HADMÉRNÖK

A ZMNE BOLYAI JÁNOS KATONAI MŰSZAKI KAR
ÉS A KATONAI MŰSZAKI DOKTORI ISKOLA
ON-LINE TUDOMÁNYOS KIADVÁNYA

V. Évfolyam 4. szám 2010. december

ZMNE
BUDAPEST

A szerkesztőbizottság elnöke:
Prof. Dr. Halász László

A szerkesztőbizottság elnökhelyettese:
Prof. Dr. Munk Sándor ezredes

A szerkesztőbizottság tagjai és egyben rovatvezetők:
Prof. Dr. Berek Lajos nyá. ezredes CSc (Biztonságtechnika)
Dr. Eleki Zoltán PhD. (Fizikai felkészítés)
Dr. habil. Haig Zsolt mk. alezredes PhD. (Védelmi elektronika, informatika és kommunikáció)
Dr. habil. Horváth László alezredes PhD. (Védelmi igazgatás)
Dr. Jászay Béla PhD. (Védelemgazdaság)
Prof. Dr. Lukács László nyá. mk. alezredes Csc. (Katonai mûszaki infrastruktúra)
Dr. Paskó József CSc. (Térképészet és geoinformatika)
Dr. Szűcs László nyá. ezredes CSc. (Katonai logisztika és közlekedés)
Prof. Dr. Turcsányi Károly nyá. mk. ezredes Csc. (Haditechnika)
Dr. Földi László mk. alezredes PhD. (Környezetbiztonság, ABV- és katasztrófavédelem)

Főszerkesztő: Prof. Dr. Kovács László. mk. alezredes PhD
Szerkesztő: Poroszlai Ákos nyá. mk. alezredes
Webmester: Prof. Dr. Kovács László. mk. alezredes PhD

A szerkesztőség elérhetősége:
Zrínyi Miklós Nemzetvédelmi Egyetem, 1101. Budapest, Hungária krt. 9-11. A. épület 8. emelet
Postacím: 1581. Budapest Pf.:15.
Telefon: +36-1-432-9048
Fax: +36-1-432-9208
HM: 29-734
e-mail: hadmernok@zmne.hu
web: http://hadmernok.hu

Kiadó: Zrínyi Miklós Nemzetvédelmi Egyetem (ZMNE)
Kiadásért felelős: Dr. Lakatos László ny. vezérőrnagy, a ZMNE főtitkára
ISSN 1788-1919

JELEN SZÁMBAN MEGJELENT ÍRÁSOK SZERZŐI:

Ágoston Tibor – ZMNE BJKMK hallgató (BSc)

Dr. Berek Tamás mk. őrnagy – ZMNE BJKMK egyetemi docens

Bodrácska Gyula

Dr. Bottyán Zsolt – ZMNE BJKMK egyetemi docens

Fialka György – ZMNE KMDI doktorandusz

Fleiner Rita – ZMNE KMDI doktorandusz

Dr. Földi László alezredes – ZMNE BJKMK egyetemi docens

Gábri Máté – ZMNE KMDI doktorandusz

Gyarmati Gábor mk. őrnagy – ZMNE KMDI doktorandusz

Illési Zsolt – ZMNE KMDI doktorandusz

Dr. Kassai Károly mk. alezredes – HM Informatikai és Információvédelmi Főosztály

Koleszár Béla – ZMNE KMDI doktorandusz

Prof. Dr. Kovács László mk. alezredes – ZMNE BJKMK egyetemi tanár

Körmendi Krisztina – ZMNE KMDI doktorandusz

Dr. Kun István – LSI Oktatóközpont főiskolai tanár

Kuris Zoltán – ZMNE KMDI doktorandusz

Lipics László – ZMNE HDI doktorandusz

Miskolczi Ildikó – ZMNE KMDI doktorandusz

Dr. Molnár András – Óbudai Egyetem Neumann János Informatikai Kar főiskolai docens

Dr. Muha Lajos – ZMNE BJKMK főiskolai tanár

Prof. Dr. Óvári Gyula ny. ezredes – ZMNE BJKMK egyetemi tanár

Pántya Péter – ZMNE KMDI doktorandusz

Papp Zoltán – ZMNE KMDI doktorandusz

Serege Gábor főhadnagy – ZMNE KMDI doktorandusz

Dr. Seres György – ZMNE KMDI

Dr. Sipos Marianna – ZMNE BJKMK főiskolai tanár

Prof. Dr. Solymosi József – ZMNE BJKMK egyetemi tanár, KMDI vezetője

Stojcsics Dániel – Óbudai Egyetem Neumann János Informatikai Kar

Szabadi Vilmos – MH. 59. Szentgyörgyi Dezső Repülőbázis

Szalkai Attila – ZMNE HDI doktorandusz

Szász Gábor – Gábor Dénes Főiskola főiskolai tanár

Dr. Szegedi Péter mk. alezredes – ZMNE BJKMK egyetemi docens

Szegediné Lengyel Piroska – Zsigmond Király Főiskola, ZMNE KMDI doktorandusz

Vágföldi Zoltán – MH Görgei Artúr Vegyivédelmi Információs Központ

Vizi Pál Gábor – ZMNE KMDI doktorandusz

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Gyarmati Gábor
gyarmati.gabor@zmne.hu

AZ ASP[1] FÉM TAKTIKAI TELESZKÓPOS BOTOK KIKÉPZŐI ÉS FELHASZNÁLÓI KIKÉPZÉSI PROGRAMJÁNAK BEMUTATÁSA, ALKALMAZHATÓSÁGÁNAK LEHETŐSÉGEI A MAGYAR HONVÉDSÉGBEN

Absztrakt

A fém taktikai teleszkópos botok hazai alkalmazásának szélsőséges megítélése, továbbá az eszköz túlmisztifikálása háttérbe szorította az eszköz elterjedésének lehetőségét a védelmi szférában. A nemzetközi viszonylatban rohamosan terjedő alkalmazás arra enged következtetni, hogy a fém taktikai botnak van létjogosultsága. Az alkalmazásnak egyik, ha nem a legfontosabb feltétele a magas szintű kiképzettség és annak professzionális alkalmazása a gyakorlatban.

The exaggerated adjudication of domestic usage, the mistification of the device inhibited the permeation of the telescopic tactal baton in the defence sphere. Meanwhile the spread of the usage on international level confirms the raison d'étre of the device. High-level training, and professional appliance of the gained knowledge are vital requirements of the successful appliance.

Kulcsszavak: *ASP, fém taktikai teleszkópos bot, vipera, kiképzés ~ ASP, tactical telescopic baton, training*

[1] ASP – Armament System and Procedures, INC - Amerikai rendvédelmi eszközöket gyártó cég

„Protecting Those Who Protect” – „Óvni az oltalmazót”[2]

A Magyar Honvédségben a fém taktikai teleszkópos botoknak elsősorban a katonai rendész tevékenységek (járőr**,** tömegkezelés, stb.) során van létjogosultsága. A hagyományos gumibottal szemben a fém taktikai teleszkópos bot számos előnnyel rendelkezik, mely megkönnyíti használatát, viselését. Összecsukott állapotban mérete jelentősen csökkenthető, kiegészítői révén (taktikai lámpa, gázspray, taktikai tükör, üvegtörő, stb.) lényegesen sokoldalúbb eszköz a gumibotnál. A fenti előnyök révén az alkalmazó olyan előnyökhöz juthat, amely a napi szolgálat ellátását megkönnyíti, még abban az esetben is ha nem kerül sor az eszköz alaprendeltetés szerinti (ütés) használatára.

Az eszköz téves megítélése, az elmúlt évek politikai eseményei és a média szenzációhajhász, sok esetben szakmailag megalapozatlan, téves ismeretei miatt nagyon rossz. Sokan sokféleképen értelmezik a fém taktikai teleszkópos bot lényegét, túlmisztifikálják azt.

A negatív megítélést az eszköz alvilági körökben történő megjelenése és azzal történő egyeztetése, továbbá a 2006. évi tömegkezelések negatív tapasztalatai felfokozták.

A fém taktikai teleszkópos botot (gyártmánytól függetlenül) rendkívül alapos kiképzést követően lehet eredményesen, súlyos személyi sérülések elkerülésével használni.

A vezető taktikai bot gyártó cégek (ASP, ESP[3], Monadnoch[4], stb.) a termékeik mellé a felhasználók részére létrehoztak kiképzési programokat, melyek tartalmilag nagymértékben lefedik egymást (nehéz is a bot alkalmazását nagyon sokkféleképpen értelmezni), viszont rendelkeznek olyan különbségekkel, amelyekre hivatkozva kizárják azok kompatibilitását. A különbségek üzleti érdekek generálják. A cégek által nyújtott kiképzési program szerves része a garanciális feltételeknek, ezzel is védve az ellátásra kerülő eszközök típus homogenitását.

A Magyar Honvédség taktikai bot beszerzései esetében csak az eszköz beszerzése esetén, amennyibe a kiképzési programot nem veszik át, úgy szükséges egy saját kiképzési tematika, mely a botok (független attól, hogy teleszkópos, vagy hagyományos) alkalmazására történő felkészítést biztosítja.

A különböző kiképzési programokat egyértelműen a védelmi szférából, elsősorban a rendőrség kötelékéből kikerülő olyan szakemberek hozták létre melyek magas szinten rendelkeztek küzdősportok területén jártassággal. Az ideális az lenne, ha minden katona iletve rendőr rendelkezne igen magas színtű professzionális küzdősport imeretekkel.

A különböző küzdősportok elemeit tartalmazó bothasználat ezekben, a kiképzési rendszerekben végtelenségig leegyszerűsített formákat tartalmaz, melyek biztosítják a gyors elsajátítást. Az alapok elsajátítása, nem jelenti a készség szintű, minden szituációban alkalmazható jártasságot. Mivel a kiképzési programok küzdősportok (általában bottechnikákat tartalmazó) alapelemeit tartalmazzák, ezért ezen a téren megoszlanak a vélemények a közelharc szakemberek körében.

Természetesen minden szakember egészséges szakmai sovinizmustól vezérelve a saját küzdő módszerét tartja a megfelelőnek. Ez természetes és elfogadható, viszont a kérdés attól még nem megválaszolt, hogy akkor melyik az a botos küzdősport, melyet az alap kézitusa ismeretekkel rendelkező kiképzendő rendvédelmi személynek oktatni kellene.

A taktikai botokat forgalmazó cégek egyértelműen a saját kiképzésüket tartják a legmegfelelőbbnek, a különböző harcművészeti ágak képviselői a saját harcművészetük mellett teszik le a voksukat. Akkor most melyik a megfelelő módszer.

---

[2] ASP INC jelmondata
[3] ESP – Euro Security Products, Cseh rendvédelmi eszközöket gyártó cég
[4] Monadnoch - Amerikai rendvédelmi eszközöket gyártó cég

A megfelelő kiképzési program kiválasztásához meg kell vizsgálni a következőket:

- Melyik az a program, melynek az elsajátítása biztosítja a leghatékonyabb alkalmazást?
- Melyik programot lehet a leggyorsabban elsajátítatni és a későbbiekben a gyakoroltatást (a képesség szinten tartás érdekében) a napi, heti munkarendbe megfelelően beiktatni?
- Melyik az a program, mely alkalmas más nem halálos és hagyományos fegyverekkel együtt történő alkalmazásra, annak kiképzési rendszerébe hogyan integrálható.
- Milyen kiképzői szakállományt lehet biztosítani az adott eszközökre?
- Milyen technikai és infrastrukturális követelményei vannak a kiképzésnek?

A kiképzés egyik legmeghatározóbb összetevője az idő. Felmerül a kérdés, hogy az összes hagyományos és nem halálos fegyver alkalmazásának gyakorlása (mivel, gyakorlat teszi a mestert), hogyan illeszkedhet be a a napi munkavégzésbe. Az idő itt a kritikus, mivel minden ilyen gyakorlati képességnek a magas szinten tartása rendkívül időigényes. A munkaidőben végrehajtásra kerülő gyakorlás a szolgálati tevékenység rovására megy, viszont nem lehet elvárni a rendőrtől, katonától, hogy szabadidejéből, anyagi lehetőségeiből, jelentős mértékben fordítson időt a bottechnikák, pusztakezes technikák, kézi lőfegyverek alkalmazása, és egyéb tevékenységek magas szintű gyakorlására.

A munkaidő és a szabadidőben történő időfelhasználás között kell megtalálni a kényes egyensúlyt, mely biztosítja a folyamatos készség fenntartását.

Jelen írás az ASP cég által forgalmazott fém taktikai teleszkópos botok kiképzési programját kívánja bemutatni, mely alapvetően két fő irányból áll, ezek a kiképzők kiképzése, és a felhasználók kiképzése. Általában erre a kiképzésre épülhet rá a cég által forgalmazott bilincsek alkalmazására irányuló kiképzés is.

Az ASP cég jelenleg 75 országban folytat kiképzői kiképzési programot. Az elsősorban gyakorlatorientált kiképzés két nagy részből tevődik össze. Az első az ASP alapkiképzés, amely a felhasználók kiképzésének a programja (ASP Basic Certification - ABC), a második az ASP kiképzői program (ASP Instructor Certification - AIC), amely a leendő kiképzők felkészítésének a programja. A kiképzők hajtják végre a felhasználók kiképzését. Ennek érdekében az Ő kiképzésük időigényesebb, miután Nekik az oktatási módszereket is el kell sajátítani a bot használatán kívül. Az ideális megoldás, ha már kiképzett felhasználókból történik a kiképzők kiválasztása. A kiképzés nagyon rövid, a legszükségesebb elméleti képzést tartalmazó része után a jelentős fizikai igénybevételt tartalmazó gyakorlati kiképzés követi. A felhasználói alapkiképzés egy napos kurzus (8 óra), mely nagyon kevésnek tűnhet, de a kiképzés alapfeltétele, hogy a kiképzendők, megfelelő fizikai és mentális felkészültséggel rendelkezzenek, ami joggal el is várható a rendvédelmi szerveknél szolgálatot teljesítő személyektől. A kiképzői program kiegészül – az alapprogramhoz képest – oktatói módszerek elsajátításával és az oktatás gyakoroltatásával. Ennek időszükséglete 2 nap (16 óra).

A kiképzési program felépítése:

1. Kiképzési program felépítésének ismertetése
2. Az alkalmazás elmélete, alapvető szabályai
3. Az ASP botok technikai adatai, felépítésük
4. Testhelyzetek
5. A gyakorlati kiképzés terminológiája
6. A gyakorlati kiképzés felépítése
7. Alap gyakorlatok
8. Ütésmódok gyakorlása
9. Értékelés
10. Kiképzői módszerek
11. Kiképzői segédlet

Jelen írás egy, a ZMNE-n 2009-ben megtartott 3 napos AIC kurzus tapasztalataira épül. A kiképzésen számos olyan ismerettel gyarapodtunk (főleg gyakorlati), melyek választ adtak olyan kérdésekre, melyek segítettek velem eloszlatni számos olyan tévhitet, melyet eddig a fém taktikai teleszkópos botról hallottam és a médiából sugallnak.

Kiképzési program felépítésének ismertetése

A kötelező regisztrációt követően a kiképzői állományt bemutatták, mely általában áll egy ASP kiképzőből (ATC)[5], technikai biztosító szakember (TSM)[6]. Az ASP igyekszik a kiképzőket autentikus közegből (rendvédelmi szerveknél tapasztalatot szerzett szakemberek) biztosítani, a hitelesség érdekében.

A továbbiakban ismertették a kiképzés lefolyását, felépítését. Nagyon érdekes, hogy a kiképzők felvállalták, hogy semmi fantasztikus és misztikus dolgot nem fognak tanítani, hanem nagyon egyszerű tevékenységeket fognak megmutatni.

Figyelembe vették, hogy a kiképzendők milyen szervezettől, milyen kiképzettséggel, egyéni képességekkel rendelkeztek. Ebből a szempontból célszerű a kiképzendők körét azonos képességekkel, adottságokkal rendelkezőkből összeállítani, mert így érhető el a leghatékonyabb képzés. Kiemelt figyelmet fordítottak itt is a biztonsági rendszabályok ismertetésére.

