok egymás teljesítményéért nem lehetnek felelősek? Esetleg más csoportok vagy más csoporthoz tartozók teljesítményéért?
- *A vezető az, aki összehangolja és felügyeli mások munkáját, hogy a szervezeti célok teljesülhessenek. A vezető munkája nem a saját eredményeiről szól, hanem mások segítéséről abban, hogy munkájukat elláthassák.* [3] Itt viszont a felelősség hiányzik. A vezetői eredményesség megfogalmazásában a felettesek szempontja (ti. a feladatok teljesülése) jelenik csak meg a magyarázatban, de a másik két fontos szempont – a munkatársaké és a szervezeté – nem. Ráadásul azzal, hogy a lehetséges célok közül kiemelik a szervezetieket, azt az érzést keltik, hogy a vezetés csakis valamely formális (jogilag meghatározott) állapot lehet.
- *A vezetők érik el, hogy a dolgok megtörténjenek a vállalatnál. Az eredeti üzleti ötlettől kezdve a működtetéséhez szükséges erőforrások megszerzésén és felhasználásuk legjobb módjának meghatározásán át az emberek kezeléséig a vezetők [minden téren] felelősek a vállalat sikeréért vagy bukásáért. A vezetők döntései határoztatják meg, mit*

tesz a vállalat és milyen jól fog teljesíteni.[4] Ez a definíció már jóval erősebben hangsúlyozza a vezető feladatainak komplexitását, mint az előzőek – de még mindig inkább arra keres, választ, MI a vezető, és nem arra, KICSODA.

KICSODA A VEZETŐ?

A jó felettes: szerencse. Méghozzá nagy. Legalább akkora, mint amekkora istenverése a rossz. Amíg azonban az utóbbit mindenki tudja, az előbbi csak akkor tudatosul bennünk, ha volt már igazán rossz vezetőnk.

A jó felettes életre szóló pozitív hatással lehet a munkatársaira szakmai és személyes téren egyaránt – akár döntő mértékben is meghatározhatja további karrierünket, döntéseinket, életünket. A rossz viszont rombol és visszavet.

A jó felettes energiát sugároz, élvezetessé téve a munkahelyet és eredményessé a munkát. A rossz energiákat szív el feleslegesen.

A jó felettes kihívások elé állítja és sikerre viszi csoportját, ezzel is építve belső motivációjukat. A rossz kudarcot képes csinálni az eredményekből is.

A jó felettes a stratégiai kudarcot taktikai győzelmekkel kárpótolja. A rossz viszont a taktikai kudarcok stratégiai győzelemként való beállításával próbálja magyarázni a bizonyítványt.

A rossz felettest a megbízása vagy kinevezése teszi – formálisan – elöljáróvá. Ez a formális aktus pozicionális hatalommal ruházza fel, vagyis a szervezeti szabályok értelmében utasítási és ellenőrzési joggal rendelkezik. Mindez azonban csak akkor ér valamit, ha a beosztottak ezt *elfogadják* – kényszerből, mert sakkban tarthatók a megélhetésükkel, vagy mert szeretik a munkájukat, kollégáikat, elkötelezettek a munkahelyük iránt. Az ilyen zsarolás azonban ritkán működik hosszú távon – szinte humánpolitikai közhely, a munkahelyüket elhagyó dolgozók túlnyomó többsége a felettesük miatt távozik. Ha az elfogadás hiányzik, a felettesből nem lesz „főnök", nem lesz vezető.

Érdekes, hogy a vezető személyes elfogadását mint kritériumot tulajdonképpen a hawthornei tanulmányok [5] óta ismerjük. Mayo és társainak eredményei egyértelművé tették, hogy a formálisan kinevezett elöljárók akaratérvényesítési lehetőségei a munka eredményessége terén igencsak korlátozottak akkor, ha nem „szupportívak" (vagy újabb kifejezéssel: „emberorientáltak"), vagyis nem illeszkednek be sikeres kommunikációjuk és szociális magatartásuk segítségével az informális hálózatokba – magyarán szólva nem fogadja be őket a „szerves" közösség. A csupán pozicionális hatalommal rendelkező felettesnek ugyanis – legyen szó akár ígéretről, akár szakmai véleményről – egyszerűen nem fognak hinni az emberek. Minél hagyományosabb, minél inkább a klasszikus centralizált, bürokratikus, funkcionális berendezkedésű az adott szervezet, annál valószínűbb, hogy szervezeti kultúrájában a szervezeti elöljárókba vetett bizalom csak kevéssé játszik szerepet.

Minél jobb az alkalmazottak szakmai felkészültsége, minél gyakorlottabbak és képzettebbek, annál feltűnőbb, ha a pozicionális hatalom mellé nem járul a szaktudás elismertségéből eredő autoritás. A 21. században azonban láthatólag egyre többször olyan feladatok elé állít embert és munkacsoportot egyaránt a szervezet, melyek vagy új voltuk, vagy komplexitásuk okán meglevő szaktudásával nem tudhat a felkészült vezető sem átfogni. Az „szupportív", vagyis támogató, facilitáló (feltételeket biztosító) vezetés, a konszenzuális csoportok hálózatára alapuló szervezet hatalom-alapú irányítással és a vertikálisan meghatározott, szélsőségesen a hierarchia biztosította utasítási láncra alapozó szegényes kommunikációval szemben, ilyenkor is rejt magában megoldási lehetőségeket. Nem helyes ezt összekeverni az autoriter elöljáró feladatorientáltságával – ellenkezőleg, a facilitáló vezető egy konszenzuális szervezetben a csoport feladatáról természetszerűleg leválasztja a sajátját, egy hierarchikusabb, centralizáltabb szervezetben pedig „burokba helyezi" a csapatát, melyen belül a másféle szervezeti szokások ellenére a tagok képesek lesznek konszenzuális szakmai működésre [6].

A kérdésünkre egyfajta válaszhoz elvezethet a facilitálás fogalma. Mi az, amit a facilitáló vezetőnek biztosítania kell a maga szakmailag jól felkészült, esetleg multidiszciplináris csapata számára, ha eredményt akar eléretni velük akkor is, amikor ő maga a feladat komplexitása (vagy önmaga más jellegű előképzettsége és tapasztalatai) miatt a munkatársainál kevésbé – vagy akár semennyire sem – képes értékelni és elemezni az előálló döntési helyzeteket és meghozni a kellő döntéseket? Biztosítania kell, hogy teamje szakértői mindezt helyette megtehessék. Ennek feltétele, hogy (1) a teamtagok nyílt, szakmai kommunikációt folytathassanak egymással, (2) rendelkezésükre álljanak a kellő eszközök és erőforrások, illetve (3) a kellő nyugalom, valamint hogy (4) mindemellett a team kellő mértékben beilleszkedhessen a szervezetbe. A facilitáló vezető tehát alapvetően négy dolgot fog tenni:

- megszervezi a teamtagok közötti (laterális) szakmai kommunikációs hálót anélkül, hogy ő maga ebben centrális helyet foglalna el, vagy akár érdemben részt venne,
- eléri, hogy a szervezet a szükséges mértékben és minőségben biztosítsa számukra a megfelelő feltételeket és erőforrásokat,
- a szükséges mértékben elszigeteli a teamjét a zavaró tényezőktől, akár önmagáról, akár a felettesekről, akár kívülállókról legyen szó,
- maga tesz eleget a szervezet kívánta olyan követelményeknek, mint például a jelentési kötelezettség, hiszen (1) a teamtagok ideje túl drága ehhez, (2) nem valószínű, hogy a szakmai nyelvezetű, bonyolult jelentéseket a (szintén) nem szakértő felettesek megfelelően értelmezni tudnák, ezért a facilitáló menedzsernek magának kell ezt a feladatot is ellátnia.

Nyílt szakmai kommunikáció, biztonság, a szükséges erőforrásokhoz való hozzáférés – és a team le fogja venni a felettes válláról a szakmai vezetés számára vállalhatatlan feladatait. Nem neki kell majd a szakmai kérdések megválaszolását, a szaktudást igénylő döntések előkészítését és meghozatalát, valamint a feladat megoldását biztosítani – meg fogja tenni mindezt helyette a szakértői team. Annyiban kell csupán a vezetőnek tájékozódnia, hogy tudja, mely erőforrásokra lesz szükség a következő periódusban, illetve mit kell jelentenie. A többit szinte automatikusan megoldja helyette a spontán csoportszerveződés.

Érzékelhető azonban a fenti eszmefuttatásból is, hogy a vezető „pozicionális", beosztásából adódó hatalma itt is kiegészül egy másik autoritás-típussal. Az erőforrásokhoz való hozzáféréshez szükséges kapcsolati háló a vezető számára olyan hatalomforrás, amely biztosítja számára az alapot arra, hogy a csoport elfogadja. Ebben az értelemben tehát a vezető az, aki szervezeti kapcsolatait mozgatva az ezeken keresztül elérhető erőforrásokat a csoportja számára biztosítja, ugyanakkor képes arra is, hogy megvédje annak nyugalmát és biztonságát a szervezet és környezete zavaró tényezőivel szemben, valamint hogy megszervezze a belső, egyidejűleg pedig ellássa a külső (a szervezet más részeivel folytatandó, hivatalos) kommunikációt Mindezek révén a vezető biztosítja magának a csoporttagok elfogadó hozzáállását, az informális csoportba való illeszkedés lehetőségét. A facilitáló vezető ily módon éppúgy felelős az egységéért, annak tagjaiért, teljesítményeikért, döntéseikért stb., mint hagyományos társa. A vezetői felelősség azonban nem csupán ennyiből áll, érdemes tehát közelebbről is szemügyre vennünk.