Az alkalmazás elmélete, alapvető szabályai

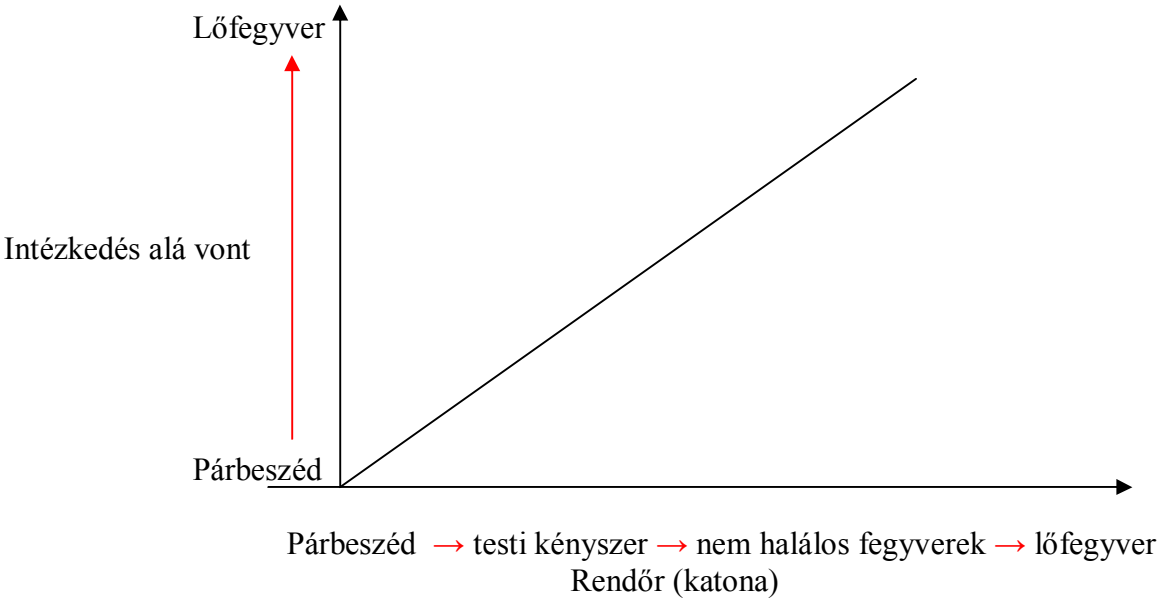
A botok szabályos és biztonságos (mind a felhasználóra, mind az intézkedés alá vont szemszögéből) alkalmazásának egyik legfontosabb alapkérdése, hogy mikor, hova, mekkorát, miért ütünk! Minden rendvédelmi szerv alkalmaz, úgynevezett erő alkalmazásának folytonossági elvet (Confrontational Continuum), mely az intézkedés alá vont személlyel szemben alkalmazható eszközök sorrendjét vázolja fel a szembenálló fél által alkalmazott eszközök függvényében, melyet az 1. számú ábra mutatja be.

Az intézkedés alá vont személy esetében a párbeszédtől az alkalmazott eszközök tárháza a lőfegyverig, szinte végtelen variációt tartalmazhat. Ezzel szemben a rendőr (katona) szinte kizárólag (kevés kivételtől eltekintve) a rendszeresített eszközöket alkalmazhatja, jól megválasztva, hogy az arányosság elvét szem előtt tartsa.

„Nem halálos fegyvernek nevezünk minden olyan eszközt, anyagot és eljárást, amelyet kifejezetten abból a célból terveztek, és oly módon alkalmaznak, hogy a szemben álló fél élő erejét, valamint technikai eszközeit infrastrukturális létesítményeit semlegesítse, azokat harcból kivonja, harcképességeiket és alkalmazástehnikai lehetőségeiket korátozza, alkalmazásukat lehetetlenné tegye. A nem halálos fegyverek – bizonyos esetek kivételével – a célszemélynek csekély mértékű sérülést, az anygi javakban és a környezetben pedig minimális járulékos kárt okoznak.” [7]

Ebbe a nagy csoportba tartoznak a botok (gumi, műanyag, taktikai teleszkópos botok, tonfák), gázspray-k, nem áthatoló lövedékek, elektromos sokkolók (kontakt, kilőhető elektródás és kilőhető elektromos sokkolók), bilincsek, irányított energiájú nem halálos fegyverek (ultrahang, infrahang, mikrohullámú és lézer, stb.).

[5] ASP Trainer Certification
[6] ASP Technical Support Managers
[7] Bartha Tibor: Nem halálos fegyverek Egyetemi jegyzet, ZMNE, Budapest 2009, p.: 17



1. ábra. Az erő alkalmazásának folytonosság elve (Confrontational Continuum)

Mivel minden rendvédelmi szerv más-más fajta nem halálos fegyverekkel van ellátva, így nem lehet törvényszerűsíteni az alkalmazható nem halálos fegyverek sorrendjét, csak elvi sorrendek javasolhatók. Egy adott ország területén rendőrségi tömegkezelés, és egy hadműveleti területen végrehajtásra kerülő katonai rendészek által végrehajtott tömegkezelés az alapelveken túl számos olyan sajátosságot tartalmaz, amelyek alapvetően befolyásolhatják az alkalmazott eszközök fajtáit és az alkalmazás sorrendjét.

A különböző eszközök alkalmazásának további speciális körülményei a célszemély állapota (kora, neme, fizikai állapota, motiváltsága, stb.), továbbá az alkalmazó felkészültsége, jártassága az eszközök alkalmazásában, közelharcban és az alkalmazott eszköz minősége.

A kiképzendő (majd a későbbi intézkedő) személytől a következő alapvető tulajdonságokat várták el a kiképzésen:

- Reagáló képesség
- Állóképesség
- Rugalmasság
- Koncentráció
- Sebesség, gyorsaság
- Fizikai erő
- A feladatok legegyszerűbb végrehajtása

Természetesen túl egyszerű volna, ha ennyi elég lenne az eredményes feladat végrehajtásra, de az alapkövetelményeket átfogóan tartalmazza.

Az ASP botok technikai adatai, felépítésük

A taktikai bot rövid történeti áttekintését követően, nagyon röviden bemutatták annak részeit, szétszerelését, karbantartási alapelveket, mindezt röviden tömören, szétoszlatva minden misztikumot, amellyel az eszközt a média felruházta.

Gyors áttekintést adtak a forgalmazott botok méret, tömeg felületkezelés és kiegészítők, azok alkalmazhatóságáról.

Az alapvetően négy méretben készülő botok két anyagból készülhetnek. Acélötvözet és a 45%-al könnyebb alumínium ötvözet. Tájékoztatást nyújtottak, hogy melyik felhasználási területen melyik típusú bot az előnyösebb és miért.

Testhelyzetek

Alapállás – „piramisállás”

Minden alkalmazást egy úgynevezett igazoltató állásból indítattak, mely az igazoltatás (ellenőrzés, stb.) során gyakorolt állás. Ebből a bot alkalmazásának megkezdésével az intézkedő felveszi az úgynevezett piramisállást, amely egy alapvetően stabil helyzetet biztosít, és amelyből lehet indítani az ütéseket. Kiemelt figyelmet fordítottak a kezek helyes tartására, a bot elhelyezésére a testen. Ez a mozdulatsor nem egy egymástól jól elkülönült mozdulatokból áll, hanem kellő gyakorlás után egy folyamatos mozdulatsor, melynek a végén az ütés (ütések) a záró elem.

Miután az alapképzés nem tartalmazza a speciális felhasználási területekre (pl.: tömegkezelés) vonatkozó testhelyzeteket, ezért ezt azon katonák kiképzésébe akik tömegkezelési feladatokra kerülnek kijelölésre, mindenféle képpen be kell állítani a képzési programba.

A gyakorlati kiképzés terminológiája, a gyakorlati kiképzés felépítése, alapgyakorlatok, ütésmódok gyakorlása

A következő kiképzési részek szinte egybeolvadtak, olyan szorosan kapcsolódtak össze, hogy a továbbiakban egy részben kerülnek bemutatásra.

Ebben a részben a kiképzendők elsajátították a bot használatával kapcsolatos alapismereteket. A legegyszerűbb fogásokat, az egyszerűbb mozdulatsorokat, részletesen begyakoroltatták. A gyakorlatokat önállóan hajtottuk végre („a levegőt ütve”). Minden mozdulatnak tökéletesen kell beidegződni, mind a kiképző, úgynevezett „Soft baton”-nal ami egy habszivacsból készült gyakorló bot (2. számú kép), mind a fém taktikai teleszkópos bottal. Csak ezek elsajátítása után következett a „céltárgy” a kiképző pajzs megütése, ami nem olyan egyszerű, mint ahogy az elsőre tűnik. Érdekes tapasztalat, hogy az egyszerű mozdulatsorok a gyakorlás előtt milyen esetlenek, mennyire nem az, amire a kiképzés végére alakul.



2. ábra. Puha kiképző bot
(Forrás: http://www.google.hu/imgres?imgurl=http://www.copquest.com/21-2500.jpg 2010.11.23.)

Az egyszerű mozdulatsorok begyakorlása után a következő részben ezek összeillesztése és az ütések gyakorlása következett, de már kiképző pajzs (3. számú kép) segítségével.



3.számú kép.: kiképző pajzs
(Forrás: http://www.google.hu/imgres?imgurl=http://images1.opticsplanet.com/136-180/opplanet-asp-baton-instruction-tactical-training-bag-07102.gif 2010.11.23.)

Az egész gyakorlati részt megelőzte egy szigorúan előírt tematika alapján levezetésre kerülő bemelegítés, nyújtás gyakorlatsor. Mivel az ütés kevés munkakörtől eltekintve nem a mindennapi általános mozdulatsorokból tevődik össze, így a kiképzésen végzett mozdulatsorok számos olyan izomcsoportot is megmozgattak, amelyek máskor nem szenvednek el nagyobb igénybevételt. A sérülések, húzódások elkerülése érdekében a bemelegítést kiemelt figyelemmel kezelték.

A kiképzés ebben a fázisában általában párban dolgoztunk a kiképzők állandó felügyelete alatt, folyamatosan visszacsatolást kaptunk a tevékenységünkről.

A korábbi kiképzési részben elsajátított alap technikák itt öltöttek teljes képet, álltak össze folyamattá, egészültek ki dinamikával, erővel. (4. ábra)

Különböző időtartamú gyakorlatok (általában 2-3 perc) folyamán szembesültünk a fizikai korlátainkal, az egyszerűnek tűnő bothasználat nehézségeivel. Kellő számú gyakorlat sorozattal elérhetővé vált, hogy az ütések pontossága, ereje, gyorsasága elérje azt a szintet ami az eredményes feladat végrehajtás megkövetel.



4. ábra. Páros gyakorlás puha kiképző bottal és ütőpajzzsal
(Forrás:http://www.google.hu/imgres?imgurl=http://www.securityacademy.org/sitebuildercontent/sitebuilderpictures/sota002.jpg 2010.11.23.)

A gyakorlás során a kiképző terem adta lehetőségeit a kiképzők a kiképzési alakzat variációival optimalizálták. A kiképzés nem csak vonalalakzatban (a párok egymással szemben vonalban sorakoztak fel), hanem köralakzatban (a párok egyik feléből álló sor kört alkottak háttal befelé a másik sor pedig szembe velük), majd egy ütéskombináció után egy párral egyik irányba elmozdult. A feladatok (ütésváltozatok) szóbeli parancsok alapján dinamikusan változtak, melyek a koncentrációs képességet hivatott, fejleszteni.

A másik gyakran alkalmazott gyakoroltatás a „szabad küzdelem” volt, mely során a párokban 3 perces dinamikus gyakorlatot hajttunk végre, melyek meghatározott ütéskombinációkat tartalmazhattak. 3 perc után szerepcsere következett.

Természetesen ezek a feladatok kiképző pajzzsal, és kevés kivételtől eltekintve puha kiképző bottal kerültek végrehajtásra, ennek ellenére rendkívül megterhelő és fárasztó tevékenység. Ebben a gyakorlási fázisban is, mind a többiben is, rendkívül nagy figyelmet fordítottak a folyamatos ellenőrzésre, továbbá a párbeszédre, instrukciókra.

Az egyik talán legmeghatározóbb kiképzési rész a védőfelszerelésben lévő ellenfél (RED MAN) (5. ábra) elleni küzdelem (kiképző bottal) volt, mely egy komplex feladat végrehajtást követel meg. Tartalmazta az intézkedés előtti protokoll végrehajtását, a bot használata előtti tennivalókat (figyelmeztetés, felszólítás, utasítások), majd a bot alkalmazásával történő szabályos kényszer alkalmazását. A feladat rendkívül nehéz volt, mivel a szinte statikus, nem mozgó pajzs után az emberként mozgó, viselkedő emberi célpont, szituációban realisztikusabb (továbbá a RED MAN-nek nem fájnak az ütése, viszont tud ütni). A védőfelszerelés ebben a gyakorlatban kiegészült fogvédővel.



5. ábra. REDMAN védőöltözetes, puha kiképzőbotos gyakorlás
(Forrás: http://www.expeditionarycenter.af.mil/photos/mediagallery.asp?galleryID080404-F-9429S-018.jpg 2010.11.23. **)**

Kisebb fizikai igénybevétellel járt, ezért pihentető jellegű a hordmódokkal kapcsolatos gyakorlati ismeretek elsajátítása, továbbá a bot nyitási módjainak gyakoroltatása.

Ebben a részben fektettek nagyobb hangsúlyt a célterületekre. Kiemelt figyelmet fordítottak a tiltott zónákra, mind a fej, nyak, has, gerinc, ágyék.

Érdekes módon a bot összecsukására sem fordítottak kevesebb figyelmet, mint a nyitására. A felhasználó hiteles képet kell, hogy nyújtson (nem válhat nevetségessé), azzal, hogy az intézkedés után többszöri kísérlet után is csak nagy nehezen, esetleg sérülés árán képes összecsukni a botot.

Értékelés

A kiképzés végén írásbeli vizsgán tettünk számot a megszerzett elméleti ismeretekből, majd a gyakorlati képességeinkből is megmérettünk, melyet a kiképzők helyben kiértékeltek. A kiképzők (Instructor) vizsgafeladatai kiegészültek egy kijelölt kiképzési rész bemutatásával.

A kiképzők eszközei, kiképzői segédletek

A kiképzők egységes megjelenésére, és felszerelésére külön figyelmet fordítottak. A kiképzők viselkedése, öltözete, felszerelése, a biztonsági felszerelések, ismerete is a elsajátítandó ismeretek közé tartozik.

Külön előírások tartalmazták a kiképzésen történt balesetek, sérülések történtekor végrehajtásra kerülő feladatokat, elsősegélynyújtástól az esemény dokumentálásáig.

Az ASP cég kiemelt figyelmet fordít a kiképzők képzését támogató személyes felszerelésére. A kiképzők rendelkeznek minden olyan eszközzel, mely a kiképzés során bemutatásra kerül, így gyakorlatias betekintést nyújtanak, így nem csak prezentáción tekinthetők meg azok. Rendelkeznek a cég által kiadott, egységes bemutatókkal, levezetési tervekkel a legapróbb részletekig. Az egyik ilyen érdekesség a bemelegítést és a levezető nyújtás lazítás tartalmát is egy kulturáltan szerkesztett, nyakba akasztható kis emlékeztető, amely alapján végre lehet hajtani.

Elégedettségi kérdőív

A kiképzés végén a minőségbiztosítási szempontok miatt, egy név nélküli elégedettségi kérdőívet töltöttünk ki, amelyből levont tapasztalatokat a későbbi kiképzéseken hasznosítják.

Az ASP kiképzési rendszer alkalmazhatóságának korlátai Magyar Honvédségben

A Magyar Honvédség alaprendeltetéséből adódóan a nem halálos fegyverekkel korlátozott számban és típusválasztékkal rendelkezik. Ezek alkalmazási, kiképzési terminológiája az alap kényszerítő eszközök kiképzési terminológiáján alapul.

A fém taktikai botokkal szembeni önkéntelen ellenszenv, esetleg félelem a közvéleménytől és a médiától gátolja, hogy megjelenjen az alkalmazásban.

A kiképzők és kiképzendők körének meghatározása nehezen definiálható, míg a katonai rendészek esetében egyértelmű, de a missziós tevékenységben résztvevők körében már feladatorientált és eseti.

A megfelelő eszköz beszerzése, a hozzá tartozó kiegészítők hiányában csak részmegoldást biztosít, nem használja ki azokat az előnyöket, amelyeket a teljes rendszer alkalmazása jelent. Például egy olcsó (ez is egy szempont!) gyöngyvászon utánzat hordtok nem teszi lehetővé a bot viselés közbeni előnyeinek létrejöttét, abban az esetben nem gazdálkodunk jól a bot és gyári kiegészítői (műanyag hordtok) által biztosított előnyökkel.

A nem halálos fegyverek alkalmazása sajnos a Magyar Honvédségben nagyon kezdetleges, ellenben a szövetséges haderőkben alkalmazott gyakorlattól. A nem halálos fegyverek ismeretének hiánya egy együttműködés során rosszul végződő tevékenységet eredményezhet. Amennyiben a szövetségi partner alkalmaz ilyen eszközöket, nekünk ismerni kell az alkalmazott eszköz paramétereit, hatásmechanizmusát, speciális képességeit, hogy elkerülhessük egy lehetséges saját erőnkben történő károkozást.

Az ASP kiképzési program alkalmazhatóságának előnyei Magyar Honvédségben

Az ASP kiképzési program alkalmazhatóságának előnyei Magyar Honvédségben a következők lehetnek:

- A fém taktikai teleszkópos botra történő kiképzés nagyon biztos alapot képezhet a hagyományos gumi (műanyag) botok alkalmazásához is. Természetesen az alkalmazás jellegéből adódó különbségek kivételével (bot nyitása, zárása, zárt bottal történő ütés, stb.)
- A katona felszerelésének sajátosságai (nagy mennyiségű felszerelés) esetén az összecsukható bot lényegesen praktikusabb, mérete és előnyössebb hordmódjai, továbbá kiegészíthetősége miatt
- A kiképzési program önmagában is fejleszti a bot biztonságos alkalmazásának képességét az erőnlétet, reflexet és az állóképességet.

Felmerül a kérdés, hogy a Magyar Honvédségben milyen típusú kiképzési program lenne alkalmas a bot alkalmazásának szempontjából, amely nem okoz jelentős változtatásokat a meglévő kiképzési programokban.

Egy nagy, minden részletre és katonára kiterjedő kiképzési rendszer, nehezen alkalmazható a jelentős idő és felszerelés szükséglet miatt. Számos katona nem kerül olyan feladatkörbe, beosztásba, hogy érdemben kamatoztassa a megszerzett ismereteket.

Egy sok, eszközönként különálló kiképzési program (ilyen az ASP taktikai bot kiképzés is), mely minden eszközre külön kiképzést igényelne ugyancsak nagy idő és technikai eszköz szükséglettel bír.

Az eredményességet egy moduláris (egy meghatározott alapra épülő, könnyen variálható) kiképzési program biztosítaná, mely feladatorientáltan alakítható. Különálló modulokból összeállítható lenne a feladatorientált alkalmazásnak megfelelő program. Ez a kiképzési program biztosítaná a feladathoz rendelt eszközök alkalmazásának biztos elsajátítását, továbbá a nagy fontossággal bíró egymással együtt történő alkalmazás, kombinált alkalmazás lehetőségét, képességét! Ebbe a kiképzési rendszerbe be kellene illeszteni a speciális alkalmazási körülményekre történő felkészítést (tömegkezelési sajátosságok, hadifogoly kezelési, rendészi tevékenységek, stb.) Például egy katonai rendész járőr esetében bilincs, gázspray, bot kiképzési modulokból felépülő alap program lenne célszerű, továbbá ezek együttalkalmazhatósági (hagyományos fegyverrel is), tömegkezelési programokkal kellene kiegészíteni.

A fém taktikai botok alkalmazásának egyik legnagyobb akadálya a jogi szabályozás által biztosított alkalmazhatósága. A rendőrség vonatkozásában már megszületett a szabályozás (32/2009. (VIII.19.) IRM rendelet), mely lehetővé teszi a fém taktikai botok rendszerbe állítását. Az eszközök megjelenésére a rendőrök kezében még várat magára mindaddig míg nem születik egy szakmailag indokolt jó döntés, mely fel meri vállalni a közvélemény ellenséges megnyilvánulásával szembeni harcot. Az eszközök biztonságos alkalmazása csak magas szintű kiképzettséggel érhető el, tehát nem elegendő a taktikai botokat kiadni a felhasználók részére.

Felhasznált irodalom

1. Bartha Tibor: Nem halálos fegyverek, Egyetemi jegyzet, E-jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem, Bolyai János Katonai Műszaki Kar, Budapest, 2009.
2. 32/2009. (VIII.19.) IRM rendelet – A Rendőrségnél rendszeresíthető kényszerítő eszközök típusairól, fajtáiról.
3. Tactical baton ASP instructor certification (AIC) course syllabus, ASP, INC ISBN 0-9650547-0-5, USA, 2006.
4. www.asp-usa.com
5. www.asp-usa.com/products
6. www.esp-baton.com/euro-security.info
7. www.batons.com/products

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Óvári Gyula
ovari.gyula@zmne.hu

Szegedi Péter
szegedi.peter@zmne.hu

HAGYOMÁNYOS REPÜLŐGÉP-ÜZEMANYAGOK KIVÁLTÁSÁNAK LEHETŐSÉGEI ÉS KORLÁTAI

Absztrakt

Az egymást követő energiaválságok, a fokozódó környezetszennyezés következtében is fenyegető klímaváltozás és a fenntartható (fenntartani kívánt) gazdasági fejlődés energetikai biztosítása elodázhatatlanná teszi olyan új energia hordozók felfedezését, amelyek hosszú távon kitermelhetőek, előállíthatóak, rövid határidővel gazdaságosan, széles körben bevezethetőek, elterjeszthetőek, nem terhelik (előállításukkal sem!) a környezetet és lehetőleg – lényeges átalakítás nélkül – alkalmasak a jelenleg alkalmazott erőgépeink, hajtóműveink működtetésére is.

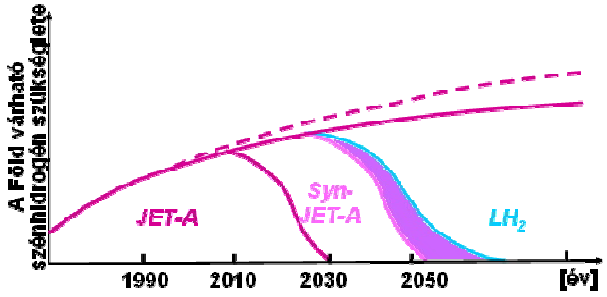
The consecutive energy crises, the threatening climate change, caused mainly by the increasing environmental pollution, and the necessary energy supply for endurable development of economy has made inevitable to find new alternative energy sources, which can be exploited for a long time, produced at short notice and economically and introduced widely, while they do not burden (even with their production process) the environment, in addition they are suitable – without significant technical conversion – to operate the presently used heat engines.

Kulcsszavak: *repülés, üzemanyag, alternatív energiahordozók ~ flight, fuel, alternative energy*

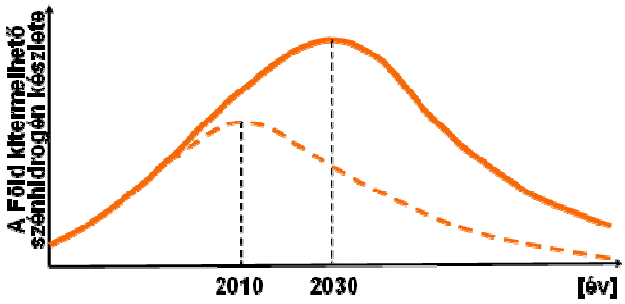
1. A KŐOLAJALAPÚ TŰZELŐANYAGOK KITERMELÉSI, ALKALMAZÁSI PERSPEKTÍVÁI

A jelenleg használatos légijárművek hajtóművei szinte kivétel nélkül olyan szénhidrogén alapú folyékony tüzelőanyagokkal működnek, melyek fűtőértéke 42000–44600 kJ/kg. Ez, dugattyúsmotorok esetében (repülő-)benzin, gázturbinás sugárhajtóműveknél kerozin.

A ’70-es évek első energia-árrobbanását követő sokk utáni első higgadt és tudományosan megalapozott elemzések már egyértelműen jelezték, hogy a műszaki fejlődés és növekvő népesség okán folyamatosan növekvő energiaigény (1. ábra) fedezésére, a Föld rendelkezésre álló és kitermelhető folyékony szénhidrogén készletei csak korlátozott ideig elégségesek (2. ábra). Változatokat ugyan lehetséges volt kimunkálni a várható igények növekedési üteméről és a kitermelhető mennyiség szükségszerű csökkenésének időpontjáról (az 1.-2. ábrákon szaggatott vonal a pesszimista, folyamatos az optimista, 2010-ben prognosztizált változatot jelöli), a trendek azonban sajnálatosan egyáltalán nem vitathatóak.



1. ábra [7. p. 138]



2. ábra [7. p. 138]

Megjegyzés: az 1. ábrán és a továbbiakban L – liquid (ang.) rövidítés, a gáz folyékony (cseppfolyósított) halmazállapotát jelzi.

A tüzelőanyagok árának folyamatos, drasztikus növekedése, a költség-hatékonyságot fokozatosan, még a katonai repülésben is elsődleges elvárássá tette. Az, hogy a tüzelőanyag-igény növekedés nem vált lineárissá (1. ábra), annak is köszönhető, hogy már pl. a 2. és 3. generációs (közepes hatósugarú, polgári) repülőgépnél is kimutatható a takarékosságra való törekvés (korszerűbb, takarékos hajtóművek /turbófan, propfan stb./ és sárkányok /szuperkritikus szárny, winglet, pontosan meghatározott aerodinamikai formák és csatlakozások stb./ alkalmazása).

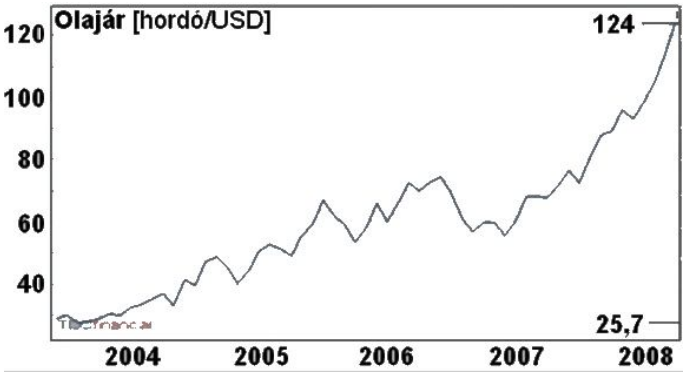
Tovább bonyolítja, egyben sürgeti is a megnyugtató megoldás mielőbbi kimunkálását, hogy - a várakozásokkal ellentétben - a rendelkezésre álló nyersolaj készletek és azok időarányos kitermelhetőségének, a szükségletek változása reális trendjének (1.és 2, ábrák) pontos ismerete sem elég, a várható árak alakulásának közel megbízható prognosztizálásához. A kitermelhető mennyisége, a tényleges hosszú távú átlagos szükségletek és a beszerzési árak között viszonylag alacsony a korreláció. Márpedig az üzemanyag (energia) kiszámítható, megfizethető ára a világ-, és ezen keresztül a nemzetgazdaságok állapotát, közérzetet, életszínvonalat, háborút és/vagy békét határoz meg.

Tapasztalatok szerint az árképzést, a hosszú távú, egyenletes fogyasztás növekedés alapján prognosztizált növekedési trendjeit, időszakosan drasztikusan módosíthatják:

- a piaci viszonyok, ennek szerves részeként, nem elhanyagolható mértékben a spekuláció;
- utóbbival szoros összefüggésben a nemzetközi válsággócokban, különösen a közel-keleti olaj-övezetekben, rendszerint az USA részvételével vívott helyi háborúk és ezek

nyomán katonai szükségletek jelentős növekedése, esetlegesen egyes olajbányászati övezetek termelésből, szállításból történő időleges kiválása, kiiktatása;

- különösen az ezredfordulót követően, az újonnan viharos ipari, gazdasági fejlődésnek indult ázsiai hatalmak (Kína, India) rohamosan növekvő energia igénye nyomán (is) kibővült a kereslet. Mindezek együttesen, 1-2 év alatt 100÷400 %-os üzemanyagár ingadozást eredményezhetnek (3. ábra).



3. ábra [16.]

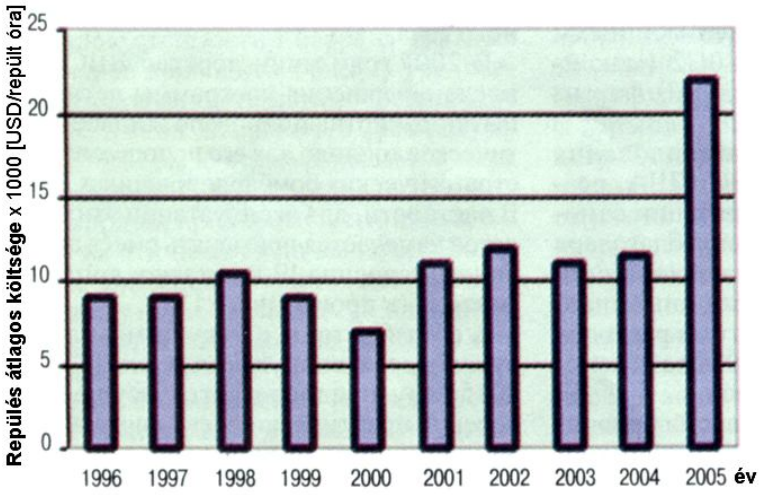
Ugyancsak a fenti okokra vezethető vissza az is, hogy az üzemanyagok termikus krakkolással történő előállítása kiinduló anyagaként szolgáló nyersolaj magasabb szinten (drágábban) előállított származékainak (pl. benzin) beszerzési árát időlegesen meghaladhatja az alacsonyabb szinten feldolgozottét (pl. gázolaj).

A csak repülőgép tüzelőanyagból átlagosan évi 20 milliárd liter beszállítást igénylő, folyamatosan magas harckészültségű USA hadsereg szükségletei, világviszonylatban is alapvetően befolyásolják az üzemanyag árakat. Elemzések szerint 1 barrel (~163,5 liter) kőolaj árának 10 USD-os emelkedése a PENTAGON éves kiadásait 600 millió dollárral növeli. Egyebek mellett, a folyamatos közel-keleti katonai jelenlét miatt is - változatlan struktúrában – de 2008-ra, napi 10 millió literre növekedett repülő-tüzelőanyag felhasználás.

A mennyiségi növekedés és az általa generált árfelhajtó hatása következtében, az amerikai hadsereg éves hajtó- és kenőanyag költségei az alábbiak szerint változtak:

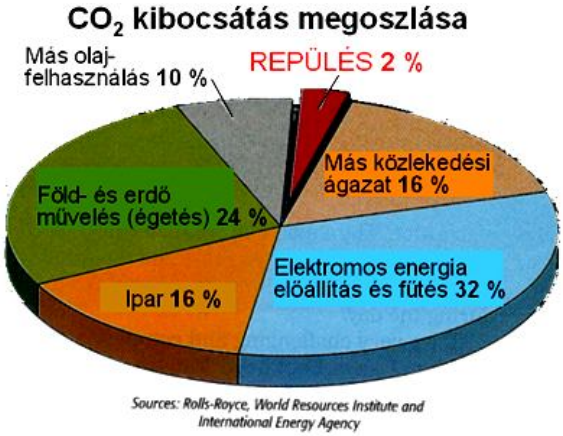
- 2004-ben 6,7 millió USD;
- 2005-ben 8,8 millió USD;
- 2006-ban 11,2 millió USD.

Mindezek ebben az idő-szakban, egy repült óra átlagos költségeit – az éppen aktuális katonai, politikai helyzet befolyásolta, némileg hullámzó jelleggel, de – egyértelműen a növekedés irányába módosították (4. ábra).



4. ábra [16.]

A XX. század második felére - a vonatkozó kutatások eredményeként is - ugrásszerűen megerősödött és megkerülhetetlenné vált a környezettudatos szemléletmód. A várakozásokkal ellentétben 2006-ról 2007-re globálisan három százalékkal emelkedett a fölmelegedést okozó széndioxid-kibocsátás. Az emberiség történetében soha nem tapasztalt mértékű, 9,34 milliárd tonnányi volt a főképp az ipari tevékenységekből, a közlekedésből és az erdőirtásból eredő globális széndioxid-kibocsátás (a Global Carbon Projekt nevű, klímakutató intézet adatai alapján). 2006-hoz képest ez körülbelül 3%-os emelkedést jelent, a szén-dioxid légköri koncentrációja elérte a 383 ppm-es értéket (a levegő minden egymillió molekulájából 383 széndioxid-molekula).