A VEZETŐK FELELŐSSÉGE

A vezető tehát felelős az egységéhez tartozó emberekért, teljesítményekért, döntésekért, de ez nem minden. A szervezet vezetése (vezetői, vezetési rendszere, vezetőfejlesztése stb. együttesen) felelős a szervezet problémáinak túlnyomó többségéért, sőt, akár a szervezet teljes kudarcáért is. A vezetés hibás működése okozza – közvetve vagy közvetlenül – a szervezeti problémák túlnyomó többségét. Ennek következménye és eredménye lehet ilyenkor akár a „vesztes"

szervezet megsemmisülése is, amikor a szervezetet a környezete az erőforrások megvonása útján felszámolja, esetleg egyes részeit – egységeit, készleteit, erőforrásait stb. – értékesítve vagy felhasználva.

Egy másik lehetőség, mely a szervezet azonban annak látszólagos fennmaradásával jár, a degradálódás, valamint és ennek folytatásaként a megcsonkoltatás. A szervezetet egy magasabb rendszer, a „győztes agresszor" szervezete teljesen vagy túlnyomórészt a maga felügyelete alá vonja, elvéve annak döntési jogosítványait (sőt sokszor a döntésben való tkp. mindenféle valós és hatós részvétel lehetőségét) a vesztes szervezettől, beillesztve azt a maga kiszolgáló alrendszerei közé, vagy akár beolvasztva valamely alrendszerébe.

A harmadik lehetőség a „relikvizálódás" – a szervezet a múlt emlékévé, valós és hatós társadalmi tevékenységet nem végző, legfeljebb ideológiai, hagyományőrző stb. szerepet vivő, de valódi, a nevesített eredeti (rendeltetési, működési) céljához kapcsolódó, társadalmilag valóban hasznos és előrevivő tevékenységre tkp. szinte teljesen alkalmatlan zárvánnyá válik. Az erőforrásokat azonban továbbra is fogyasztja, sőt nem egyszer aránytalan méretekben. Az ilyen szervezetmaradvány számos esetben a társadalmi erőforrásokat önnön fontosságának állandó bizonygatására atavizmussá korcsosul, mely egyes esetekben a szervezet egészére nézve kifejezetten ártalmas folyamatokat indít el.

Ez a felelősség természetesen csak akkor vállalható, ha a vezetőnek a meghatározó döntések meghozatalára joga és lehetősége van, vagyis szervezete „teljes", „egész", sőt „egészséges" szervezet.

Vezetéstudományi, szervezetelméleti szempontból a „teljes", „valódi", vagy másképp „érett", „felnőtt" szervezet az, amely *saját döntési hatáskörében képes tartani* az összes jelentős stratégiai és operatív működéséhez kapcsolódó folyamatot, akár maga végzi, akár mással végezteti azokat – vagyis tulajdonképpen ura a maga döntéseinek és saját jövőjének.

A vezető(k), a vezetés egyik feladata tehát a szervezet relatív függetlenségének, a szervezet „teljességének" védelme mindaddig, amíg a szervezet működési célját képező környezeti igény, társadalmi érdek vagy közérdek így hatékonyabban és eredményesebben elégíthető ki, mint másképp. Következésképp a vezető felelős szervezete értelmes és hasznos működése mellett annak jövőjéért is.

Az „érett, felnőtt" szervezet azonban „érett, felnőtt" munkatársakat igényel, vagyis szakmailag és emberileg egyaránt autonóm döntésekre és felelősségvállalásra hajlandó és képes, a maguk jövőjét alakítani – vagy legalábbis befolyásolni – tudó, egyéni és teammunkára egyaránt alkalmas, autonóm személyiségekre van szükség. A vezetői felelősség ezért kiterjed a munkatársak szakmai fejlődésének segítésére éppúgy, mint személyiségük alakítására. A személyiségfejlődés holtig tartó folyamat, márpedig állítólag többet tartózkodunk a munkahelyünkön, mint otthon, így szinte elengedhetetlen, hogy a munkahelyen a személyiségformálás maga is a vezetői figyelem körébe ne kerüljön.

KINEK ÉS MIBEN FELELŐS A VEZETŐ?

Első sorban a munkatársainak, beosztottjainak, a csapatának – hiszen ők a „legvédtelenebbek" vele és döntéseivel szemben. Másodsorban feletteseinek, illetve a szervezetnek, mellyel szemben szerződésileg is különböző kötelezettségeket vállalt. Harmadsorban mindenki másnak a szervezet releváns környezetében: az ügyfeleknek, a többi érdekeltnek és más érintetteknek, egyénileg és csoportosan; a családjának éppúgy, mint a mai társadalomnak és a jövő generációknak és ez nem csupán történelmi felelősség, hanem (legalábbis részben és névlegesen) pénzügyileg is kalkulálható. Végső soron pedig önmagának, a saját lelkiismeretének.

Ezek közül azonban, ha a szervezet modern humánpolitikát folytat, közvetlenül értékelni csak egy jóval szűkebb kör fogja a munkáját: a főnökei, a beosztottjai és önmaga. Az értékelés is három szempontot követhet, melyek híven tükrözik a vezetői felelősség három fő irányát [7]:

1. Hogyan és mennyiben teljesülnek a csoportja feladatai?
2. Mennyire és miért elégedettek vele munkatársai?
3. Hogyan és mennyire képes beilleszteni csoportját a szervezetbe?

Amennyiben a három szempont bármelyikével probléma van, a vezető segítségre szorul, melyet – elöljárói mellett – a humán erőforrás-menedzsment szervezeti szakértőitől kaphat meg. Az a vezető, aki jól kívánja végezni a munkáját, ezt nem csupán elfogadja, de – a modern vezetés történetének tanúsága szerint – maga is elemzően viszonyul saját munkájához és annak környezetéhez. A vezetéstudomány a 19. század utolsó és a 20. század első évtizedeiben azért jöhetett létre, mert a munkájukhoz alkotó módon hozzáálló személyiségek górcső alá vették és vehették maguk és társaik vezetői tevékenységét, hozzáállását, eredményességét. Nem csupán mintákat követtek, amikor a maguk közigazgatási, vállalati vagy katonai közegében kisebb-nagyobb szervezetcsoportokat, szervezeteket, szervezetrészeket irányítottak, hanem mintát adtak másoknak – tudatosan alakított, átgondolt mintákat, melyeket saját gyakorlati tapasztalataik próbáján megedzett elméleteik, ideológiájuk, racionális gondolkodásuk formált. Nem véletlen, hogy a vezetéstudományi kutatásmódszertan (*management research*) a világ vezető egyetemein a jelen és a jövő menedzsereinek képzésében jelentős szerepet játszik – részben, mert olyan hozzáállást közvetít és ismereteket ad át, melyek elengedhetetlenek nem csak a színvonalas egyetemi szakdolgozatok megszületéséhez, de a munkahelyen is: a szervezeti döntéselőkészítési folyamat egyes szakaszaiban résztvevők számára éppúgy, mint a vezetők egyéni döntéshozásában. A mélyben azonban ott van valami más, valami sokkal alapvetőbb: *az igazi vezetők elkötelezett érdeklődése saját maguk, beosztottjaik, szervezetük működése iránt*.

Felhasznált irodalom

[1] Marilyn M. Helms (szerk.): *Encyclopedia of Management* (Gale, 2009)

[2] Andrew J. DeBruin: *Essentials of Management* (Cengage, 2012) p. 2.

[3] Stephen P. Robbins és Mary Coulter: *Management* (Prentice Hall, 2012) p. 5.

[4] James L. Burrow, Brad Kleindl és Kenneth E. Everard: *Business Principles and Management* (Thomson South-Western, 2008) pp. 270f.

[5] Elton Mayo: *The Human Problems of an Industrial Civilization* (Macmillan, 1933); F. j. Roethlisberger és W. J. Dickson: *Management and the Worker* (Harvard University Press, 1939)

[6] Richard L. Daft: *Organization Theory and Design* (South-Western, 2010), pp. 450-489.

[7] Laurie Mullins: Management and Organisational Behaviour (Pitman, 1994) pp. 424-433.

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

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

A KÚTFÚRÁS TÖRTÉNETE, AZ ARTÉZI KUTAK MAGYARORSZÁGI HELYZETE

Absztrakt

A víz a földi élet nélkülözhetetlen eleme az élőlények számára. Ez a felismerés egyidős az emberiséggel. A történelem folyamán az ember megtanulta a vizet saját céljainak megfelelően hasznosítani, mely folyamat során annak szennyezése is megtörtént, melyet saját eszközeivel később megpróbált helyrehozni, védeni. A mindennapi élethez ivóvízre, ivóvízkészletekre volt szüksége, melynek tisztaságához nem fért kétség. Sokáig a felszín feletti vizeket hasznosította, majd később rájött, hogy a felszín alatti vizek minősége sokkal jobb, biztonságosabb. Ivóvíz kutakat hoztak létre, amelyek kezdetlegesek voltak, majd a történelem folyamán korszerűsödtek. Hazánkban az első fúrt kút a 19. század elején készült. Cikkemmel a kútfúrás történetét mutatom be, valamint a hazai szabályozási rendszerre szeretnék rávilágítani.

The water is the indispensable element of the eartly life for the living beings. This recognition is of the same age with the humanity. The man, which is its pollution in the course of a process, learned to utilize the water according to his own aims during the history occurred, which one his own devices later tried to put right, to save. To the everyday life he needed a drinking water, drinking water sources. Utilized the waters above the surface for a long time, realised that the quality of the waters under the surface is right, safer one with a shock later then. Drinking water good, which were crude, were created, they got modernized during the history then. In our country, the first wells drilled in the early 19th century. Part view of the history of drilling are presented, and I would like to highlight the domestic regulatory system.

Kulcsszavak: *víz, vízvédelem, ivóvízkészlet, kutak ~ water, water protection, drinking water source, wells*

BEVEZETÉS

Napjainkban - a növekvő vízárak hatására - egyre inkább alternatív vízforrásokból igyekeznek megoldani a háztartások ivóvízellátását, illetve a kertek, mezőgazdasági területek öntözését. Erre a célra a legelterjedtebb megoldás a kút. A háztartásokban a sok évvel ezelőtt készített kutakat újítják fel, vagy új kutakat létesítenek. A magas beruházási költség néhány éven belül megtérül, emellett említést érdemel, hogy a kút vízminősége, illetve oldott ásványi anyag tartalma a növényekre nagyon jó hatással van. A kút létesítés a figyelem középpontjába került, mivel számuk napjainkban egyre nő.