5. ábra [16]

Így, egyértelművé vált, hogy a légköri szennyezés 2 %-áért felelős repülés (5. ábra) – mely prognózisok szerint, évi 5 %-os légiforgalmi növekedést feltételezve, ~2025-re már elérheti a 3 %-ot – csak olyan korszerűsítésekben, alternatív és/vagy át-meneti tüzelőanyagok alkalmazásában gondolkodhat, amelyek nem terhelik a környezetet, nem járulnak hozzá további széndioxid kibocsátással az üvegházhatás fokozódásához. Mindezek egyszerre jelentenek új impulzust, de egyben további korlátokat, nehézségeket a fejlesztésben.

2. ALTERNATÍV ENERGIAHORDOZÓK

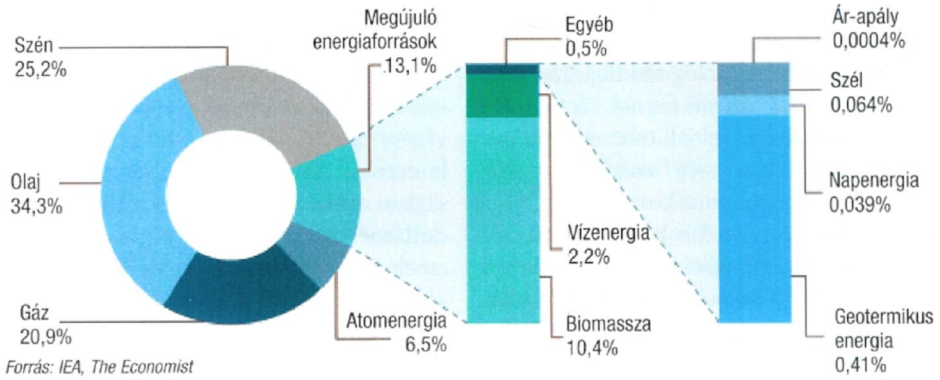
2.1. Alternatív energiaforrások kiválasztásának szempontjai

Az előzőekből (is) következik, hogy belátható időn belül elengedhetetlenül szükséges a jelenleg használatos (repülőgép-) üzemanyagok (benzin, kerozin) kiváltása olyan(ok)kal, amely(ek) lehetőleg egyszerre felel(nek) meg az alábbi követelményeknek:

- magas fűtőértékű, nem környezetszennyező;
- kémiailag, halmazállapotát tekintve stabil, nem lép reakcióba a fedélzeti tüzelőanyag-rendszer elemeivel, berendezéseivel;
- hosszú időre, megbízható, könnyen kitermelhető és olcsón feldolgozható tartalékok álljanak belőle rendelkezésre, a kitermelésre, feldolgozása, átalakítása sem tartalmazhat nagy energiaigényű és/vagy, környezetet terhelő technológiát;
- alkalmas a repülőgép szükséges berendezéseinek, hajtóműve(inek), légkondicionáló rendszerének és hordfelületeinek (a lamináris áramlási zóna kilépőél irányába történő kitolása érdekében) a kívánt mértékű hűtésére;
- a jelenleg meglévő repülőgéppark és az annak kiszolgálásához szükséges infrastruktúra, lehetőleg változtatás nélkül, vagy minimális átalakítással, korszerűsítéssel legyen alkalmas a vele történő működésre.

A hagyományos fűtőanyagok (szén, kőolaj, földgáz) kiváltására, pótlására, minden hőenergiát hasznosító ipari, közlekedési, háztartási energetikai ágazatban már évtizedek óta, több irányba is folynak a kutatások megújuló energiaforrások feltalálására és alkalmazására (6. ábra).

Ennek aránya, a XXI. század első évtizedére – az atomenergiát is ideszámítva - sem haladta meg a 20 %-ot. Ráadásul a megismertek egy része (víz, szél, árapály, geotermikus) tökéletesen alkalmatlan repülőgépben történő közvetlen hasznosításra, míg a többiek különböző mértékben, módon és kutatásra, fejlesztésre fordított további időigénnyel számításba vehetőek, mint alternatív lehetőségek. Gazdaságossági szempontból meghatározó fontosságú, hogy a néhány éven belül, jelentős mennyiségben alkalmazni kívánt üzemanyagok, vagy üzemanyag kiegészítők csak olyanok lehetnek, melyek a meglévő repülőgépek üzemanyag tartályaiba feltölthetőek, a rendszer elemei azokat továbbítani képesek, a hajtóművek vele, legalább korábbi hatékonyságukkal működnek.



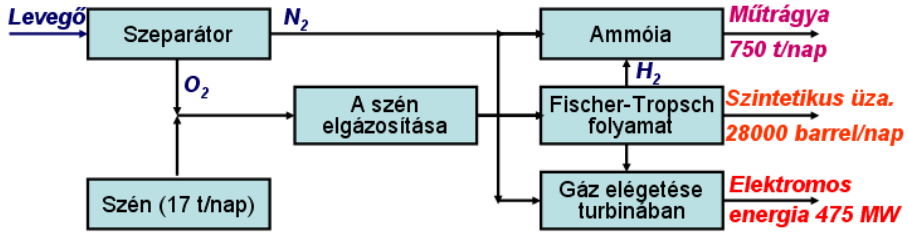
6. ábra

2.2. Biomassza és szintetikus tüzelőanyagok

A jelenlegi üzemanyagok kiegészítésére, helyettesítésére – kezdetben legnagyobb ígéretnek tartott - biomasszák alkalmazása kétséges, mivel nagytömegű, hosszú távú termelhetőségük korlátozott és ellentmondásos. Abban szakemberek többsége egyetért, hogy 2030-ig a biomasszából termelt, megújuló energia mennyisége maximum megduplázódhat. A biomassza-termelés haszna döntően az olyan országokban jelentkezhet, ahol sok az erdő. (A

biomasszával az az alapvető gond, hogy a növényi fotoszintézis csak ~1 %-os hatás-fokkal alakítja át a napenergiát kémiai energiává, ezért az alapanyagul szolgáló növényi kultúra termesztése hamar eléri terjeszkedésének korlátait). Napjainkban nagy reményeket fűznek a tengeri és édesvízi algák üzemanyagként történő felhasználásához is.

A jelenleg alkalmazott légijárművek benzin-, kerozin-felhasználása csökkentésének, időleges, de akár teljes kiváltásának egy lehetséges módszere lehet, az iparilag előállított szintetikus üzemanyagok alkalmazása (7. ábra).



7. ábra [saját a 16. alapján]

A módszer nem új, de az előállítási folyamat tetemes hagyományos energia igényének – ezáltal környezetszennyezésének – csökkentése még mindig jelentős kihívás.

2.3. Cseppfolyósított (kriogén) gázok, mint lehetséges repülőgép üzemanyagok

Hosszútávú utánpótlás, kitermelhetőség legnagyobb valószínűséggel a vízből biztosítható, mivel belőle gyakorlatilag korlátlanul kinyerhető a hidrogén. Ezenkívül a kőolaj, valamint földgáz kitermelés során melléktermékként megjelenő un. paraffin-szénhidrogének (minden tagjuk a közös, általános C_nH_{2n+2} képlettel előállítható homológ sor eleme, kémiailag is hasonlóak), közülük az első 5-7 gáznemű, illetve folyékony. Utóbbiakat napjainkig előírások és kimunkált technológia hiányában rendszerint a feltárás helyszínén elégetik.

A repülőgépek (járművek) működtetésére a 1. táblázatban felsorolt gázokat, a tárolás gazdaságossága, a hajtóműbe történő adagolás pontossága miatt cseppfolyósított (kriogén) állapotban célszerű alkalmazni.

Üzemanyag képlete	**Kerozin JET A**	**Hidrogén H_2**	**Metán CH_4**	**Etán C_2H_6**	**Propán C_3H_8**	**Bután C_4H_{10}**	**Pentán C_5H_{12}**	**Hexán C_6H_{14}**
olvadás [^{0}C]*	< -60	-261,9	-182,5	-183,3	-187,7	-138,3	-129,7	-95,3
forrás [^{0}C]*	136÷227	-252,8	-161,7	-88,6	-42,1	-0,5	36,1	68,7
$\Delta t_{cseppfolyós}$ [^{0}C]*	196÷287	~9	~21	~95	~145	~138	~166	~163
Kritikus jellemzők								
hőmérséklet [^{0}C]	374	-240	-82,6	32,3	96,8	152	196,6	234,7
nyomás [MPa]	2,42	1,3	4,6	4,9	4,3	3,8	3,3	3
Üzemanyag sűrűsége [kg/m^3]								
olvadáskor	775÷785	71,07	424,4	546,4	582	601,5	610,1	664
forráskor	835 (-60 ^{0}C)	77,15	453,4	650,7	733,1	736,4	761,2	756,9
Égéshő (20 ^{0}C-on)* [kJ/kg]								
maximális	46470	135380	56290	51910	50380	49535	49045	48710
minimális	43290	114485	49930	47515	46390	45745	45380	45130

1. táblázat [15. alapján]

Megjegyzés: A táblázatban felsorolt gázok közül – rendkívül magas égéshője, és/vagy a hosszú távú, ipari méretekben biztosítható kitermelhetősége miatt – a hidrogén, metán, propán és bután részletes vizsgálatát célszerű elvégezni.

2.3.1. Hidrogén (H_2)

Az egységnyi tömegéből nyerhető égéshője 2,7-szeresse a kerozinénak, de beláthatóan a többi, 6. táblázatban és 10. ábrán bemutatott gázét is lényegesen meghaladja. Igen kedvező az

égési karakterisztikája is, a láng terjedési sebességét és hőmérséklet megoszlását illetően, valamint egyetlen gáz a felsoroltak közül melynek égéstermékeiből hiányoznak a széngázok (2. táblázat).

Égéstermék	Kerozin	LH_2
Elsődleges égéstermék	CO_2 H_2O	H_2O
Égési melléktermék és az atmoszférával való reakciók termékei	$HC \rightarrow O_3$ $NO_x \rightarrow O_3$ $CO \rightarrow O_3$ $SO_2 \rightarrow H_2SO_4$	$H_2 \rightarrow H_2O$ $NO_x \rightarrow O_3$

2. táblázat [7.]

1 kg kerozin elégetésekor 3,16 kg CO_2 (széndioxid) és 1,25 kg H_2O (víz) keletkezik. 1 kg hidrogén elégetésekor 9 kg H_2O jön létre. 0,36 kg hidrogén 1 kg kerozinnak megfelelő energia-tartalommal rendelkezik, ennyi hidrogén elégetése 3,21 kg vizet eredményez.

A cseppfolyós hidrogén égetése sem üvegházhatású CO_2-t, sem a kerozin elégetésekor keletkező más mérgező melléktermékeket hoz létre, kivéve a nitrogén-oxidokat. A hidrogénből azonban 2,6-szor több víz keletkezik, ami nagy magasságokban szintén kedvezőtlenül befolyásolja az üvegházhatást.

Kedvezőtlen viszont, hogy sűrűsége mindössze 1/11÷1/12-e a kerozinénak, így egységnyi, kerozinéval megegyező energia tárolására ~3,7-szeres tartálytérfogat szükséges, melyet számottevően tovább emel a cseppfolyós halmazállapothoz tartozó, rendkívül alacsony hőmérséklet ($t<250\ ^0C$) fenntartásához szükséges aktív és passzív hőszigetelő rétegek beépítése. Valamennyi vizsgált gáz közül az LH_2 - szerkezeti hűtésre, a hordfelületek körüláramlásának javítására, stb. használható - hűtőképessége a legnagyobb. Jelenleg még megoldatlan a cseppfolyós halmazállapota fenntartásához szükséges, alacsony hőmérséklethatárokhoz tartozó $(-253)\div(-262)\ ^0C$, rendkívül szűk, $\Delta t=9\ ^0C$-s tartományban, a megbízható és gazdaságos tárolásának lehetősége is.

Vélelmezhetően a LH_2 repülőgép üzemanyagként történő rövid távú elterjedését elsődlegesen nem a felsorolt nehézségek, nem is csak a legmagasabb közvetlen - és a szükséges infrastruktúra kiépítése miatt - közvetett költségek akadályozzák, hanem döntően az előállítás módja. A jelenleg ismert két ipari előállítási módszer (vízbontás elektrolízissel, vagy vízgázból, földgázból, bázisok, sók oldatának elektrolízisével) olyan, nagy mennyiségű hagyományos energiát felhasználó folyamat eredménye (pl. szénerőműben termelt villamosságét!), mely a környezetet súlyosan terheli. Emiatt, a cseppfolyósított hidrogén sem tekinthető kémiailag tiszta energiának.

2.3.2. Metán (CH_4)

Alkalmazását az célszerűsíti, hogy a földgáz legnagyobb arányban előforduló komponense (lényegesen meghaladja a propán és bután együttes tömeghányadát). Ugyanakkor gyakorlati felhasználhatóságát ugyanazok a repülőgépszerkezeti, szilárdsági, aerodinamikai, légi- és földi üzemeltetési, valamint az infrastrukturális átállás kimagasló anyagi terhei nehezítik, mint a hidrogén esetében. (Ld. még 3.4. fejezet!).

A metán égéshője ugyan 15 %-kal meghaladja a kerozinét, de még az alacsony hőmérséklet ($t<160\ ^0C$), szűk tartományában ($\Delta t=21\ ^0C$) fenntartható cseppfolyós halmazállapotában is viszonylag kicsi a sűrűsége $\rho_{CH4}=424\div453$ kg/m3 (v.ö. 1. táblázat !), így a kerozinéval ekvivalens energiamennyiség tárolására 1,5÷1,6-szoros tartálytérfogat kialakítása szükséges. (Az üzemi hőmérsékletet figyelembe véve, a szükséges hőszigetelés

beépítése tovább növeli a tartályok, vezetékek és kapcsolódó berendezések tömeg és térfogat hányadát.)

Annak ellenére, hogy égéshője, hűtőképessége meghaladja a propánét, annak nagyobb sűrűsége és a folyékony halmazállapothoz tartozó lényegesen magasabb hőmérsékleti minimum, illetve maximum, valamint a köztük lévő széles üzemi hőmérsékleti tartomány (Δt=145 ^{0}C), tapasztalatok szerint a vele alkotott keverék gyakorlatban egyszerűbben alkalmazható, olcsóbb üzemanyagot alkot, mint tiszta formában (ACKT-M). Az optimális keverési arányok kialakítása még további hosszadalmas kísérleteteket igényel.

2.3.3. Propán (C_3H_8)

Mivel mind a kőolaj gázainak, mind a földgáznak egyaránt jelentős mennyiségű összetevője, de viszonylag nagymennyiségben szabadul fel a különböző kőolaj származékok előállításakor is, gazdaságos, ipari méretű kitermelhetősége még hosszú időre biztosított. A repülőgép-üzemanyagként történő alkalmazáshoz szükséges fontosabb jellemzői a 6. táblázatból olvashatóak ki.

A cseppfolyós halmazállapothoz tartozó szélesebb hőmérséklettartomány és magasabb forrási hőmérséklet (-42 ^{0}C) nagymértékben leegyszerűsíti a fedélzeti tartályokban és a repülőtéren történő tárolását, illetve szállítását, különösen, ha figyelembe vesszük, hogy 1,6 MPa tartálytúlnyomást alkalmazva már hőszigetelésre sincs szükség cseppfolyós állapotának fenntartására. Az ehhez tartozó – az előző kriogén gázoknál – magasabb sűrűség (ρ_{C3H8}= 582÷733 kg/m3), és az égéshő figyelembe vételével, kerozinéval ekvivalens energia tárolása mindössze 4÷8 %-kal nagyobb tartálytérfogatot igényel. Mindez valószínűsíti, hogy a meglévő repülőgépek szükségszerinti propán üzemanyaggal működőre történő átalakítása, nem lesz különösebben bonyolult és költséges feladat, főként mert ehhez, maga a hajtómű is csak kisebb mértékű módosításokat igényel.

A propán (és bután) gyakorlati alkalmazását az is célszerűsíti, hogy magas a termikus stabilitásuk és sokkal kevésbé agresszívek a szerkezeti-, gumi- és tömítő-anyagokkal szemben, mint a kerozin.