A víz minőségének követelményeit törvények szabályozzák, amelyeket kutak létesítésénél figyelembe kell venni.

„Az ivóvíz megfelelő minőségének biztosítása érdekében EU Parlament és a Tanács 98/83/EK irányelve szükségesnek tartja a megfelelő vízvédelmi intézkedések foganatosítását a felszíni és felszín alatti vizek vonatkozásában. Ezek némelyike közvetlenül kapcsolódik a vízszolgáltatáshoz, ugyanakkor látókörbe kerülnek olyan, a vízellátás hosszú távú környezetbiztonsági kockázatai csökkentését és a vízbázisok védelmét célzó határozatok, mint például a vizek mezőgazdasági eredetű nitrát-szennyezéssel szembeni védelméről szóló 91/676/EGK, melynek érvényesítése a szennyezés kockázatával járó tevékenység korlátozásával járul hozzá a vízvédelemhez. 2012 decemberében az Országgyűlés elfogadta a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló (2012. évi CLXVI.) törvényt, melynek 1. sz. melléklete szintén kitér a víz alágazatra az alábbi illusztráció szerinti felosztásban. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény rendelkezése szerint a Kormánynak évente jelentést kell benyújtania az Európai Bizottságnak, melynek tartalmaznia kell egyrészt azon létfontosságú rendszerelemek ágazatonkénti számát, melyek európai létfontosságú rendszerelemnek kijelöltek, másrészt az Európai Unió azon tagállamainak számát, amelyek az európai létfontosságú rendszerelemektől függenek. „ [1]

1. ábra. A víz, mint kritikus infrastruktúra ágazat és alágazatai
(forrás: 2012. évi CLXVI. tv.a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről 1.sz. melléklete alapján szerk.:Berek)

KUTAK TIPÚSAI

A kutak a felszín alatti vizeket hasznosítják. A felszín alatti vizeket mélységbeli elhelyezkedésük alapján osztályozzuk:

- a legfelső vízzáró réteg felett elhelyezkedő, a talajszemcsék közötti hézagokat csak részben kitöltő vizet talajnedvességnek
- a szintén a legfelső vízzáró réteg felett elhelyezkedő, de a talajszemcsék közötti hézagokat teljesen kitöltő vizet talajvíznek
- a két vízzáró réteg közrefogta vizet rétegvíznek
- a kőzethasadékaiban, repedéseiben elhelyezkedő vizet résvíznek nevezzük.

A kút vízellátás céljából készített építmény. A kutaknak két típusát különböztetünk meg, aszerint, hogy honnan használja fel a vizet a közeli talajvízből, vagy a mélyebb rétegekből, illetve mélységük alapján. Eszerint a kutak lehetnek sekélyek (50 m-nél kisebb mélységű), kis mélységűek (50-200 m mélyek), közepes mélységűek (200-500 m mélyek) és mély kutak (500 m mélyebbek).

Szerkezetét tekintve minden kút három fő részből áll. Az első maga a kút, amely összegyűjti a vizet a felszín alatti rétegből. A második a kútfejkiképzés, amely véd a szennyeződéstől, illetve tartja a vízkitermelő eszközöket. A harmadik a vízkitermelő eszköz, amellyel a kútból a vizet kivesszük. [2]

Mélységi kutak

A mélységi kutak rétegvizet használnak fel, ezek adják a legjobb minőségű vizet. A rétegvíz kétféleképpen kerülhet a felszínre. Természetes úton forrásként, vagy mesterségesen az ember által kút segítségével. A rétegvíz egy része a felszínről szivárog be a vízzáró rétegek közé, a másik része még sosem volt a felszínen. Utóbbi víz a juvenális (fiatal) víz. A nagy mélységből származó rétegvíz tiszta, fogyasztásra alkalmas.

A rétegvíz fajtái:

- *Ásványvizek:* A legalább 1 g/l oldott ásványi anyag tartalommal rendelkező természetes vizek. Ide tartoznak az 1 g/l-nél kevesebb oldott ásványi anyagtartalommal rendelkező természetes vizek is, ha egy-egy elem (pl. jód, bróm, nátrium, magnézium, lítium stb.) tekintetében határértéket meghaladó mennyiséget tartalmaznak. Kereskedelmi forgalomban a 0,5 g/l határértékkel rendelkező ivóvizeket nevezik ásványvíznek (pl. Theodora – Kékkúti).
- *Gyógyvíz:* Olyan víz, amely gyógyításra alkalmas ásványi anyagokat tartalmaz. Rendszerint egy uralkodó ásványfajtával jellemezhető, aszerint osztályozható. Budapesti gyógyvizeink: Gellért fürdő, Rudas fürdő, Rác fürdő. Vidéken: Hajdúszoboszló, Hévíz, Harkány, Szeged stb.
- *Hévíz:* Minél mélyebbről erednek, annál melegebbek, annál magasabb az ásványi anyag tartalmuk. Ha az ásványi anyag tartalmának töménysége határfeletti értéket mutat, akkor az adott víz gyógyhatású is.
- *Résvíz:* A szilárd kőzetek repedéseiben, hasadékaiban, illetve réseiben mozgó víz. Speciális esete a mészkövekben előforduló karsztvíz.
- *Artézi kút:* Az artézi kút olyan nyomás alatti rétegvizet megcsapoló kút, ahol a nyugalmi vízszint a víztartó réteg fedőjénél magasabban húzódik, így a víz magától feltör, akár a felszín fölé is, vagyis pozitív nyugalmi vízszintű kút.

Hazánk ivóvíz forrásának második legnagyobb arányban felhasznált vize a mélységi rétegvíz. Ezt mennyiségileg csak a parti szűrésű vizek haladják meg.

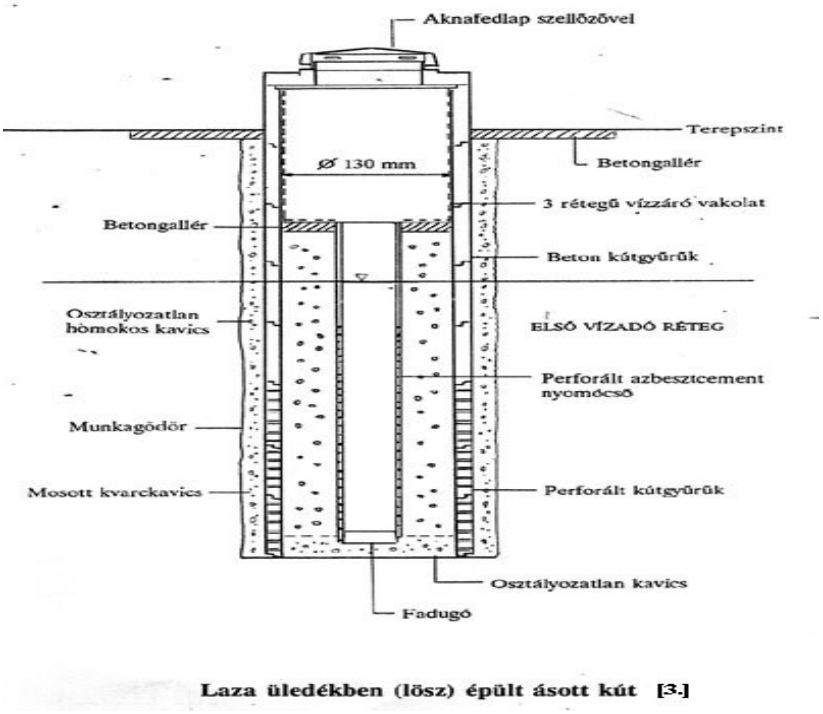
2. ábra. Magyarország ivóvíz forrásának százalékos elosztása
Forrás: http://vizmegoldas.hu/vizszures/ivoviz-kerdes-hazankban/ letöltés:2014. február 15.

A mélységi kutak, mint már említettem rétegvizet használnak fel, azonban léteznek még a talajvíz gyűjtésére készített kutak is. Ezen kutak vízminősége sokkal gyengébb, mint a mélységi kutaké, ezért is használják általában locsolásra, állatok itatására, illetve egyéb felhasználásra.

Az alábbiakban rövid ismertetés ezekről a kutakról a teljesség igénye nélkül.

A talajvíz gyűjtésére készített kutak

Az ilyen építményekre jellemző, hogy ivóvíz fogyasztására csak abban az esetben lehet felhasználni, ha elég mélyen található, megfelelő a talaj szűrőképessége és megvan a megfelelő áramlás. Ugyanis a víz, akkor cserélődik, ha állandó mozgásban van. Az ilyen kutak sok esetben csak állatok itatására vagy öntözésre használható.



3. ábra.
Forrás: http://fenntarthato.hu/epites/leirasok/epulet/vizgazdalkodas/vizellatas/kuttipusok-rajzokkal
Letöltés: 2014. március 08.

Sírkutak

A legegyszerűbb kutak. Alakjuk sírgödörhöz hasonlít, innen kapták nevüket. Egyszerű kiásással, vagy döngöléssel készül olyan helyen, ahol 2-3 méter mélységben vízadó réteg helyezkedik el.

Aknás kút

Ez egy ásott kút, melyet téglával vagy betongyűrűvel raknak ki. Két fajtáját különböztetünk meg: lebegő kút, vagy teljes kút.

Lebegő kútról beszélünk, ha a talajvízszint után még 2-3 méter mélyen tovább ásnak a vízszigetelő agyagréteg elérése nélkül.

Teljes kútról beszélünk, ha a talajvízszint után még 2-3 méter mélyen tovább ásnak a vízszigetelő agyagréteget elérve. A teljes kút falazata vízáteresztő, a legfelső betongyűrű a talaj szintjétől számítva 30 cm-rel magasabban van, felső, másfél méteres részét agyaggal döngölik be a szennyező anyagok bekerülése végett. A szennyező forrásoktól 20 méterre kell, hogy épüljön. Időnként tisztítani szükséges.

Csápos kút

Az ipari termelésben használják nagy hozamuk miatt. A furaton keresztül egy acélcsövet sajtolnak kifelé, miután megfúrják az akna falát a vízszűrő réteg magasságában. Ha a sajtoló eléri az akna falát hegesztéssel újabb csöveket helyeznek az előzőre és ez így folytatódik. Az így készített csáp több méter hosszú is lehet. A csápot a folyamat végén szigetelik.

Vert kút

A talajvíz szintjéig levernek egy perforált vascsövet. A vascső lyukain befolyik a víz, amit ki lehet termelni. Az így nyert vízhozam igen alacsony, hátránya, hogy nem tisztítható. A szennyeződés kizárása mellett alkalmazható megoldás.

A KUTAK LÉTESÍTÉSE

A vezetékes vízhálózat terjedésével nem tűntek el a fúrt kutak. Gazdaságossági szempontból az utóbbi időben számuk egyre nőtt. Egyre több család vállalja az igen drága, egyszeri beüzemelési és engedélyeztetési költséget. Az egyszeri befektetési díj hamar megtérül, mellőzve az igen magas víz- és csatorna használati díjat. Így lehetőség nyílik a családoknak arra, hogy magukat, háztartásukat és kertjüket vízzel tudják ellátni.

Kútfúráshoz Magyarországon hatósági engedély szükséges. Saját részre, 500 m3/év talajvíz vételezéséhez az önkormányzattól kell beszerezni a vízjogi engedélyt. Az engedély feltétele, hogy a vízhasználat a kérelmező háztartása szükségleteit, vagy egyéb tevékenységét szolgálja kielégíteni. Más felszín alatti víz (rétegvíz, karsztvíz, parti szűrésű víz) igénybevételéhez a Zöldhatósághoz kell fordulni.

Miután eldöntöttük, hogy a kitermelt vizet milyen célra szeretnénk használni szakemberrel meg kell vizsgáltatnunk a talajt, illetve a vízadó réteg szemcseszerkezetét minőségi szempontból. Mi magunk soha ne próbálkozzunk a kútfúrással, mert az nagy szakértelmet igénylő munka, még akkor is, ha kutunk talajvizet hasznosít. Artézi kút készítése során pedig nagy mélységbe kell fúrni, ami nem csak nagyobb szaktudást, de több munkagépet, magasabb műszaki követelményeket is igényel. Ezért elkészítése jóval költségesebb, mint egy talajvíz gyűjtésére alkalmas kúté.

A kútfúró elkészíti a kivitelezési lapot, amely a kút dokumentációja, minden adat részletesen fel van rajta tüntetve. A szakember, ezáltal felelősséget és garanciát is vállal munkájáért. Minden esetben célszerű ellenőrizni, hogy szakemberünk rendelkezik-e a megfelelő szakképesítéssel.

A fúrást követően a kút beüzemelése történik, az-az a tisztító, majd a próbaszivattyúzás. A próbaszivattyúzás során növelik a víz mennyiségét odáig, amíg homokolást nem tapasztalnak.

A homokolási határt soha nem szabad túllépni, mert akkor a kút körüli talajszemcsék megmozdulhatnak és a vízszűrő réteget eltömítheti. A kút kivitelezési lapján a homokolási határ térfogatáramának (időegység alatt kivett víztérfogat) szerepelnie kell. Meg kell még határozni

a nyugalmi és az üzemi vízszintet is. A nyugalmi vízszint az az állapot, amikor nem történik vízkivétel a kútból. Az üzemi vízszint vízkivételt követő vízszint a kútban. Ez az adat határozza meg, hogy a kútban milyen szivattyút kell elhelyezni. Ha az üzemi vízszint mélyebben van 8 méter mélységnél, akkor csak búvárszivattyút, ha 8 méternél magasabban van, akkor szárazbeépítésű szivattyút kell elhelyezni a kútban. Szivattyút ennek az értéknek a megállapításakor célszerű beszerezni. A nyugalmi vízszintet szintén fel kell tüntetni a kivitelezési lapon.

Az utolsó állomás a kút kitisztítása, illetve a természetes szűrőváz kialakítása. Kis vízhozammal elkezdjük kitermelni a vizet, majd amikor tiszta a víz és beállt az üzemi vízszint, akkor növeljük a vízhozamot, amíg el nem éri a kívánt vízhozam másfélszeresét. Eközben méréseket végzünk, figyeljük a vízhozamot és a kút vízszintjét. Ezek az adatok az engedély megadásához szükségesek.

A kút létesítés folyamatának lezárását követően el kell végeztetni a vízminőség vizsgálatát. Ekkor határozzák meg, hogy a kitermelt vizet milyen célra lehet használni. A vizsgálatot a területileg illetékes ÁNTSZ végzi.

Az ivóvíz minősítése fizikai, kémiai, bakteriológiai, hidrobiológiai, toxikológiai és radiológiai jellemzői alapján történik. Alapvető követelmény az ivóvízzel szemben, hogy ne tartalmazzon az emberre ártalmas élő- és élettelen anyagokat, feleljen meg a fogyasztók esztétikai igényeinek, sőt biztosítsa az emberi élethez szükséges mikro- és makro elemek felvételét és a só utánpótlást is. 201/2001. (X. 25.) Korm. rendelet az ivóvíz minőségi követelményeiről és az ellenőrzés rendjéről tartalmazza az erre vonatkozó szabályokat. [3]

Az engedélyezéshez és a kútfúráshoz az alábbi szabályozások a követendők:

- 72/1996. (V. 22.) Korm. rendelet a vízgazdálkodási hatósági jogkör gyakorlásáról [4]
- 18/1996. (VI. 13.) KHVM rendelet a vízjogi engedélyezési eljáráshoz szükséges kérelemről és mellékleteiről [5]
- 101/2007. (XII. 23.) KvVM rendelet a felszín alatti vízkészletekbe történő beavatkozás és a vízkútfúrás szakmai követelményeiről [6]

ARTÉZI KUTAKRÓL RÖVIDEN

Az artézi kút nyomás alatti, rétegvizet megcsapoló kút, ahol a nyugalmi vízszint a víztartó réteg fedőjénél magasabban húzódik, így a víz magától feltör, akár a felszín fölé is. Magyarország vízellátásában a felszín alatti vizeknek kiemelkedő szerepe van. Sérülékenysége alapvetően a víztartó tulajdonságaitól és mélységétől függ. Hazánk legjelentősebb ivóvízbázisát a rétegvizek jelentik, amelyek hasznosítását azok fizikai-kémiai jellemző határozzák meg.

Kútfúrással először Kínában és Líbiában próbálkoztak. Európa első kútját Franciaországban fúrták az Artois-i Grófság területén 1126-ban. Innentől kezdve minden fúrt kút az artézi nevet kapta a gróf tiszteletére.

Hazánkban az artézi kutak fúrása, létrejötte és annak elterjedése Zsigmondy Vilmos nevéhez fűződik (Pozsony, 1821. május 15. – Budapest, 1888. december 21.). 1867-ben építette meg a Margit-szigeten lévő kutakat. Kiváló bányamérnökként vizsgálatokat végzett a talaj, illetve a víz összetételére vonatkozóan. Egy év elteltével készítette el a világ legmélyebb artézi kútját a városligeti I. számú kutat. Nagyságát, mérnöki szaktudását számos kút fémjelzi.

Elméleteit rendszerezte, ahol leírta hogyan lehet a hőforrásokat feltárni, hasznosítani, biztonságos kutakat létrehozni.[7] Felismerték azonban, hogy az ásott kutak vize egészségtelen, sokszor ihatatlan. A víz szennyezettsége adódhatott a kút nem megfelelő mélységéből, a talaj szennyeződésétől, amely eső alkalmával a kútba szivárgott. A vizek minősítése sem volt még ekkor megfelelő. Mindezek mellett és figyelembe vételével megszületett a gondolat az artézi kutak törvényi szabályozására.

Az ő tevékenységét folytatta méltó utódként unokaöccse Zsigmondy Béla (Pest, 1848. március 7. – Budapest, 1916. június 12.) magyar gépészmérnök, hídépítő. Számos artézi kút készítése fűződik a nevéhez az Alföldön. Nagy szaktekintély a mélyfúrási technika terén. [8]

Miután 1883-84. évben megfúrta az Alföldön, Hódmezővásárhelyen az első kiváló vizet adó artézi kutat, megnőtt népszerűsége, egyre többen keresték fel messze vidékekről kútfúrás miatt. Ezek után gombamód jöttek létre artézi kutak az Alföldön és hazánk más tájain. Sajnos foglalkoztak a kútfúrással hozzá nem értő emberek is, ezért előfordult, hogy eredménytelen volt a kútfúrás, vagy a kút vizét vesztette. A leggyakrabban előforduló hiba, hogy szorosan egymás szomszédságában fúrtak kutakat, amelyek a hidrosztatikai nyomás csökkenéséhez vezettek, így a vizük kevésbé ömlött ki, illetve elapadt, vagy csak szivattyúzással lehetett vizet nyerni belőlük.