2.3.4. Bután (C_4H_{10})

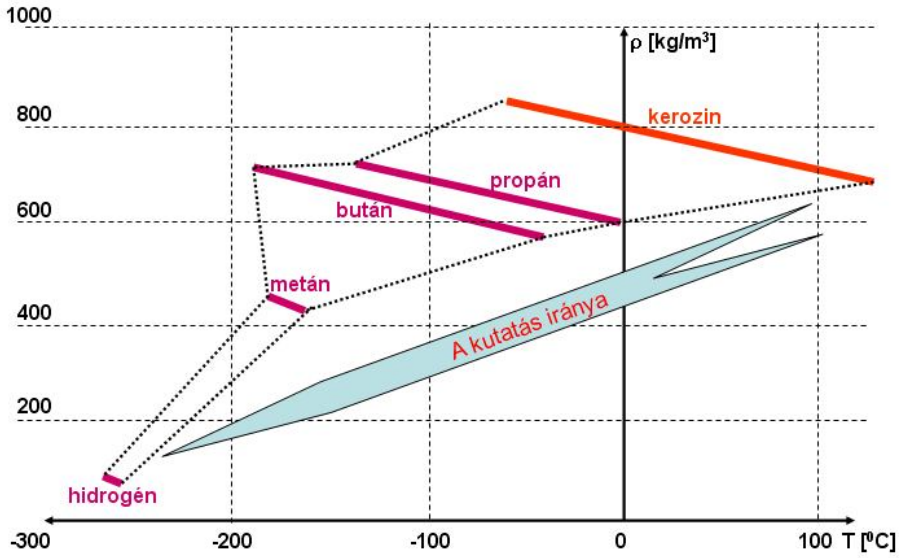
A fizikai jellemzői alapján megállapítható, hogy ennek a gáznak a tulajdonságai állnak legközelebb a repülő-benzinéhez, illetve kerozinéhoz, a vele folytatott, előrehaladott repülő-kísérleteknek dokumentáltan, kimutatható eredményei vannak. A gyakorlati alkalmazást nagymértékben segíti, hogy forráspontja sarkkörön túli regionális vonalaknál az év 10 hónapjában lehetővé teszi a zavartalan alkalmazást. Amennyiben 0,5 MPa-os túlnyomást hoznak létre a tartályban forrási hőmérséklete +45 ^{0}C-ra nő, ami járulékos energia felhasználása nélkül is biztosítja a légijármű, jelenleg használatos - akár sík lemezlapokkal határolt - fedélzeti tartályaiban történő korlátlan idejű üzemanyag tárolását, klimatizálási kötöttségek nélkül.

Tapasztalatok szerint:

- javul a felhasználás gazdaságossága, ha nem tiszta formában, hanem propánnal, hexánnal, vagy heptánnal keverve alkalmazzák;
- közepes szállító helikopter, illetve merevszárnyú repülőgép (MI-17, IL-114) bután üzemanyagra történő átállítása esetén, a módosítások következtében a tüzelőanyag-rendszer szerkezeti tömege mindössze 20÷25 kg-mal növekszik.

2.4. A kriogén gázok üzemanyagként történő gyakorlati alkalmazásának lehetőségei

Az előzőekben bemutatott cseppfolyósított gázok fizikai, termodinamikai jellemzői a 1. táblázatból ismerhetőek meg. Ezek közül is döntően az alkalmazhatóság hőmérséklete és termikus intervalluma (8. ábra) alapvetően meghatározzák a kutatás és a várható alkalmazás gazdaságosságát (3. táblázat), ezen keresztül bevezethetőségének idejét, kronológiai sorrendjét.



8. ábra [saját a 15. alapján]

A fejlesztés időszakai	4.	3.	2.	1.
Üzemanyag	Cseppfolyósított			Normál
	LH_2	LCH_4	LC_3H_8	C_4H_{10}
Viszonylagos költségek (kerozint egységnyinek tekintve)				
Egységnyi hő előállítása	10÷15	1,2÷1,6	0,6÷0,8	0,5÷0,6
Repülőtéri infrastruktúra	>100	~6	2	1,3
Az eredeti sárkányból és rendszereiből az átalakítás után megmaradhat [%]				
- teherviselő elemek	10	50	50	100
- tömítő elemek	0	20	21	100
- hőszigetelés	10	50	50	50
A hajtómű átalakítás szükséges mértéke				
- hajtómű	Új létrehozása szükséges		nagymérvű átalakítás	kisebb módosítás
- üzemanyag tartály	létezik már prototípusa			készen van
- üzemanyag rendszer	létezik prototípusa		átalakítás	kisebb módosítás
Légkondicionáló rendszer	Kutatások szükségesek		Bizonyított magas hatékonyság	
Földi infrastruktúra	Kutatások szükségesek			Rendelkezésre áll szériában
Ipari előállítás	Új üzem építése szükséges		Létező üzem átalakításával	Megoldott
Gyakorlatban létező üzem-anyag (orosz)	?	ACKT-M	ACKT-K	ACKT, ACKT-Б
A fejlesztés feladatai	Szűk, alacsony hőmérséklet-tartományban a cseppfolyós halmazállapot stabil fenntartása		További kísérletek cseppfolyós hal-mazállapotban	gáz halmaz-állapotban

3. táblázat [15. alapján]

Az árakat tekintve, a jelenlegi technológiákkal, egységnyi energia tartalmat figyelembe véve, az LH_2 ára 10÷15-szörösse a kerozinénak, ami – előrejelzések szerint - leghamarabb 2010 után csökkenhet kismértékben, de ~2030-nál előbb nem közelítheti azt. Valószínűsíthetően, ennek oka sem elsődlegesen a cseppfolyósított hidrogén előállítási

költségeinek viharos csökkenése, hanem a kerozin árának számottevő növekedése lesz. Amennyiben e tendenciák reálisak, úgy 2050 után a kriogén gáz ára, kevesebb, mint fele is lehet a jelenleg használatos üzemanyagokénak.

Természetesen, az egyes megoldások bevezethetőségének költségeit - az üzemanyag ipari előállítási árán kívül - a repülőtereken történő tárolás, tisztítás, továbbítás, az oda történő, illetve belső szállítások, a légijárműveken belüli tárolás, ülepítés, szűrés, továbbítás, adagolás, az elégetésre alkalmassá tétel konstrukciós biztosításának anyagi ráfordításai nagymértékben módosítják (gyakorlatilag növelik!). Valójában a hidrogén (metán) tartós tárolására, továbbítására szolgáló tartályok, csővezetékek anyagának megtalálása, létrehozása - a fémes anyagok ezen a tartós hőmérsékleten bekövetkező ridegedése miatt – még számos kihívást tartalmaz a konstruktőrök számára. Hasonló gondot jelent a mozgó alkatrésze – mindenek előtt a nagy nyomáson működő szivattyúk, munkahengerek – kenésének, tömítésének folyamatos, meghibásodás-mentes biztosítása.



9. ábra [17.]

Az összehasonlító tesztrepülések eredményeit a 4. táblázat tartalmazza. A külső függesztésű, két darab 1800 literes gáztartály miatt megnövekedett homlokellenállás a helikopter teljes légellenállását 3%-kal, üres tömegét 160 kg-mal növelte, hasznos terhelhetőségét 55 kg-mal csökkentette, ami Ghaszn = 1550 kg = const összehasonlító terhelés esetén 35 km-rel (~5,5 %-kal) kisebb hatótávolságot eredményezett.

A gáz, kerozinét meghaladó hőfejlesztő képessége miatt a MI-8MTG óránkénti és kilométerenkénti üzemanyag-fogyasztása is egyaránt ~2 %-kal csökkent (No 5. és 6.). Ennek is következménye, hogy a MI-8MTG, 1800 literes gáztartályok miatt 738 km-re növekedett hatótávolságát, amit a kerozinnal működő helikopter csak 260 kg plusz üzemanyag, felvételével képes elérni (ld. 4. táblázat 7. oszlop).

A helikopterekkel folytatott komplex kísérleti repülések eredményei alapján a gáz üzemanyagra állítottak át néhány, belföldi, regionális légiszállításban használt IL-114-es merevszárnyú repülőgépet is (10. ábra). A tesztek együttes tapasztalatai egyértelműen igazolták, hogy ebben a kategóriában a propán (-bután-stb.) gáz-üzemanyag keverék(ek)re történő áttérés nem rontja a légijárművek gazdaságossági-hatékonysági jellemzőit.

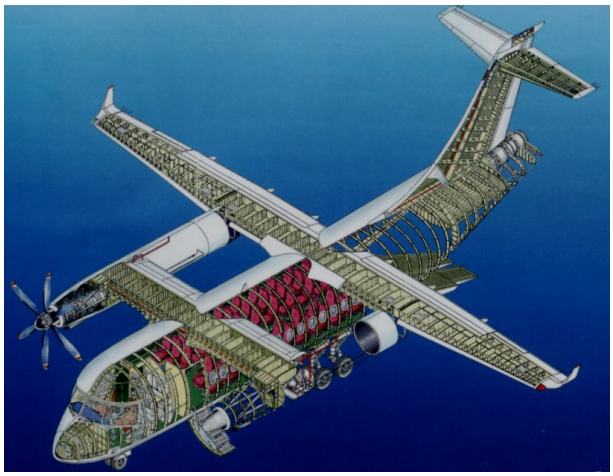


10. ábra [17]

N°	Vizsgált jellemző	MI-8MT bázis	MI-8MTG gáz üzemanyaggal			MI-8MT +260 kg kerozinnal
			L=const (640 km)	G_{terh}=const (1550 kg)	teljes feltöltés	
1.	$m_{norm,\ felszálló}$ [kg]	11100	11130	111130	**11130**	11100
2.	$m_{üres}$ [kg]	7523	7683	7683	**7683**	7623
3.	müza, felszálló [kg] - kifogyasztó tartály: - főtartály: - póttartály:	2027 345 1682 -	1988 345 1643 -	1897 345 1552 -	**2241** **345** **1896** **-**	2287 345 1682 260
4.	Üza. fogyasztás [kg] H=const esetén	1682	1651	1560	**1904**	1941
5.	Óránkénti üzemanyag fogyasztás [kg/ó]	605	593	593	**593**	605
6.	Kilométerenkénti üza. fogyasztás [kg/km]	2,63	2,58	2,58	**2,58**	2,63
7.	Utazó sebesség [km/ó]	230	230	230	**230**	230
8.	$H_{max.\ stat}$ [km]	4	4	4	**4**	4
9.	Hasznos terhelés [kg]	1550	1495	1550	**1206**	1191
10.	Repülési távolság [km]	640	640	605	**738**	738

4. táblázat [17.]

A kísérletek további eredményeként megkezdték a teljesen gázüzemű TU-156-os légcsavaros-gázturbinás repülőgép tervezését (11. ábra). Oroszországon és a repülőipari nagyhatalmakon kívül, intenzív kutatás, fejlesztés folyik a közel-keleti olajkitermelő országokban is. Ezeknél természete-sen magas prioritást kapott a hagyományos kerozinokkal lehetőleg magas arányban keverhető szintetikus összetevők és cseppfolyósított gázok felfedezésének és előállításának igénye. Ez és a bőséges anyagiak (is) katalitikusan hatottak a kutatások eredményességére.



11. ábra [18.]

2009-ben, a Qatar Airways egyik - két, Rolls Royce Trent 556, kétáramú, gázturbinás hajtóművel felszerelt - Airbus A340-600-asa, repülőgépe - első kereskedelmi légijárműként a világon - földgázból előállított üzemanyag keverékkel repült Londontól Doháig. A Shell fejlesztett ki és gyártotta az 50%-ban szintetikus Gas to Liquids (GTL) cseppfolyósított gázt, valamint 50%-ban hagyományos olajalapú kerozint tartalmazó üzemanyagot. Elégetése során kevesebb kéndioxid és más káros anyag kerül a levegőbe, mint tiszta kerozin elégetésekor, így a levegőt is kevésbé szennyezi.

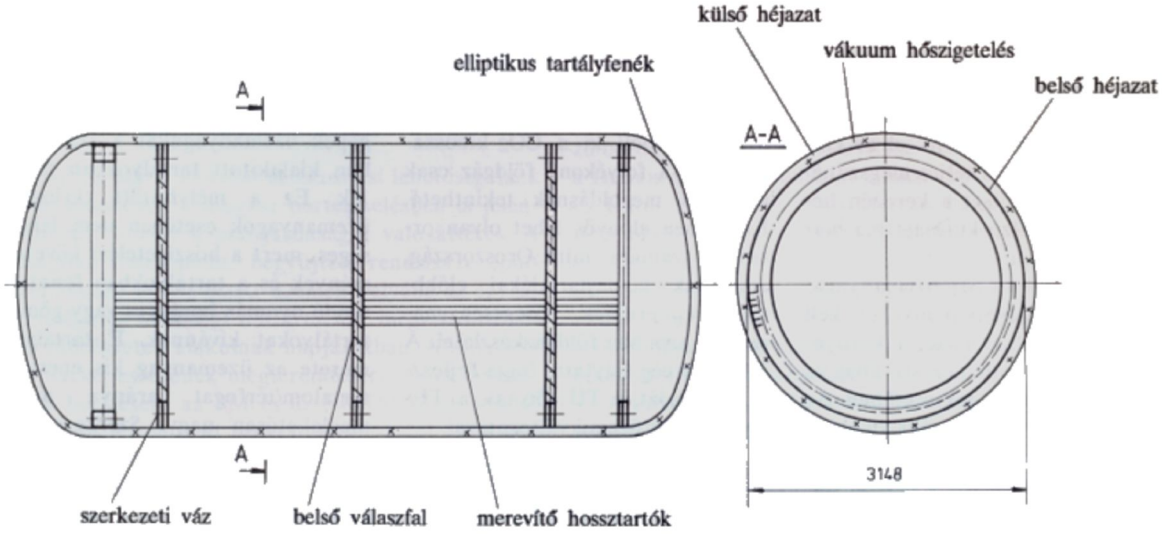
A hagyományos üzemanyag és GTL elegyének új neve GTL Jet Fuel lesz. Ez a repülőút volt az utolsó lépcsője annak a több mint két éve zajló tudományos kutatásnak, melyet az Airbus, a Qatar Airways, a Qatar Petroleum, a Qatar Science & Technology Park, a Rolls-Royce, a Shell és a WOQOD konzorciuma folytatott a GTL Jet Fuel használatának előnyeiről a kereskedelmi repülésben. A munka java része a Qatar Science & Technology Parkban folyik Dohában. Az együttműködésnek köszönhetően Katar lehet majd a világ vezető GTL kerozin-előállítója 2012-től: ekkor kezdik meg az üzemanyag kereskedelmi előállítását.

2.5. Alacsony hőmérsékletű kriogén repülő-üzemanyagok hatása a tüzelőanyag rendszer és a sárkányszerkezet kialakítására

2.5.1. Fedélzeti gáztartályok és csövek

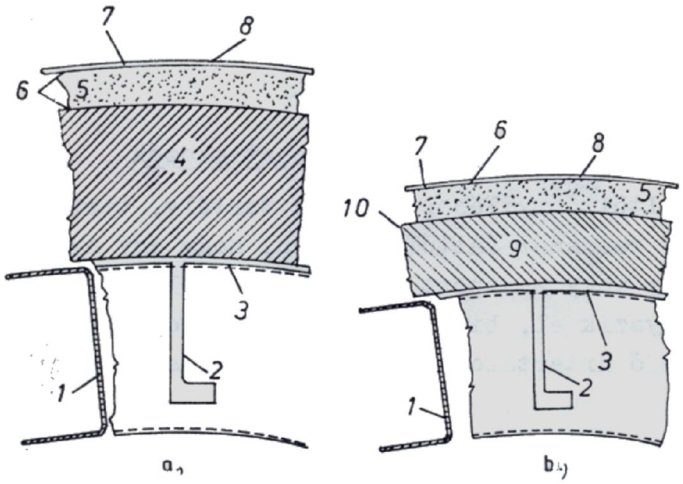
A cseppfolyósított gázok tárolása alacsony hőmérsékleten és/vagy magas nyomáson történik. Így a tárolásra alkalmas *tartály* (12. ábra):

- lényegesen szilárdabb konstrukció szükséges mint a hagyományos kerozin tároló tartályok, a reá ható esetenként jelentős nyomáskülönbségek miatt aminek elviselését az alacsony hőmérsékleteken (t<100 0C) bekövetkező szerkezeti anyag ridegedés csak nehezíti;
- nagyobb túlnyomások (Δp>3 bar) esetén tartályformaként nem alkalmazható - a sárkány szabad belső tereit optimálisan kitöltő – bonyolult térbeli alakzat, csak gömb, vagy henger jöhet számításba;
- a folyékony gáz alacsony hőmérsékletének fenntartására vastag hőszigetelő réteg(ek)kel kell bevonni, illetve párolgásának (térfogat növekedésének) megakadályozására többnyire aktív hőszigetelést is szükséges alkalmazni. Utóbbiak működtetése rendszerint járulékos energia felhasználást is igényel.