Zsigmondy Vilmos és unokaöccse Zsigmondy Béla geológiai vizsgálataik eredményeit és fúrásaik alkalmával szerzett tapasztalataikat összegyűjtötték, feldolgoztatták, hogy az utókor megismerhesse hazánk földtani viszonyait. Az általuk összegyűjtött anyagot a magyar királyi földtani intézetnek ajándékozták. [9]

Táblázatot készítettek a kutak területi eloszlásáról, a fúrások számáról és annak eredményességéről évek szerinti bontásban is. Munkásságuk eredményeként jöttek létre számos díszkutak hazánkban. [10]

Hazánkban a legtöbb artézi kút az Alföldön található jelentős számban. Az általuk kitermelt víztömeg majdnem azonos a Balaton víztömegével. A kisebb mélységű (100 méter körüli) kutak ivóvizet szolgáltatnak. Kiemelkedő a hajdúszoboszlói gyógyfürdőt támogató kút, amely 2000 méter mélyről tör fel. Legnevezetesebb artézi kutjaink Alcsúton, a Margit-szigeten, Komáromban illetve alföldi városokban találhatók.

ÖSSZEGZÉS

A víz, az egyik legnagyobb érték. Alapvetően meghatározza a növénytársulásokat, arra is hatással van, milyen állatfajok élnek egy területen. Elődeink a települések helyét vízpart, források, természetes átkelők mentén hozták létre. Nélkülözhetetlen a mezőgazdaság és az ipar számára, ugyanúgy, mint a háztartások számára.

A felszín alatti vízkészlet a teljes földi vízmennyiség 16%-t képezi, a vízkörforgás tartalékai, a mezőgazdaság számára rendkívül fontos, az ivóvízellátásban növekvő szerepet képvisel.

Az artézi vizek jelentőségét egyrészt a tárolt vízkészlet nagysága, másrészt - nagyobb mélységük és a felszínnel való lazább kapcsolatuk révén - a felszíni szennyező hatásoktól való védettsége, tisztasága adhatja.

A víz mennyisége, eloszlása a világon különböző. Vannak országok, akiknek vízkészlete kisebb, mint amennyire épp szüksége van, de vannak olyanok is, akik komoly vízkészlettel rendelkeznek, mint hazánk is. Méltán nevezik hazánkat a vizek országának. Vízkészletünk 96%-a külföldről érkezik. Így a vízkészlet és vízszennyezés szempontjából a magasabban fekvő országok tevékenységétől függünk. Az Alföld felszín alatti vízkészlete értékes ásványi kincs, kitermelhető mennyisége azonban az utánpótlódás mellett sem korlátlan. Ezzel a természeti erőforrással korábban nem gazdálkodtunk okosan.

Készleteinek védelme, a magyar állam tulajdonában tartása, gazdaságos használata, minőségének megőrzése, néhány esetben annak javítása nemzeti érdek. Jövőnk egyik kulcsa a vízkészletek védelme és a fenntartható vízgazdálkodás.

Felhasznált irodalom:

[1] Berek Tamás - Rácz László István: Vízbázis mint nemzeti létfontosságú rendszerelem védelme Hadmérnök VIII. Évfolyam 2. szám - 2013. június ISSN1788-1919 http://www.hadmernok.hu/132_11_berekt_rli.pdf

[2] Dr. Léczfalvy Sándor: Kútépítés, Műszaki Könyvkiadó, Budapest 1971, p.10-11.

[3] 201/2001. (X. 25.) Korm. rendelet az ivóvíz minőségi követelményeiről és az ellenőrzés rendjéről

[4] 72/1996. (V. 22.) Korm. rendelet a vízgazdálkodási hatósági jogkör gyakorlásáról

[5] 18/1996. (VI. 13.) KHVM rendelet a vízjogi engedélyezési eljáráshoz szükséges kérelemről és mellékleteiről

[6] 101/2007. (XII. 23.) KvVM rendelet a felszín alatti vízkészletekbe történő beavatkozás és a vízkútfúrás szakmai követelményeiről

[7] Jószerencsét!
http://www.joszerencset.hu/eletrajz/zsigmondy.htm, letöltés 2014. március 08.

[8] Magyar Elektronikus Könyvtár
http://mek.oszk.hu/00300/00355/html/ABC17155/17393.htm, letöltés 2014. március 08.

[9] Elektronikus Periodika Adatbázis Archivum
http://epa.oszk.hu/02100/02181/00323/pdf/EPA02181_Termeszettudomanyi_kozlony 1896_366-374.pdf, letöltés 2014. március 10.

[10] Csath Béla: A Zsigmondyak szerepe a magyar vízkutatás és fúrás történetében, Budapest, Vízdok 1983

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Tóth Eszter
sztr.tth@gmail.com

NŐK AZ ŰRBEN
NŐK SZEREPE A HOSSZÚ TÁVÚ ŰRREPÜLÉSBEN

Absztrakt

Korunk űrkutatásának egyik legnagyobb kihívása a Mars utazás. Egy ilyen utazás kapcsán azonban számos kérdés merül fel, ami megválaszolásra vár. Kik menjenek először? Robotokat vagy embereket küldjenek? Milyen összetételű legyen a csapat? Nők, férfiak vegyesen? Egyedülállók, vagy párok? Legyen teljesen homogén a csoport, csak férfiak, esetleg csak nők? Férfi vagy női vezetője legyen egy ilyen missziónak? Hány fős legyen a legénység? Nemzetközi csapat legyen, vagy egy nemzet adja a misszió tagjait? A cikk során szeretném áttekinteni, hogy a NASA hogyan választotta ki a korábbiakban az űrhajósait. Emellett áttekintem, hogy milyen problémák adódhatnak a legénység összeállítása során, hogyan lehet megelőzni ezeket a problémákat. Legvégül szeretnék arra kitérni, hogy a nőknek milyen szerepük volt az űrhajózásban napjainkig, és milyen szerepük lehet egy Mars utazásban.

On of the greatest challenges of today's space research is the travel of to Mars. However there are several points to agree on regarding to this mission such as would they send robots or human first? Besides the nature of the trip they have decide who they want in the research team: whether they want a homogenous or mixed team (gender, marital, status etc)., if they want a female or male leader. There is also the issue of the number of the team members and wheter they want an international team or they will choose the members from one nation. In this article I would like to give a review of the NASA's recruiting-methods. I also would like to summarize, what sort of the problems usually occur during the selection of astronauts, and how could these problems be prevented. Finally I would like to mention the most important details about the role of women in the history of spaceflight from the beginning until today, and I would also like to describe what role they could play in a Mars-expedition.

Kulcsszavak: *hosszú távú űrrepülés, NASA, kiválasztás, csoportproblémák, nők az űrrepülésben ~ long-term spaceflight, NASA, selection and recrutiment, team-problems, women in spaceflight*

A NASA KIVÁLASZTÁSI RENDSZERE

A NASA űrhajós szelekciója egyidős az űrrepülés kezdetével. A Mercury idején két pszichiáter 30 órát töltött el minden egyes jelölttel. Ez az Apolló program idejében 10 órára, az űrkomp személyzetének kiválasztásakor 3 órára csökkent. A kiválasztás során alkalmazott tesztek 25-ről 10-re csökkentek, majd teljesen el is tűntek. Az „alkalmassági kritériumok" esetében nagyobb hangsúlyt kapott az érzelmi stabilitás, az önismeret és a társas kapcsolatok minősége. Az évek és a tapasztalatok alapján azonban érdekes dologra figyeltek fel a szakemberek a tesztek érvényességével kapcsolatban. Nem találtak összefüggést a különböző teszteken elért eredmények és a későbbi teljesítmény között [1], azaz a vizsgálatok nem jósolták be megbízhatóan a későbbi teljesítményt. Ez volt az egyik ok, amiért változtattak a különböző alkalmassági kritériumokon. A kiválasztási rendszer megváltoztatásának másik oka az lehetett, hogy feldolgozásra kerültek az addigi repülések tapasztalatai.

A kiválasztási rendszer evolúciójában a következő lépcsőfok annak felismerése volt, hogy a nem alkalmatlan nem egyenlő azzal, hogy valaki alkalmas űrhajósnak. Kezdetekben - amikor berepülő pilótákból kerültek ki a legénység tagjai - az űrprogramba való bekerülés feltétele a kötelező repült óraszám mennyisége volt. Amikortól kutatók és tudósok is bekerülhettek az űrhajósok közé, ez a kritérium már nem volt elegendő. Ekkor kezdték elkülöníteni az alkalmasságot az alkalmatlanságtól.

A kiválasztás első foka innentől kezdve az alkalmatlanság vizsgálata és annak kiszűrése volt. Ez a vizsgálat a klinikai pszichológia kompetencia körébe tartozik melynek során mentális betegségeket, patológiás eltéréseket, illetve további eleve kizáró okokat keresnek. (Ilyen például Magyarországon az ejtőernyős jelöltek esetében a gerincröntgen. Amennyiben a vizsgálat során találnak eltérést, akkor a jelölt nem folytathatja a szűrési folyamatot.) Abban az esetben, ha itt megfelelt az űrhajós jelölt, még nem mondható rá, hogy alkalmas, csupán az, hogy nem alkalmatlan. A következő vizsgálatnál már azt nézik, hogy vannak-e a jelöltnek olyan képességei, kompetenciái, amelyek szükségesek az ő - legalább megfelelő szintű - munkavégzéséhez, beváláshoz. A kiválasztásnak ez a szintje a munkapszichológia körébe tartozik.

Az egyes személyek kiválasztása során a szakemberek a legjobb pszichológiai profilú embert keresik, akinek a képességei megfelelőek és képesek csapatban dolgozni. [2] Egyszerűen hangzik, de figyelembe kell venni azt, hogy ezek a kiválóságok csapatban fognak dolgozni, együtt kell működniük, élniük extrém körülmények között és pont az együttműködés a kulcs egy ilyen misszió sikeres elvégzéséhez. A következő részben azt tekintem át, hogy milyen problémái lehetnek a legénység összeállításának.

Csoport összeállítása

Több probléma adódhat a legénység összeállítása során. Az első és legfontosabb a csoport heterogenitása lehet. Heterogén lehet egy csoport életrajzi (nem, életkor, szocioökonómiai státusz, kulturális háttér) és képességbeli különbségek szempontjából. Ezek az eltérések komoly problémákat tudnak okozni.[3] Erre példa egy amerikai űrhajós esete, akit az orosz kollégái "vendégként" kezelték az űrállomáson, komoly munkát nem végezhetett, evésnél elkülönültek tőle, valamint egymás közt oroszul beszéltek, amiből az amerikai kolléga nem értett semmit. [4] De ezt támasztja alá a különböző nemzeti karakterisztikák, kultúrák hozzáállása a feladatokhoz (német precizitás szemben a latin lazasággal). Ugyanakkor megfigyelték, hogy a koedukált csoportok alkalmazkodóbbak, az egynemű csoportok inkább feladat orientáltak, versengők. [5] Egy olyan helyzetben, amikor a hangsúly a hosszú távú együttélésen van, szinte biztos, hogy fontosabb az alkalmazkodás, mint a versengés.

További nehézség a csoport koherenciájának a változása, a nyelvi problémák.[3] A Shuttle/Mir program egyik tanulsága az volt, hogy a megfelelő nyelvi, kulturális felkészítés

nélkül az űrhajósok negatív érzelmekről számoltak be. Az űrhajósok nehezen – vagy egyáltalán nem - tudtak beilleszkedni a nemzetközi környezetbe, nem élték meg magukat hatékonynak mivel nem értették a nyelvet és a munkatársaik is úgy kezelték, mintha "vendég lett volna" az űrállomáson. Ez a probléma mind amerikai, mind pedig az orosz fél részéről megjelent. [4] A csoport mérete is okozhat problémákat: a kis csoport homogénebb, ugyanakkor egy nagyobb 5-6 fős csoportban már alakulhatnak ki barátságok, melyek coping mechanizmusként működhetnek és segíthetik a stresszel való megküzdést.

Egy csoportban kulcsszerepe van a csoport vezetőjének és annak, hogy milyen vezetői stílust alkalmaz. Az Antarktiszon zajló vizsgálatokból kiderült, hogy a jó vezető tudja, milyen helyzetben milyen vezetői stílust kell alkalmaznia. Ő az, aki szervez, irányít és koordinálja a csoportot. Segíti a csoport harmonikus működését, kibékíti az aktuálisan konfliktusban lévő munkatársakat (igazságot tesz), meghatározza a célokat, tartja a kapcsolatot a külvilággal: ő közvetíti az igényeket mindkét irányba. A legjobb, ha a vezető saját maga választja ki a csoportot, akivel együtt kíván dolgozni. Fontos, hogy végig ott legyen a felkészülés során és pontosan ismerje a csapattagok közötti viszonyokat. [1]

További nehézséget jelent a szervezeti kultúrák eltéréseiből adódó különbség. Gondoljunk csak az orosz amerikai különbségekre, az eltérő vezetési stílusukra, az űrhajósaikra nehezedő nyomásra, a parancsadási rendszerre. [6] Korábban volt szó arról, hogy kezdetekben csak pilóták lehettek űrhajósok, de ez megváltozott, ma már civilek is bekerülhetnek az űrhajós programba. Ez kihívás volt az űrprogram számára, mivel a kutatók nem katonai környezetből jönnek, ők a civil közegben szocializálódtak. Ebből adódik, hogy fontos számukra az autonómia, és nehézségeik adódhatnak egy hierarchikus parancsuralmi rendszerben. Ezzel szemben a pilóták-, akik katonai közegben szocializálódtak- "nem értik" a tudósokat, és a jól felépített parancsrendszert preferálják [1]. További érdekes probléma a földi irányítás és a legénység közötti kapcsolat. A földi irányítás az egyik fontos kapocs a külvilág, a Föld felé az űrhajósoknak. Megfigyelték, hogy a két csoport közötti kapcsolat korántsem problémamentes, indulatáttétel, érzelemáttétel jelenik meg a kommunikáció során az űrhajósok részéről.[7]

Nehézségek kezelése

Ezeket a nehézségeket nem lehetetlen kiküszöbölni. Első lépésben hasznos lenne, hogy a tervezett legénység által kitöltött személyiség tesztek profiljait összevessék. Bebizonyosodott, hogy hasonló a hasonlóval jobban együtt tud dolgozni, könnyebben össze tudnak szokni és ezáltal a konfliktusok is kisebb valószínűséggel alakulnak ki. Az ilyen módon összeállított legénységet tréningnek, szimulációnak lehetne alávetni, ezáltal növelni a csoport hatékonyságát. Például a Nemzetközi Űrállomáson hosszabb-rövidebb ideig lehetnének együtt annak érdekében, hogy kiderüljön milyen problémák léphetnek fel a későbbiekben. Továbbá a közös munka segíthet leküzdeni a különböző (nemi, kulturális) sztereotípiákat. [5] A nyelvi különbségek kiküszöbölésére fontos lenne a nyelvi felkészítés biztosítása. (Bár ez a korábbiakban nem volt sikeres, de a tapasztalatok levonása után lehetne rajta fejleszteni.)

Amennyiben a tréning, szimuláció közben kiderül, hogy a csoport tagjai nem tudnak együttműködni, akkor lehet variálni a csapattagokat, annak érdekében, hogy megtalálják az ideális csoport összetételét.

Fontos, hogy a legénység és a földi központ személyzetének felkészítése együttesen történjen. Hatékony lehet egy pszichológiai felkészítés is, ami a különböző pszichoszociális kérdésekben nyújt eligazítást, például: vezetői szerep, kulturális különbségek, a legénység és a földi irányítás közötti nehézségek. Egy informális csapatépítés is segítheti a felkészítést. Valamint lehetne tanítani a jelölteknek autogén tréninget, relaxációt, meditációs technikákat annak érdekében, hogy javuljon az alváshigiéné, csökkenjen a felhasznált gyógyszermennyiség, javuljon a koncentrációs készség, könnyebben kezeljék a konfliktusokat. [8]

A NŐK SZEREPE AZ ŰRREPÜLÉSBEN

Hivatalos űrprogramok keretében eddig 57 nő vett részt űrrepülésben, ebből 45 amerikai. Az első nő Valentyina Tyereskova 1963 júniusában repült.[9] Érdekesség, hogy az ő repülése után 19 évig nem járt nő az űrben. A női űrhajósok részaránya 2013 végéig, 10, 6% a férfiakhoz viszonyítva.[10] A NASA a legkorábbi időszaktól kezdődően tervezte, hogy nőket küld az űrbe. Az első női űrhajósjelöltek a Mercury idejében készültek fel. Ők végül nem repülhettek, mivel az akkori hozzáállás szerint, a nők "szerepüknél fogva nem tudták volna hitelesen képviselni az űrben az amerikai nemzetet".[11] A férfiak és nők közötti különbségeknek evolúciós, történelmi és kultúrtörténeti okai vannak. Néhány példa abból, hogy melyik nem miben erősebb: a férfiaknak jobb a térérzékelő képessége, magabiztosabbak, erősebb bennük a küzdőszellem, agresszivitás jellemzi őket és fontos számukra az előrejutás. A nőknek kifinomultabbak az érzékeik, pontosabban tudják értelmezni a metakommunikációs jeleket, erősebbek a nyelvi készségeik –jobban ki tudják fejezni magukat-, hamarabb kiismerik magukat a társas, személyes viszonyokban, gyorsabban dolgozzák fel az információkat, rugalmasabbak.[12]A nők alapvetően kitartóbbak, szorgalmasabbak, gyorsabban tudják a külvilág jeleit érzékelni, nyitottabbak a tudásmegosztásra, másokra jobban odafigyelnek, színvonalasabb munkát képesek végezni, több új ötletük van- amiket meg is valósítanak-, képesek az együttműködésre, jól tudnak csapatban dolgozni, munkájukban eredményesek. [13]

Képességeik tekintetében bebizonyították, hogy ők is megállják a helyüket férfias helyzetekben. A fentebb említett női űrhajós csoport bizonyos helyzetekben jobban teljesített mint férfi kollégáik. Antarktiszi expedíciók beszámolójából kiderül, hogy a férfi kollégák elfogadták női munkatársaikat, elismeréssel nyilatkoztak munkájukról. (Ez természetesen egyénfüggő is.) [14]

Ugyanakkor a nők részvétele egy Mars expedícióban erősen megosztja a szakértőket. Mellettük és ellenük is vannak érvek, tapasztalatok. Mellettük szól, hogy erős a kommunikációs készségük, hatékonyan érzékelik a metakommunikációs jeleket- ez segíthet megelőzni a konfliktusokat-, könnyebben elsimítják a konfliktusokat, nyitottak és empatikusak. Pozitív példa, hogy egy űrhajós hölgy két orosz kollégájával volt fent az űrállomáson és a beszámolók szerint pozitívan élte meg a missziót, kollégái elfogadták, jól tudtak együtt működni csapatként. A férfiak hasonlóan számoltak be a hölgy kollégáról. [14] A nők részvétele ellen szól, hogy megbontják a csapat egységességét. Amilyen jól el tudják simítani a konfliktusokat, legalább annyira kiváltói is a konfliktusos helyzeteknek. Néhány példa a konfliktusokra: az egyik űrhajós hölgy összetűzésbe keveredett kolléganőjével, mert megcsalta vele a barátja. Egy másik esetben két űrhajós összeverekedett a misszió hölgy tagjáért. Figyelembe kell tehát venni, hogy amennyiben vonzalom alakul ki két űrhajós között, ennek lesznek következményei. Előfordult az is, hogy a misszió során a legénység két tagja között románc alakult ki, amit a pár próbált diszkréten kezelni, ennek ellenére a társaikat zavarta a viselkedésük.[15]

Mindenesetre az oroszok a Mars 500 program során a nők részvétele ellen tették le a voksukat. A Mars utazás szimulációjában kizárólag férfiak vettek részt azzal az indokkal, hogy a nők bonyolítják a helyzetet. (A program egyik fő kritikája pont az volt, hogy így nem volt életszerű a szimulációs helyzet). [16]

Nők, mint vezetők

Korábban áttekintettük, hogy miben erősebbek a nők, milyen érvek vannak a nők részvétele mellett és milyen érvek vannak ellenük egy hosszú távú űrrepülés során. Az utolsó részben arról lesz szó, hogy milyenek a nők vezetői szerepben. Pszichológiai értelemben véve a vezetés más emberek vezetése, azaz a vezető irányít, befolyással bír a csoport többi tagjára, a csoport céljait és teljesítményét érintő viselkedésükre. A vezetés módszertani értelmezése szerint a vezetés azt jelenti, hogy az ember saját és mások számára olyan értelmes környezetet tud teremteni

amelyben a hatalom, a felelősség átruházása, az önállóság, a munkatársak önszervezése, a tréfa, a fejlődés, a teljesítőképesség és a kreativitás játsszák a fő szerepet.[12] Összességében a vezetés "olyan tevékenység, amely egyének vagy csoportok viselkedésének befolyásolására irányul."[12] A vezetésnek vannak általánosan elfogadott -minden vezetési helyzetre igaz- alapelvei. A vezető közvetítsen egyértelmű jövőképet, legyen fantáziája, lássa át a bonyolult, hálózatos összefüggéseket, legyen a vezető emberközpontú, ismerje a technikát, legyen tekintettel a környezetére, elsőként értesüljön a hírekről, újdonságokról és ezeket ossza is meg a kollégáival, beosztottaival. A jó vezető képes egyszerűsíteni, képes csapatban dolgozni, van humora és a célokat egyértelműen tudja megfogalmazni [12].