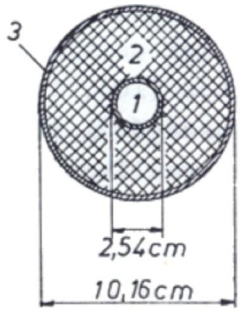


12. ábra [7]

Tapasztalatok szerint kétféle megoldású tartály-hőszigetelés mutatkozik alkalmazhatónak és továbbfejleszthetőnek cseppfolyósított gázok tárolására (13. ábra). Mindkét változatot keretszerkezethez (1) rögzítik, falukat (3) hosszmerevítők (2) erősítik.



13. ábra [7. p. 160.]



14. ábra [7. p. 174.]

A vaskosabb, súlyosabb konstrukciót eredményező megoldásnál (13. a. ábra) a tartály falára széles, zárt pórusú fenoplaszt réteget (4) rögzítenek. Ebben a 0,127 mm vastagságú MAAMF, többrétegű alumíniumszálas szövetrétegek (6) között hajlékony, porózus fenoplaszt (5) található, amit réteges kompozitból (kevlarból) (7) készült bevonat fed. Ezt viszont már a törzs borítása (8) követi. A hőszigetelés hatásfokának javítására a porózus hőszigetelő rétegbe N2 gázt vezetnek (amiből, számítások szerint 9000 km megtételéhez 90 kg felhasználása szükséges!).

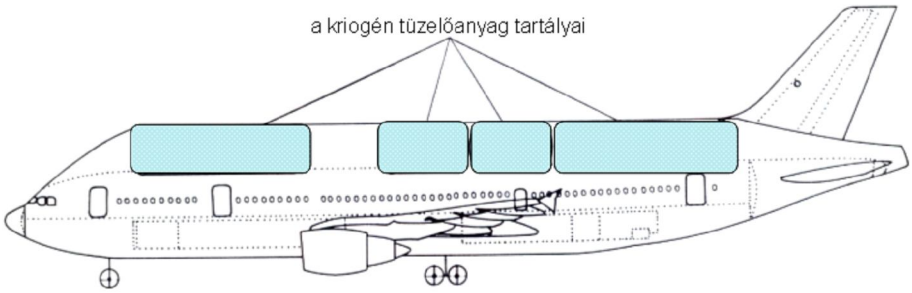
A drágább, könnyebb és vékonyabb kialakításnál (-28 mm) (13 b. ábra) hőszigetelőként vákuumot (9) ($p \approx 13$ Pa) alkalmaznak, melyet vákuum-szivattyú tart fenn. A vákuumteret a N2-vel hűtött, hajlékony fenoplaszt rétegből (5) a 0,127 mm vastagságú bor-szilikát zóna (10) választja el. (A számozás és funkció azonos a két ábrán).

Számottevően megnöveli az üzemanyagcsövek (14. ábra) súlyát és szükséges térfogatot, amennyiben cseppfolyósított gázokat szállítanak bennük. Például a cseppfolyós H2 továbbítására szolgáló 2,54 cm átmérőjű 0,4 mm falvastagságú csövet (1) olyan vastag alumíniumborítású (3) fenoplaszt (2) szigetelő réteggel vonják be, hogy átmérőjét négyszeresére (10,16 cm), így keresztmetszetének felületét tizenhatszorosára növeli.

Mivel az alacsony hőmérsékleten cseppfolyósított gázok többségének sűrűsége alig fele, a hidrogén esetében mindössze 1/11÷1/12 része a kerozinokénak, ezért, ekvivalens energia-mennyiség tárolására, - figyelembe véve magasabb égéshőjüket is - a számítások eredményei azt mutatják, hogy:

- az ilyen repülőgépek szárnya – a vastag hőszigetelő réteg szükségessége és az aerodinamikai követelmények miatt - nem vehető figyelembe a tüzelőanyag tárolására;
- csak a törzsben alakíthatóak ki tüzelőanyag tartályok. Az ekvivalens energia-mennyiséget biztosító térfogata - a hőszigetelés térfogatigényét is figyelembe véve, pl. LH_2-nél - 3,8÷4,2-szerese a kerozinénak. Ezek, nagyobb nyomás esetén - szilárdsági megfontolásból - csak hengeresek, vagy gömb alakúak lehetnek. Így, magas, széles törzsű sárkányok kialakítása szükséges (14. ábra).

A 15. ábrán egy ismert, jelenleg is széles körben használatos, korszerű közforgalmú utasszállító repülőgép gázzal üzemelő változatának kontúrrajza látható, utastér felett elhelyezett gáztartályokkal. Mivel az utastér alatti törzstérfogatot a poggyász- és teherszállításra szolgál, így a gáztartályok csak a törzs felső, járulékosan megnagyobbított részébe építhetőek be.

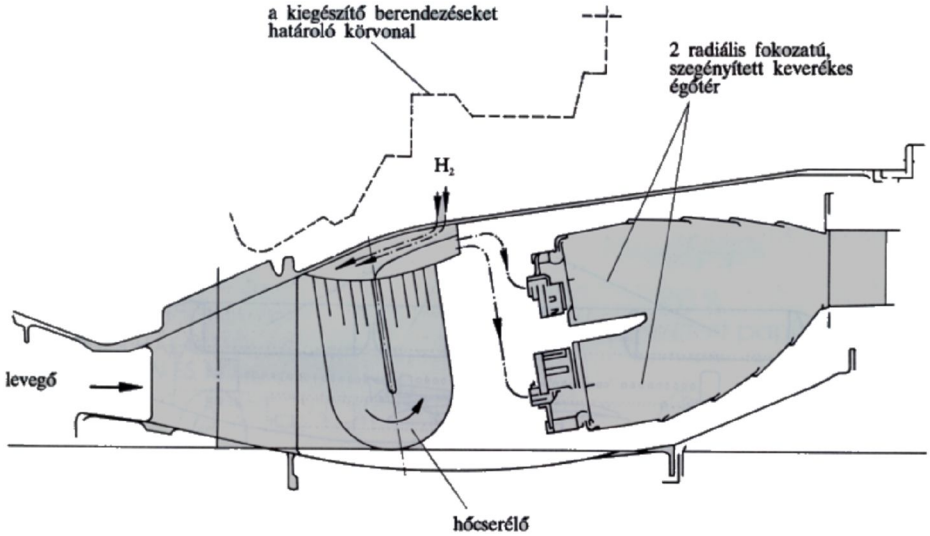


15. ábra [7.]

Az üzemeltetés során további lényeges különbség, hogy e a gázok nagy része (pl. LH2, LCH4) – külön energia betáplálása nélkül - cseppfolyós állapotban, a repülést követően nem maradhatnak a tartályokban.

3.5.2. Hajtóművek

A jelenleg ismert gázturbinás hajtóművek működési elve megfelel, a gázneműé visszamelegített tüzelőanyagokkal történő működtetésre. Gyakorlatilag a teljes hajtómű-elrendezés változatlan maradhat (20. ábra), de az égőteret teljesen át kell alakítani a hidrogén (metán) előnyös tulajdonságainak hasznosítására. Az alapvető konstrukciós törekvés a nitrogénoxidok kibocsátásának csökkentése.

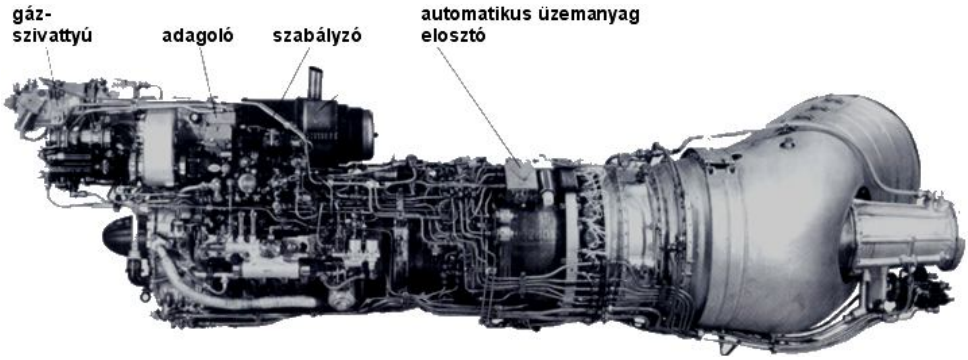


16. ábra [7.]

Az égőtér a kerozin-üzeműhöz képest jelentősen megrövidíthető, ami lehetővé teszi a járulékosan szükségesé váló hőcserélő beépítését, ami azután visszaalakítja a cseppfolyós hidrogént (metánt) gázzá az égőtérbe történő betáplálás előtt. A szükséges üzemanyag-mennyiség pontos szabályozása viszont még néhány megoldandó kérdést felvet.

Az alacsony hőmérsékletű cseppfolyós gázokkal jól hűthetők az olajrendszer, a légkondicionáló rendszer, a turbinalapátok, a sárkány egyes elemei, miközben az égőtérbe táplált üzemanyag is előmelegíthető.

Jól láthatóan, a lényegesen magasabb üzemi hőmérsékletű propán-bután üzemanyaggal működő TV-3 hajtómű (17. ábra) szerkezeti kialakítása a kerozin üzeműhöz képest, érdemben nem változott.

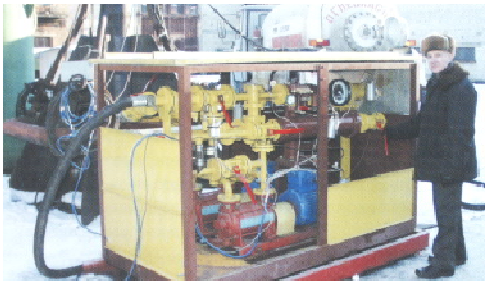


17. ábra [17.]

3.6. A repülőtéri kiszolgálás eszközei és az infrastruktúra

A cseppfolyósított gázokkal üzemelő légijárművek tüzelőanyaggal történő feltöltése (leszívása) különbözik a benzinnel és kerozinnal üzemelő rendszerekétől. A töltő–leszívó berendezés hermetikusan és hőszigetelten csatlakozik a repülőgép farokrészhez. A gépjármű, a földalatti tápcsatornában levő vezetékek és a repülőgép töltőcsonkja összekapcsolására szolgál. Ezt megelőzően, a gépkocsi saját semleges gázrendszeréből héliummal átfúvatja az összekötő csöveket és csatlakozókat a repülőgép tüzelőanyag-rendszerébe a levegő, O_2 tartalma bekerülésének megakadályozására. (Üres tartályok feltöltése ugyancsak a teljes rendszer héliummal történő átfúvatásával kezdődik).

Amennyiben a repülőgép hosszabb ideig tartózkodik az állóhelyen, a cseppfolyós H_2 gyors felmelegedésének meg-akadályozására vákuum-szivattyúval a gázneművé vált felmelegedett hidrogént elszívják és helyére a tartályok folyadék feletti terébe hűtöttet vezetnek. Amikor a feltöltött gép nincs a repülőtéri táprendszerre csatolva, a tüzelőanyag-rendszer biztosító szelepei lehetővé teszik a felmelegedett, gáz-halmazállapotúvá vált H_2 távozását a szabadba.



18. ábra [18.]



19. ábra [18.]

A hidrogén tárolása is új technológiákat igényel, tárolható például kriogén folyadéktartályokban, nagy nyomású gázként vagy szilárd formában. Szállítására vezetékrendszerek már épültek Észak-Amerikában, Belgiumban és Hollandiában, de még gondot okoz, hogy az anyagok szerkezete ridegebbé válik tőle, elvesztik szívósságukat, valamint meg kell oldani, hogy a hidrogén ne diffundáljon el belőlük. Közúton és vasúton is szállítható. A hidrogén üzemanyaggal működő járművekhez speciális üzemanyagtöltő állomásokat kell létesíteni, ami komplikált műszaki rendszert jelent - erre irányult az Európai Unió FP6-os (Framework Program) egyik kezdeményezése.

A propán, bután repülőtéri tárolása, szállítása, szivattyúzása nem jelent különösebb technikai kihívást (18. és 19. ábra)

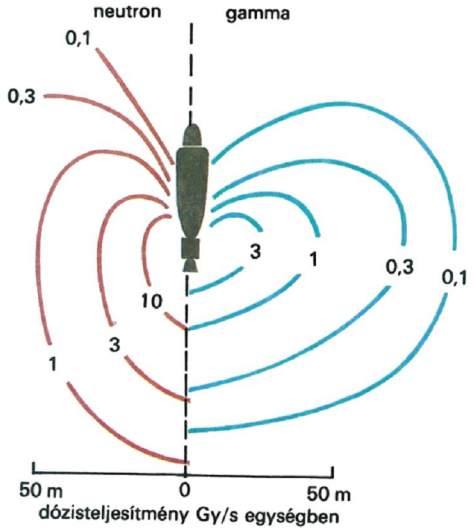
4. AZ ATOMENERGIÁVAL MŰKÖDŐ REPÜLŐGÉPEK LÉTREHOZÁSA

Gyakorlatilag az ’50-es években megjelent az igény a nukleáris energia repülőgép üzemanyagként történő hasznosítására. A számításba vett urán 233-as, 235-ös, a plutónium 239-es izotópjának alkalmazásával, egységnyi tömegből milliószor nagyobb energia szabadítható fel, mint bármely más tüzelő-anyagból. Környezetvédelmi és biztonsági szempontból azonban ennek napjainkig sincs reális perspektívája.

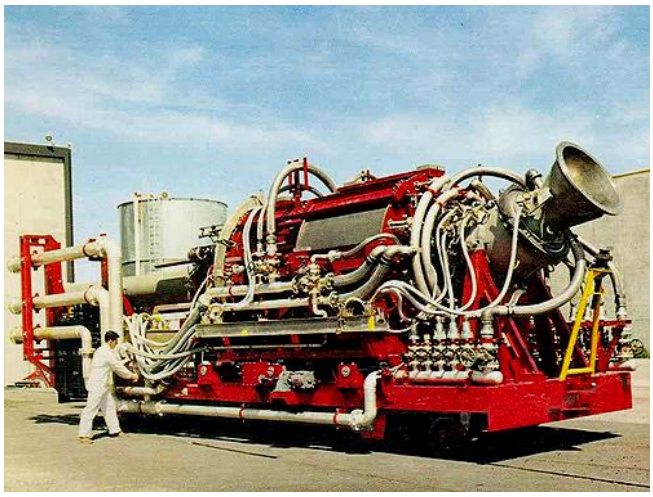
Bármilyen működési elvű nukleáris hajtóművet alkalmaznak, minden körülmények között gondoskodni szükséges a földi és hajózó személyzet sugárvédelméről. Például a 20. ábrán látható hajtóműtől 50 méterre, külön védelem nélkül, néhány másodpercen belül már halálos dózist (5 Gy, korábban 500 rad) lehet kapni.

Nagyobb reaktoroknál a káros sugárzás (adott helyen a neutron és a gamma sugárzás összegét) kell figyelembe venni. Ez, rendszerint vastag védőfalak és/vagy a reaktor és utastér egymástól nagy távolságra történő elhelyezését feltételezi. A sugárzás árnyékolására a célszerűen elhelyezett LH hajtóanyag is alkalmas lehet.

A nukleáris meghajtású repülőgép sugárhajtóműve - elképzelések szerint - több mint háromszoros hangsebességű repülést is lehetővé tehetne, gyakorlatilag korlátlan hatótávolsággal. A hajtóművében a beszívott és sűrített levegőt nem kerozin, esetleg egyéb fosszilis, vagy más kémiai tüzelőanyag, hanem egy atomreaktor hevítette volna fel, így hozva létre a tolóerőt. Egy ilyen, a ’60-as években fejlesztett 500 MW teljesítményű kísérleti reaktor (Tory) látható a 21. ábrán.



20. ábra [Makra: Űrhajózás holnapután GONDOLAT 1986. p. 93.)