Egy vezetőnek sok, különböző készségekkel kell rendelkeznie ahhoz, hogy hatékony és jó vezető váljon belőle. Fontos, hogy meglegyen a megfelelő kognitív és kivitelezési képessége, emellett megfelelően képzettnek is kell lennie. Fontos, hogy jól tudjon kapcsolatot teremteni, valamint a feladatokat helyesen tudja kiosztani. Lényeges a megfelelő kommunikációs készség és a kellő motiváció is. Egy jó vezetőnek képesnek kell lennie a csapatszellem fenntartására, tudnia kell értéket, jövőképet közvetíteni. Egy sikeres vezetőnek kritikusan kell hozzáállni a saját vezetői képességeihez. [12] A vezetői magatartásnak két fontos összetevőjét szeretném most kiemelni. Az egyik az érzelmi intelligencia, a másik a gyakorlati intelligencia. Az érzelmi intelligenciához tartozik a magabiztosság, az öntudat, a tisztesség, a lelkesedés, lendület, az empátia, a szociális érzékenység. A gyakorlati intelligencia összetevői a képzettség, a kognitív készség, a korábbi, saját tapasztalatok, a személyes példa, a hatalommal járó felelősség, illetve annak a képessége, hogy egy vezető meg tudja nyitni az utat az alkalmazottak előtt. [12] Általánosságban azt szokták mondani, hogy a nőknél az érzelmi intelligencia oldal az erősebb. De a női vezetők általában hadilábon állnak a magabiztossággal, mivel kételkednek saját képességeikben és abban, hogy van-e helyük a vezetésben. Ugyanakkor a gyakorlati intelligencia oldal is erős náluk, hiszen rendelkeznek a szükséges képességekkel, van tapasztalatuk, tudnak példát mutatni, stb. [12].

Nemrégiben kerültek előtérbe a női vezetőkkel kapcsolatos kutatások. A termelő cégek rájöttek, hogy nem lehet teljesen „kifacsarni" a munkavállalót, mert akkor gyengül a teljesítménye. (A különböző, munkahelyi stresszből fakadó megbetegedésekről nem is beszélve). Jelenleg a vállalatok fontosabbnak tartják azokat az értékeket, amiket a nők közvetítenek. A nők a vezetési stílusukkal hatékonyabb teljesítményre tudják ösztönözni a beosztottjaikat, mint a férfiak a hagyományos, teljesítményorientált vezetéssel. A női vezetői stílusra jellemző, hogy döntéseiket előre megvitatják a beosztottjaikkal, figyelembe veszik a beosztottak véleményét. A női vezetők építenek beosztottjaik érdeklődésre és munkaszeretetére. A női vezetők ugyanolyan kemények, mint férfitársaik, mert úgy gondolják, ilyen módon könnyebben tudnak érvényesülni. A női vezetők nem utasítanak, parancsolnak, hanem kérnek. Ez a kérés azonban nem mindig egyértelmű, a beosztottak sokszor úgy érzik, nem kell teljesíteniük a kérést.[17] A nőkre jellemzőbb a rugalmasság és a nagyobb teherbírás. Gondoljunk csak bele, egy nő amellett, hogy vezet egy szervezetet vagy szervezeti egységet, otthon ugyanúgy háziasszony, anya, akinek a családjáról is gondoskodnia kell. Ezekkel a jellemzőkkel szemben a férfiak vezetőként konzultálnak a tanácsadóikkal, beosztottaikkal, de a végső döntést önállóan hozzák meg. A férfiakra jellemző az autoritás, a keménység és a parancsadás, amit a beosztottak teljesítenek is.[18]

Összességében elmondható, hogy a nők és férfiak képességei között nincs jelentős különbség. A két nem között van eltérés a vezetői magatartás, stílus tekintetében. Mindkét nemnek vannak erősségei, gyengeségei. Ideális esetben ezek a tulajdonságok kiegészítik egymást. A kérdés az, hogy egy női vezetőt el tudna-e fogadni a legénység egy hosszú távú űrrepülés során, illetve egy női vezető fel tudna-e nőni egy ilyen feladathoz.

ÖSSZEFOGLALÁS

A cikk során szó volt a NASA kiválasztási rendszeréről, arról, hogy ez hogyan fejlődött az évek és a tapasztalatok tükrében. Áttekintettem milyen problémákkal szembesülhet az a szakértő, aki egy hosszú távú űrutazás legénységét szeretné összeállítani. Végül megvizsgáltam, hogy a nőknek milyen szerep jutott az űrutazásban régen és milyen lehetőségeik lehetnek a jövőben. Azt a kérdést, hogy nők vegyenek-e részt egy Mars utazásban a jövő fogja eldönteni.

Felhasznált irodalom

[1] Gilles, C. (2011). Fundamentals of Space Medicine. Chapter 6, 205-244. Space Technology and Library

[2] Fiedler, E.R., Carpenter, F.R.(2005). Evolution of the Behavioral Science Branch of the Space Medicine and Health and Health Care Systems Office at the Johnson Space Center. Aviation, Space, and Enironmental Medicine Vol. 76, No.6, Section II B31-B35

[3] Kanas, N., Manzey D. (2008). Space Psychology and Psychiatry. Space Technology and Library

[4] Kanas, N. (2005). Interpersonal Issues in Space: Shuttle/Mir and beyond. Aviation, Space, and Enironmental Medicine Vol. 76, No.6, Section II B126-B134

[5] Smith, E.R., Mackie D.: (2001). Szociálpszichológia,5. Fejezet A csoportok észlelése 257-317, Osiris kiadó

[6] Ritsher, J.B. (2005). Cultural Factors and the international Space Station. Aviation, Space, and Enironmental Medicine Vol. 76, No.6, Section II B135- B144

[7] Kanas, N., Salnitsky, V., Grund, E.M., Gushin V., Weiss, D.S., Kozarenko, O., Sled, A., Marmar, C.R.(2002). A Shuttle/Mir tanulságai: Pszichoszociális óvintézkedések. Aviation, Space, and Enironmental Medicine Vol. 73, 607-611

[8] Bagdy E. Koroknai B. (1988).: Relaxációs módszerek. Medicina kiadó.

[9] Valentina Tereshkova: First Woman in Space (2013. 06. 14.) Letöltés ideje: 2014. 06.23. http://www.space.com/21571-valentina-tereshkova.html

[10] Az űrrepülés története a számok tükrében. (2014. 05. 28.) Letöltés ideje: 2014. 06. 23. http://urvilag.hu

[11] Geraldyn és a NASA bukta, (2012.02.09.) Letöltés ideje: 2012. 03. 26. http://holgypilota.blog.hu/2012/02/09/geraldyn_es_a_nasa_bukta

[12] Popova K. (2002): Sikeres nők vezető attitűdjei. Női vezetők a férfiak világában Szakdolgozat BGF

[13] Szilágyi K., HR Portal (2008.11.13.): Eljött a női vezetők kora. http://www.hrportal.hu/mobile/index.php?filter=valtozasmenedzsment&url=/hr/eljott-a-noi-vezetok-kora-20081113.html&swidth Letöltés ideje: 2012. 03. 26.

[14] Leon, G. R. (2005). Men and women in space. Aviation, space, and environmental medicine, 76(6 Suppl), B84-8. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/15943200

[15] Keresztúri Ákos: Szex az űrben. (2010. 11. 22.) Letöltés ideje: 2012. 03. 25. http://www.origo.hu/tudomany/vilagur/20101122-szex-az-urben-vonzalom-intim-egyuttlet-terhesseg-es-ezek.html

[16] Öngyilkos küldetés: Mars-expedíció csak oda. (2010. 11. 24.) http://nol.hu/archivum/20101124-nincs_visszaut Letöltés ideje: 2012.03.25.

[17] B.K.: Női vezetők az üzleti életben (2001.01.30.) Letöltés ideje: 2012.03.26. http://www.origo.hu/tudomany/tarsadalom/20010129anok.html

[18] Balogh M.É.(2007): Nők, karrier,család. Női szerepvállalás vidéken a 21. században. Szakdolgozat BGF

HADMÉRNÖK

IX. Évfolyam 3. szám - 2014. szeptember

Károly FEKETE
fekete.karoly@uni-nke.hu

SEVERAL CONSIDERATIONS OF DISASTER RECOVERY COMMUNICATIONS

Absztrakt

In the 21st century the mankind has a lot of different kind of wired and wireless communication network, but only few of them suitable to satisfy the special demands of communications networks of disaster recovery. From point of view of command and control on system level important factors are synergy, information concentration, support of structured information flow, support of permanent operability and operative intervention into the critical positions. On the level of elements of the communications systems of disaster recovery the points of gravity are a bit different: availability, robustness, throughput, EMI resistance, support of different kind of services, such as voice, data, sensor, video and virtualization in context-sensitive social networks and environment.

A 21. században az emberiségnek jónéhánykülönböző típusú kommunikációs hálózat áll rendelkezésre, de ezek közül csak néhány alkalmas a katasztrófavédelem kommunikációs hálózatainak speciális igényeit kielégíteni. A vezetés és irányítás szempontjából rendszer szinten fontos tényezők a szinergia, az információkoncentrálás, a struktúrált információfolyam biztosítása, az állandó működőképesség és az operatív beavatkozási lehetőség támogatása a kritikus helyzetekben.A katasztrófavédelem kommunikációs rendszerének elem szintjén a súlypont egy kicsit más: rendelkezésre állás, robusztusság, áteresztőképesség, EMI ellenállóképesség, olyan különböző típusú híranyagok támogatása mint például hang, adat, szenzor, video információ és virtualizáció kontextus érzékeny társadalmi hálózatokban és környezetben.

Keywords: *C4I in disaster recovery, interoperability, specific characters of the emergency communications networks and elements ~ C4I a katasztrófavédelemben, interoperabilitás, a vészhelyzeti kommunikációs hálózatok és elemek specifikus jellemzői.*

INTRODUCTION

In the event of a disaster the effective communication can be critical to a disaster recovery. The establishing command and control is crucial. The C4I is not a new terminology, as the military has used for many years too. Beside of computer and intelligence the first three terms are essential: “command”, “control” and “communications”.

In practice the cooperation between the parts of organizations of disaster recovery of same and different levels, the interoperability, the cross-border teamwork and the liaison communications are determining from the point of view of recovery chairperson, who is establishes a transparent chain of command and who is responsible for coordinating and directing the actions on strategic levels.

In every emergency situations raises its head the persistent question: what happened? So there is an indispensable demand for instant and reliable access to the highly organized communication networks or to the direct communication as a minimum requirement in the disaster recovery.

REQURIEMENTS

There is a need to:

- synergy between measures of official and professional organizations of disaster recovery such as police, fire departments, border guard, public health, and military (pic. 1);
- concentration of information on highest level disaster management;
- well prepared and reliable system of assessment and the project evaluation of catastrophe (pic. 2);
- compatible information and communications systems for fast and structured information flow for professionals;
- support of operative interference and intervention into the critical positions;
- control of permanent operability and adequate work of communications systems [1].

Figure 1. The practice of disaster calling based on county level (Source: Zoltan Turanyi, 2013. [2])

Figure 2. The DWDM (Dense Wave Division Multiplexing) high speed optical ring communication topology in Hungary, in common with emergency networks

Disaster recovery strategies should be developed for Information technology (IT) systems, applications and data. This includes networks, servers, desktops, laptops, wireless devices, data, connectivity, physical medium for transmitting of signal and so on.

Analyzing on state of the art in information and communication management the major requirements in front of systems regarding to the relevancy are:

- fast data access and real time control of rapid changes of emergency situations;
- timeliness of information and updating of events;
- data integration and linkage;
- structured redundancy of links;
- availability of communications;
- standardization and systematization of information.

CHARACTERICTICS AND VITAL PARAMETERS OF DISASTER RECOVERY COMMUNICATION SYSTEMS

Within a disaster site with a high probability there are multiple separate or uninterrupted disaster areas. Between them and between the main management HQs usually there are a vast amount of stored and renewed data. Consequently in case of multiple separate emergency areas the communications networks should be wide area communication (WAC) linked with a robust backbone connections between them and a lot of powerful hot spot communications covered in situ [3].

Thanks to the Gordon Edwin Moore's law, the available computing power in hand is more than enough after 2kY and we generally have a good bunch of communication access to the different wide and local area networks.

They can be wired or wireless WANs and LANs:

- public access switched telephone networks;
- integrated services digital networks;
- voice over Internet Protocol;
- internet protocol telephony;
- copper wired local networks;
- fiber networks;
- coaxial cable networks;
- group system mobile networks (GSM);
- terrestrial trunked radio networks (TETRA – pic. 3);
- direct radio lines (HF and VHF);
- WI-FI, WI-Max, Bluetooth networks (WPAN);
- satellite communication lines and networks;
- radio line of sight connections.

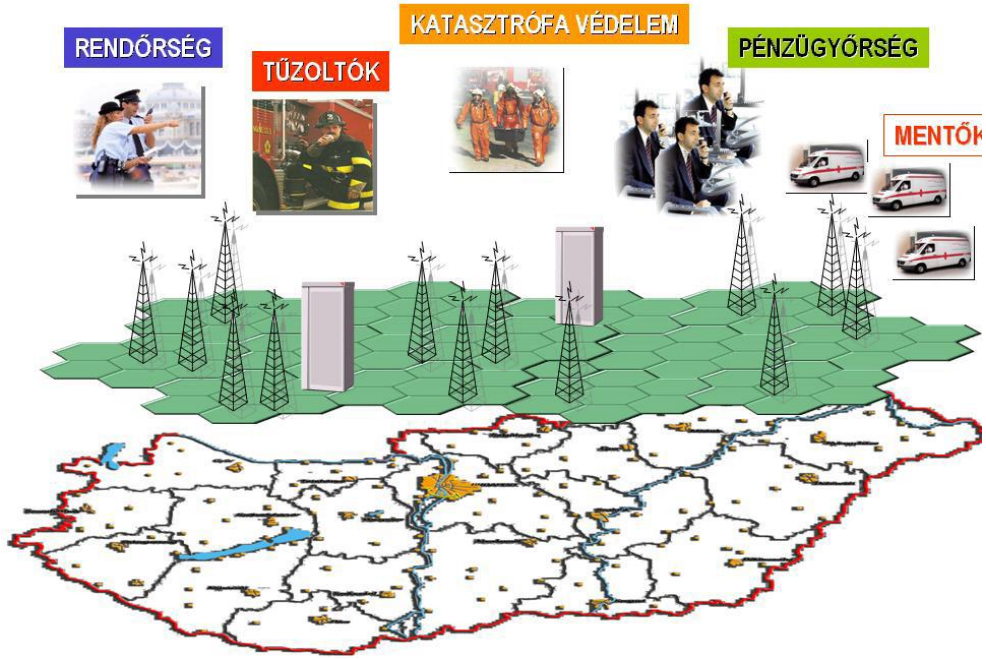


Figure 3. EDR - terrestrial trunked radio network for emergency in Hungary

From point of view of the appropriate communications systems of disaster recovery the most important characteristics and the vital parameters of them are:

- availability;
- performance and throughput of information;
- robustness and reliability;
- continuity;
- up-to-date information inflow (pic. 4, pic. 5);
- symmetry of down and upstream;
- communication overload resistance;
- response time, low jitter, wandering and latency of transmissions;
- electromagnetic interference (EMI) and noise resistance.

Figure 4. Virtualization of data in Emergency HQ, Budapest

Figure 5. Mobile communication HQ in county Somogy, Hungary, 2011

The next considerations of communications networks are mainly responsible for the quality of services:

- large number of services, support of voice, data, video, and sensor information (pic. 6, pic. 7);
- support of media, social networks [4] and different types of visualization;
- encryption capability;
- point to point, point to multipoint and multicast communication;
- peer to peer and ad-hoc mode communication;
- network in network, sub-network support;
- opportunity of group call schemes and prioritization;
- area coverage (pic. 4);
- long distance of communication lines;
- stand-alone operation;
- portability and mobility;
- high level of technical compatibility and interoperability with different kind of communications networks and communications protocols;
- dynamic and automatic configuration management.

Figure 6. Special car of disaster recovery for deploying and collecting data of chemical probes

The survivability is essential for 24 hours-7 days operations:

- longevity of working conditions;
- tolerance against of extreme climatic conditions;
- simple operation;
- low power consumption;
- possibility of different kind of electric power feeding (pic. 8) [5].

Figure 7. Deployed meteorological station with weather sensors

Figure 8. Disaster recovery infocommunication car in action

SUMMARY

In the beginning of the 21st century, the human race has a good possibilities to exploit a lot of available communication networks. But only a few of them acceptable and suitable from point of view of high demands of communications and information networks of emergency situations. In this paper, we collected and identified main characters of adequate disaster communications for disaster response and recovery, with special regard to the possible communications networks. The main point of gravity was dedicated to the assignment of vital parameters, important specifications of system elements of appropriate communication systems, quality of services and survivability.

References

[1] Kuris Zoltán: Az egységes digitális rádiórendszer (EDR) alkalmazásának lehetőségei a rendészeti szerveknél. In: Hadmérnök, 2010. V. évf. 2. sz.

[2] Turányi Zoltán (2013): Megyei tevékenységirányítási rendszer (tér)informatikai megvalósítása/háttere. Prezentáció.

[3] Andreas Meissner, Thomas Luckenbach, Thomas Risse, Thomas Kirste, Holger Kirchner: Design Challenges for an Integrated Disaster Management Communication and Information System, www.l3s.de/~risse/pub/P2002-01.pdf

[4] Endrődi István: Egy lehetséges új veszélyhelyzeti információs és tájékoztató rendszer bemutatása, jelentősége a veszélyhelyzeti tájékoztatásban, Bolyai Szemle, 2014/3., Budapest, ISSN: 1416-1443., pp. 109-121.

[5] Károly FEKETE: Several Aspects of Disaster Recovery in Stationary Military Communication System, Kommunikáció 2009 (Communications 2009) tudományos kiadvány, Budapest, 2009, ISBN 978-963-7060-70-0, Feltalálási hely: Országos Széchenyi Könyvtár, Zrínyi Miklós Nemzetvédelmi Egyetem Tudományos Könyvtár, pp. 275-280.