21. ábra
[Laczkó M. B.:Nukleáris meghajtású repülőgép hozta volna el a világvégét - Háború Művészete www.Art of WAR *Publikálva: 2008-11-11 19:17:00*]

5. NAPENERGIA A REPÜLÉSBEN

A valóban környezetkímélő energiák egyike a napenergia, amely a napban lejátszódó magfúziós folyamatok során felszabaduló energia. Hasznosíthatóságát alapvetően az indokolja, hogy a napból a földfelszínre körülbelül 70÷80 MW/m^2 energia érkezik. Az energia sűrűség a föld atmoszférájának szélén átlagosan 1367 W/m^2. Ez azt jelenti, hogy éven-ként megközelítőleg 219 milliárd GWh sugárzási energia éri el a földfelszínt, ami 2500-szorosa napjaink teljes energia szükségletének. Hozzávetőleg három óra napsugárzás képes fedezni földünk éves energia szükségletét.

A légkörben jelen lévő vízpára és jég kristályok elnyelésének eredményeképpen a földfelszínt ténylegesen elérő sugárzási energia 1000 W/m2, sík felszínen, a nap legmagasabb állásában. A beeső sugárzási energia a légköri körülmények függvényében 50 W/m2-től (erősen felhős idő) 1200 W/m2-ig (optimális felhőzet) változik. Európában a napi átlagos sugárzási energia 2,2 ÷4,8 kWó/m2nap. Jelenleg hasznosítása elhanyagolható, pedig számos kedvező tényező szól mellette:

- mindenki számára könnyen elérhető, tiszta, környezetkímélő energiaforrás;
- még évmilliókig rendelkezésre áll, kíméli a nyersanyagkészletet;
- nem kell szállítani, hozzájutásához nem kell költséges közműhálózat;
- átalakítási, felhasználási költségei minimálisak.

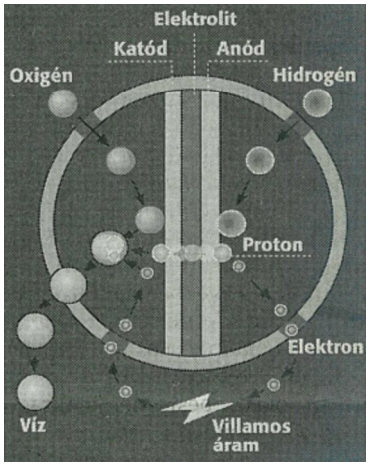
A cellákból felépülő napelemek működésének alapja, hogy a fénysugárzás fotonjai kimozdítják a félvezető elektronjait a kötéseikből, így elektron-lyuk párok keletkeznek, ezt az elektrontöbbletet pedig elektromos vezetőkkel lehet a napelem felületéről elvezetni a fogyasztókhoz, vagy az akkumulátorokhoz. Egy fotoelektromos cella teljesítményét a típusa és mérete a szolár cella anyagának, a fény intenzitása, a fény hullámhossza határozza meg, összehasonlításukra a áramerősség/felületegység (A/cm2) mérőszám ad felvilágosítást.

A szolár cellákat több különböző méretben és formában állítják elő, a felhasználási területüknek megfelelően. A kisebb, bélyeg méretűektől, a néhány 100 milliméteresig. A cellák összekapcsolásával szolár-modulokhoz jutunk. A napelemes rendszer a szolár cellákon kívül tartalmazza még az elektromos csatlakozásokat, az illesztési eszközöket, teljesítmény szabályozókat, és az akkumulátorokat Egy egyszerű cella körülbelül 0,5 V-ot tud előállítani. Ezeket párhuzamosan és/vagy sorba köthetőek, ezáltal nagyobb áramerősség/feszültség érhető el.

A repülőgépen történő hasznosításnak jelenleg két meghatározó korlátja van:

- a egységnyi felületen előállítható feszültség-áramerősség és a könnyűépítés elvének való együttes megfelelés;
- korlátozottan napfényes, vagy napfénymentes időszakban az energia megbízható pótlása tartalékolt készletekből.

A felsoroltak repülőeszközön történő alkalmazása, az elektromos energia, jelenlegi akkumulátoroknál lényegesen kisebb szerkezeti tömegű és magasabb hatásfokú tárolását, illetve át- (oda-vissza) alakítását feltételezi. Ennek egy lehetséges és ígéretes megoldása a hidrogénnel működő üzemanyagcella (22. ábra)



22. ábra [10.]

Katalizátor segítségével a hidrogén alkotóelemeire, protonra és elektronra bomlik. Az üzemanyagcellában a kémiai folyamatot a levegő oxigénjétől egy elektrolit réteg zárja el, amely csak a protonokat ereszti át, az elektronokat nem. A protonok azonban csak elektronok jelenlétében tudnak reakcióba lépni az oxigénnel. A reakció által felszabaduló energia elegendő ahhoz, hogy elektronokat húzzon át a túloldalra, ezáltal villamos áram jön létre, valamint víz keletkezik.



23. ábra

A felsorolt műszaki kérdések – legalább részleges - megoldására építette a NASA, a ’90-es évek második felében, a 23. ábrán látható napelemekkel borított szárnyú kísérleti repülő-

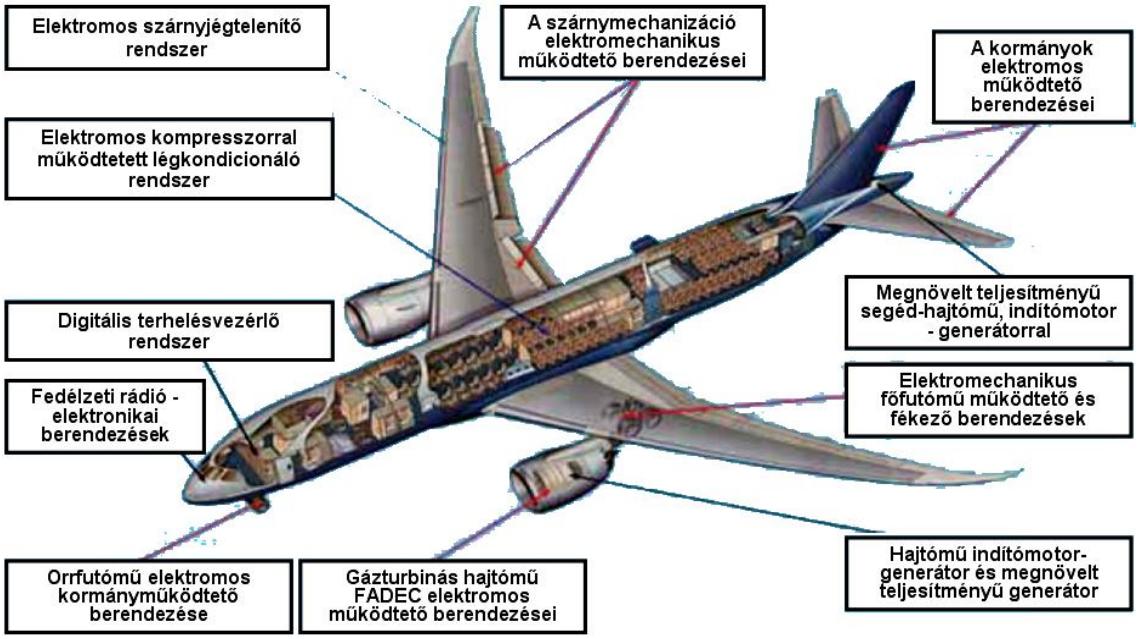
gépet, mely klimatikus viszonyoktól (tlev, Hrep, ρlev, stb.) függetlenül volt képes napokig H>20 km-es repülési magasságban tartózkodni. Nyolc darab, egyenként néhány száz Watt teljesítményű hajtóműve csak a sárkány-szerkezet önsúlyának levegőben tartására volt alkalmas, érdemi hasznos terhelhetőség nélkül.

Napjaink műszaki színvonalán már olyan villamos meghajtású robot-repülőgép építhető szériában („Global Observer"), amelynek fedélzeti táprendszere alkalmas a hajtóművek, vezérlő és hírközlő rendszerek, valamint a felderítő konténer egyidejű működtetésére.

6. A „TELJESEN VILLAMOSÍTOTT" REPÜLŐGÉP

Az alternatív hajtómű üzemanyagok kutatásával párhuzamosan, a '70-es évektől több ország kutatóintézetében vizsgálták, vizsgálják a rendszeren belüli szükségszerű energiaátalakítások hatékonyságát, ennek részeként a meglévő gázturbinás hajtóművek lényegesen hatékonyabb működtetésének lehetőségeit, estleges részleges kiváltásuk módját, (pl. villanymotorral).

Ennek időben első eredménye, a számítástechnika fejlődésével, a repülőgépek komplex automatikus vezérlő rendszerének részeként létrehozott, - a hidromechanikusat teljesen kiváltó – digitális hajtómű vezérlés FADEC (Full Authorithy Digital Engine Control), ami alkalmas valamennyi üzemmód optimalizálásával a toló-/vonóerő növelésével egyidejűleg, számottevő üzemanyag fogyasztáscsökkentésre is.



24. ábra [14.]

A gazdaságossági kutatások már a '70-es évek végén azt mutatták, hogy a - működtetésükhöz a hajtóművektől jelentős, (nagy szállító repülőgépek esetében akár több ezer kilowatt teljesítményt elvonó - segédenergia és fedélzeti légkondicionáló rendszerek hatékonysága még nagymértékben javítható, optimalizálható. Ennek okai:

- a fedélzeten segédenergiaként többnyire együttesen alkalmaznak hidraulikus, pneumatikus és villamos berendezéseket, melyek közül az első kettő hatásfoka általában lényegesen alacsonyabb az utóbbinál. A különböző rendszerek együttes működésekor a meghibásodás valószínűsége, az üzembentartás költségei is magasabbak, mint homogén energetikai megoldás esetén;

- rendszerint valamennyi rendszer (kényszer-) meghajtása a hajtómű segéd-berendezésházáról biztosított;
- a fedélzeti légkondicionáló rendszerek – teljesítményigényükön túl jelentős levegő mennyiséget is elvonnak a hajtómű kompresszorfokozatától, ami rontja annak hatásfokát.

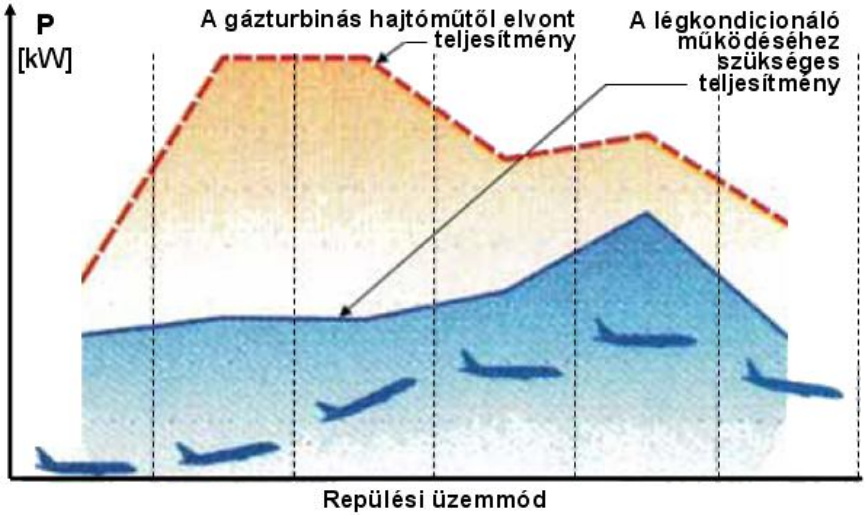
Az orosz és nyugati kutatóintézetek előzetes vizsgálatai egybehangzóan bizonyították, hogy a különböző fedélzeti rendszerek homogén, lehetőség szerint a legmagasabb hatásfokú elektromos, energiával történő táplálása - mindenek előtt nehéz szállító repülőgépek esetében - számos gazdaságossági, hatékonysági előnnyel jár. Ezek közül a legfontosabbak:

- üzemanyag megtakarítás 8÷12 %-os, a felszálló tömeg 6÷10 %-os, a közvetlen üzemeltetési költségek 5÷10 %-os, az élettartam költségek 3÷5 %-os, műszaki kiszolgálási idő 4÷4,5 %-os csökkenése. csökkenése;
- az egy meghibásodásra eső repült idő 5÷6 %-os növekedése;
- A felsorolt kedvező adatok, kisebb geometriai méretű és tömegű a repülőgépek esetében arányosan csökkenek.

A teljesen villamosított repülőgép kialakításának egymásra épülő programlépései, (’70-es évek végétől: AEA - All Electric Aircraft, ПЭС - полностью электрический самолет, a ’90-es évektől MEA – More Electric Aircraft, 400 millió € ráfordítással, 2002÷2006 POA – Power Optimized Aircraft, 100 millió € költséggel, melynek vezető résztvevői a Thales, Goodrich, Rolls-Royse, Hispano Suiza, stb.) a 24. ábrán látható – hagyományosan, többnyire más energiaforrásról táplált – rendszerek 100 %-os elektromos működtetését célszerűsíti.

A felsorolt és az ezeket kronológiailag követő MOET (More Open Electrical Technologies) program több eredménye már visszatükröződik a különböző rendeltetésű, A-380, B-787, F-35 legújabb fejlesztésű, polgári és katonai repülőgépeken, de kimutatható az UAV fejlesztésekben is („Barracuda”).

A program keretei között a gazdaságosság javításának egyik meghatározó eleme a hajtómű(vek)től - alapvetően a légkondicionáló, esetenként jégtelenítő rendszer(ek) táplálására szolgáló - levegő elvonásának megszüntetése. Ez annál is fontosabb, mert a légkondicionáló működtetéséhez szükséges telje-sítmény eléri, sőt meg is halad-hatja az 500 kW-ot, ráadásul a szükséges és a tényleges elvonás mértéke a repülés különböző fázi-saiban nagymértékben eltérhet (25. ábra).



25. ábra [14.]

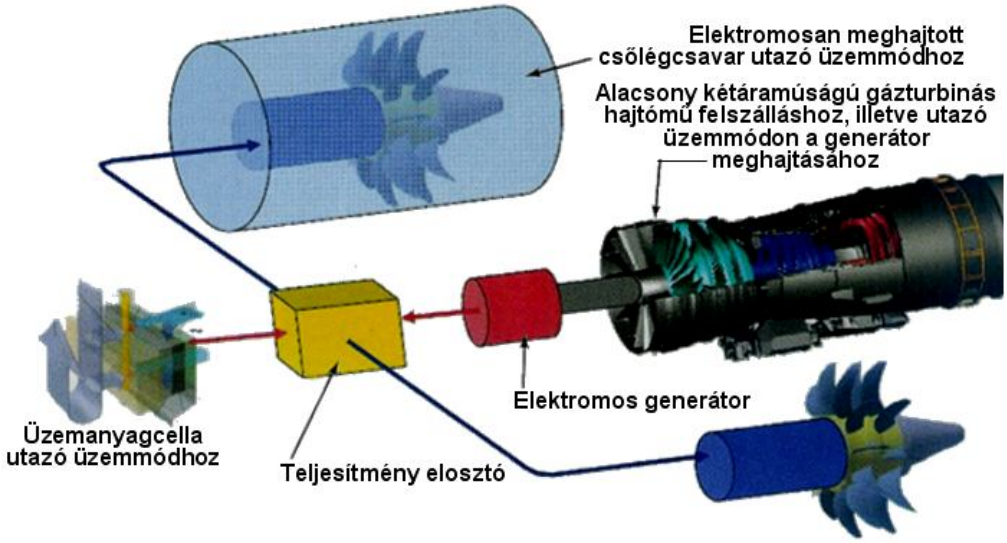
A kutatások eredményei szerint, amennyiben a légkondicionáló rendszer levegőszállítását elektromosan meghajtott, számítógéppel vezérelt kompresszor biztosítja:

- a működtetéshez szükséges teljesítmény 30 %-kal;
- a rendszer berendezéseinek és csővezetékeinek a tömege 20÷30 %-kal;
- a hajtómű(vek) üzem-anyag fogyasztása 1÷2 %-kal csökken.

A teljesen villamosított repülőgép elektromos táprendszerében, a jelenleg használatos értékekhez képest, a váltóáram feszültségét – 360÷800 Hz között változtatható frekvencia mellett - legalább kétszeresére, az egyenáramét 10÷20-szorossára (270÷540 V) szükséges emelni.

A jelenleg folyó kutatások két fontos megoldandó kérdése:

- az elsődleges kormányvezérlő rendszer hidraulika munkahengereinek kiváltása;
- a légcsavarok működtetése villanymotorral.



26. ábra [14.]

Első esetben a legnagyobb nehézség az, hogy a könnyű építés elveinek megfelelő nagy teljesítményű, minimális szerkezeti tömegű motor csak nagy, (20000÷40000 ford/perc) fordulatszám alkalmazásával lehetséges. Ennek haladó mozgássá alakítása, 1÷3 fokozatú fordulatszám-csökkentő egység (pl. bolygóműű) alkalmazásával lehetséges, így az intenzív, manőverező repülésnél szükséges gyakori, különböző irányú kormánymozgatás tartós, megbízható, késleltetés-mentes, pontos követése, nehézkes, nem éri el a hidromotorok hatékonyságát, megbízhatóságát.

A turboprop/fan repülőgépek működési hatékonyságát lényegesen növeli, a légszennyezést markánsan csökkenti a légcsavarok elektromos meghajtása, utazó üzemmódon. A gázturbinás hajtómű ennél a megoldásnál csak a felszálláshoz szolgáltatna kisegítő tolóerőt, a repülés további szakaszaiban, mint villamos erőmű meghajtóegysége működne (26. ábra). Ennek gyakorlati megvalósítása azonban, még a villamos hálózatokon belüli energia átalakítás és a megbízható tárolás hatékonyságának további érdemi javítását feltételezi.

Felhasznált irodalom

1. Ijesztőek a globális légszennyezési adatok, [origo] 2008. 09. 30., 11:28
2. Jakabffy Éva Kék bolygó, zöld jövő – mennyit érnek a megújuló energiák? www.origo.hu/tudomány, 2008. 04. 22., 8:40
3. Jakabffy Éva Kék bolygó, zöld jövő – mennyire zöldek a megújuló energiák? www.origo.hu/tudomány, 2008. 05. 02., 8:08
4. Kis kémiai szótár, GONDOLAT KIADÓ, Bp. 1972.
5. Környezetbarát energia a vízből – a jövő a hidrogéné lehet, www.origo.hu/tudomány, 2008. 06. 30.
6. Nárai-Szabó István: Kémia, MŰSZAKI KÖNYVKIADÓ, 1973.
7. Óvári Gy: Merev és forgószárnyas repülőgépek szerkezettana III. Repülőgépek rendszerei, (egyetemi/főiskolai jegyzet) KGYRMF, Szolnok, 1990. és lényegesen átdolgozott, multimediás (PDF) változata (kézirat), ZMNE RLI 2009.
8. Pesthy Gábor: Áttörés a hidrogén előállításában, www.origo.hu/tudomány, 2008. 08. 19.
9. Szenzáció, itt a repülőgép ami gázzal működik, www.hvg.hu 2009. 11. 05.
10. Új hidrogénforrás, www.termeszetvilaga.hu 2005. 06. 15.
11. Warwick, Graham: Electric Charge AWIATION WEEK & SPACE TECHNOLOGY 2010. 09. 20/27 p. 66.
12. Warwick, Graham: Fuel for Growth AWIATION WEEK & SPACE TECHNOLOGY 2010. 09. 20/27 p. 57-59.
13. www.kekenergia.hu Non-profit megújuló energiákat ismertető oldal: Kyocera japán napelemek; Napenergia hasznosítása napkollektorral, napelemmel, hőszivattyúval;
14. Вороновым, С. – Каргополцев, В. – Кутасов, В.: „Полностью электрический самолет” АВИАПАНОРАМА 2009. 03-04. p.14-17.
15. Зайцев, В.: Новое толиво для авиации АВИАГЛОБУС 2009. 07. p. 10-13.
16. Катин, Д: Работы в США по оптимизации затрат на закупку топлива для военной авиации, ЗАРУБЕЖНОЕВОЕННООВОБОЗРЕНИЕ 2008. 07. p. 46-50.
17. Мавpицкий, В. И. – Зайцев, В.: ЛТХ двухтопливного вертолета АВИАГЛОБУС 2009. 06. p. 16-17.
18. Чернышев, С. Л. – Ковалев, И. Е. – Мавpицкий, В. И.: Переход на новое авиационное топливо АВИАГЛОБУС 2009. 09. p. 24-29.
19. Цены на авиатопливо будут снижены дважды Источник: «Независимое Информационное Агентство» Опубликовано: 12.12.2008, 18:01

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Berek Tamás
berek.tamas@zmne.hu

Bodrácska Gyula
bodracska.gyula@t-online.hu

AZ ÉLŐERŐS ŐRZÉS AZ OBJEKTUMVÉDELEM ÉPÍTŐIPARI ÁGAZATÁBAN

Absztrakt

A vagyonvédelmi koncepció kialakítását követően a komplex biztonsági rendszer tervezésekor komoly elemző és értékelő munkát követel meg a védelmi alrendszerek helyes arányainak kialakítása. Az építőipari beruházásokra a nagyfokú térbeli és időbeli változások jellemzőek. A vagyonvédelem komplex rendszerében helyet foglaló élőerős védelem aránya és feladata az építkezés különböző készültségi fokozataiban eltérő. A hatékonyság szempontjából a biztonsági vezetőnek a beruházás előrehaladásával újra és újra értékelnie kell a fenyegetettségnek kitett területek veszélyeztetettségét és a főbb feladatokat. A szerzők a cikkben bemutatják az élőerős védelem kialakításának általános szempontjait, felvázolják az építőipari beruházások sajátosságait és feltárják a vagyonvédelem élőerős komponense kialakításának lényeges sarokpontjait, a humán erőforrás menedzselés egyes kérdéseivel együtt.

In order to configurate a safeguarding conception, we have to create a complex security system. We have to make a plan, the plan has to be analised and interpreted. It is especially hard and complex during safeguarding a building, the function of which is unknown. Industrial projects usually differ from what was planned both in space and in time. The proportion and the task of manpower defence in case of safeguarding can be different in any stage of a building operation. In order to be effective, security officers must again and again estimate how much endangered the safeguarded area and must promptly perform their major duties. The authors of the article introduce the general standing-points of manpower defence, the characteristics of building industrial projects. They also introduce basic points of configurating components of safeguarding manpower. They take into consideration questions about human manager.

Kulcsszavak: *építőipari beruházás, komplex vagyonvédelem, védelmi koncepció, élőerős védelem ~ construction investment, complex property protection, defense concept, manpower defence*

BEVEZETÉS

Építőipari nagyberuházások védelmének előkészítése és tervezése, valamint az ezzel összefüggő feladatok végrehajtása néhány tekintetben eltérő sajátossággal bír az objektumvédelem általános gyakorlatához képest.
A Vagyonvédelmi Nagykönyv meghatározását alapul véve az objektum ugyanis egy pontosan körülhatárolható terület, melyen felépítmények találhatóak különböző funkciókkal. A veszélyeztetettség mértékét a működés, az üzemeltetés biztonsági foka, a felhasznált különféle anyagok, technikai eszközök, információk kereslete, értéke, értékesíthetősége, a terület bűnügyi fertőzöttsége, működés rendje a napszak, az alkalmazott védelmi rendszer megbízhatósága, a beavatkozás, az elhárítás objektív- szubjektív gyorsasága, a nemkívánatos cselekmények jellege és azok területi kihatása határozza meg. [1]

Távolról megközelítve a kérdést az adott objektum veszélymentes állapotának a fenntartása a cél. Ez a veszélymentes állapot a biztonsági rendszer zavarmentes működését feltételezve – mely ideális állapotot is csak feltételezni lehet - időben állandónak tűnhet, azonban csupán látszólagos. Ez még stacioner objektum esetében sem igazolható. Minden objektum esetében az épületben végzett tevékenység, és többek között a tevékenység eszközei, a felhasznált anyagok mennyisége, értéke, veszélyessége viszonylag jól meghatározható. A veszélymentes állapot változása bizonyos tekintetben prognosztizálható többek között az objektum funkciója, a bent végzett tevékenység, az alkalmazott technológiák és anyagok ismeretében. Az építőipari projektek biztosítása során viszont a fentieken túl a biztonságot nagymértékben meghatározó tényezők folyamatos változása is tapasztalható.

A biztonság állapotát alapvetően meghatározza a veszélyeztetés és az ellene alkalmazott védelem.[2] Az objektum védelmi rendszerének felépítésekor fel kell tudni ismerni a biztonság állapotát befolyásoló veszélyeztető külső és belső tényezők jellegét, és azok értékelését követően meg kell tervezni az azokra adott válaszlépéseket, illetve a védelem felépítését.

A VAGYONVÉDELMI RENDSZER TERVEZÉSÉNEK ELŐKÉSZÍTÉSE

Az építőipari projekt környezetéből eredő veszélyeztetettség feltárása és elemzése során meg kell állapítani a védelem tárgyát és meg kell határozni a veszély forrását, és ezek ismeretében kell megtervezni és kiépíteni a védelmi rendszert, olyan körülmények között, melyben tételesen nyilván ritkán lehet megjelölni a védendő értékeket.

Az építőipari nagyberuházást biztosító vagyonvédelmi cég biztonsági stratégiájának felépítése, a vagyonvédelmi rendszer tervezése szempontjából lényeges a későbbi feladat-végrehajtás helyszínének megelőző tanulmányozása, majd ezt követően a felmért paraméterek teljes körű kiértékelése.

A kivitelezés helyszínére vonatkozóan számos biztonsági szempontból lényeges adatra fény derülhet a kivitelező vállalat nyitó kooperációján, ahol a leendő alvállalkozók megismerhetik a projektet melynek térképén, rajzain pontosan látható annak földrajzi elhelyezkedése, tájolása.

Ezen a nyitó kooperáción a biztonsági szolgálat szakmai vezetője is kézhez kapja az anyagot. A térképek, vázlatok és látványrajzok szakmai tanulmányozása abból a szempontból is hasznos, hogy a beruházás egyes későbbiekben felmerülő, a biztonsági állapotot alapvetően meghatározó, vagy megváltoztató körülményt az előrelátó biztonsági vezető felderíthet, megóvva magát az esetlegesen 15-20 hónap multán, az építkezés adott fázisába lépő beruházáson felmerülő kínos meglepetésektől.

Elsősorban a megrendelőnek kell megfogalmazni a biztonság iránti igényét és a tervezés előkészítésének folyamatában tárgyalások során kell körülhatárolni azt, hogy erre mennyi pénzt kíván áldozni. Ebben a fázisban a biztonsági vezető, illetve a megrendelő közötti együttműködés rendkívül fontos, hiszen a megrendelő biztonság „mértékére" vonatkozóan megformált igénye mögött a legritkább esetben a valós szükségletei, hanem inkább financiális megfontolások állnak. A védelem alulbiztosítása vagy éppen túlbiztosítása ugyanakkor a védelem tervezésekor hónapokkal később jelentkező problémákat generálhat.

Természetesen a helyszíni tájékozódást, a terepszemlét nem válthatja ki a legkörültekintőbb irodai projektfelmérés sem, ahol a legfontosabb szempontokat a helyszínen kell megvizsgálni vagyonvédelmi, rendészeti szempontból.

A helyszíni szemle során számos, biztonsági szempontból lényeges rejtett tényező deríthető fel. Az bárki számára nyilvánvaló lehet, hogy a beruházás helyszíne és környezete vonatkozásában lényeges különbségek jelentkeznek aszerint, hogy az urbanizált, vagy külterületi jellegű. Ha városban épül az épület, gyakorta találkozhat a biztonsági vezető foghíj beépítéssel, az is előfordulhat, hogy a szomszédos telkek is építési területek. Ezekre a telkekre jellemző a nagyfokú, esetenként fizikai körbezártság, amely lényeges körülmény a biztonság tervezése szempontjából.

A kijelölt építési terület vizsgálata ezért nem árt, hogyha már az Önkormányzatnál fellelhető területrendezési tervek, dokumentációk tanulmányozásával folytatódik. A vizsgálódás tárgyát képezik ugyanakkor a közlekedési útvonalak, a gyalogos forgalom, a tömegközlekedési vonalak, és a közvetlen környezetet alkotó lakóházak.

Ezzel szemben a „külterületi" jellegű (szántó területből frissen átnevezett belterületi építési terület) projektek tekintetében merőben más a helyzet. Ez a terület minden oldaláról nyitott könnyen átjárható, átlátható, rendészeti szempontból rettentően sérülékeny, mert legtöbbször csak egy képzeletbeli vonal választja el az építési területet a szántótól vagy egyéb más mezőgazdasági területektől (erdők, telepített erdők, művelés alatt álló táblák, mezőgazdasági útvonalak, stb.). Stratégiai szempont a megközelíthetőség a védelem kialakításának megtervezésekkor ezért mind a városi, mind pedig a külterületi jellegű kivitelezéseket komplex módon kell vizsgálni

A környék bűnügyi fertőzöttsége. A projekt helyszínének szemléjét követően értékelhetővé válik annak a védelem szempontjából meghatározó fizikai környezete, az azt alkotó lényeges terepelemek számbavételével együtt.

A biztonsági vezetőnek a védelmi koncepció kialakításához azonban még számos adatra szüksége van, többek között a terület bűnügyi helyzetére vonatkozóan. A helyi hatóságoknál érdeklődnie kell (az érintett információkat természetesen más forrásból is beszerezheti) a bűnügyi jellemzők, bűnügyi statisztika után. Ebben a szakaszban azt a kérdéskört kell tisztázni elsősorban, hogy a vagyonellenes cselekmények közül melyek fordulnak elő jellemzően (lopás, betöréses lopás, rablás, rongálás, szabotázs), ezen belül középületek, ipartelepek, építkezések, magánházak elleni, események gyakoriságát és azon elkövetések módszereit.

A bűnügyi helyzet-felmérés és tájékozódás fontos a projekt biztonsági rendszerének minimálisan szükséges védelmi kapacitásának meghatározásánál, s bár nem minden esetben lehet törvényszerű összefüggést kimutatni az adott környék bűnügyi szennyezettsége és a leendő projekt vagyonellenes cselekményei között, a megszerzett információk mégis stratégiai jelentőséggel bírnak a biztonsági terv elkészítésénél.

Néhány lényeges - már az építkezés kezdetén felmerülő – körülményről még a legkörültekintőbb helyszíni szemle sem biztosít kellő információt, ilyenek lehetnek a személy-, illetve a tehergépjármű forgalom kialakítása. Ezekről az **organizációs és forgalom**

technikai terv kínálhat felvilágosítást, melyben foglaltatott kívánalmak figyelembevétele nagyon fontos a tervezési fázisban. A kivitelező vállalatnak egyébként a forgalom technikai tervet az illetékes építésügyi hatóságnál kell engedélyeztetnie. Ezen az organizációs terven már egyértelműen látszik a későbbi gépjármű forgalom, teherforgalom, valamint a humán ki és beléptetés rendje.

Az organizációs terv egyik fő pillére a biztonsági terv elkészítésének, hiszen a rajzon jó láthatóak a kerítéssel elkerített részek a kapuk elhelyezkedése, valamint a szabadon hagyott területek is, melyek védelmének rugalmas kialakítása szempontjából az élőerő felépítése és feladatainak meghatározása kell, hogy megtörténjen.

A kivitelezésre kerülő objektum mérete és elhelyezkedése a környezetében döntő jelentőségű, melynek előzetes értékelésére ugyancsak ekkor nyílik lehetőség első ízben, ugyanis az organizációs tervben lehet látni azokat a kimagaslóan védendő épület részeket, amelyek hiányos védelem esetén könnyű támadási felületet nyújtanak az elkövetők számára.

Az objektum mérete és elhelyezkedése a kivitelezés alatt annak okán is kiemelt jelentősséggel bír, hogy az építési területen helyt foglaló konténer városok, felvonulási területek, anyag tároló területek kialakítását nagymértékben befolyásolja az épület későbbi végleges formája, és ez a körülmény szintén meghatározó az élőerős védelem szervezése szempontjából.

Ezek a területek ugyanis rendszerint túlzsúfoltak, gyakran átláthatatlanok, kevésbé védhetőek, így fokozott kockázatot rejtenek az építési területen. Az élőerő megosztása során ezekre a zónákra gyakorta túlsúlyt kell képezni, illetve tartalékolni.

A kivitelezésre kerülő épületbe szerelendő anyagok (technikai eszközök, különleges építő anyagok felhasználása, speciális technológia telepítése stb.) minősége és mennyisége szintén meghatározza a biztonsági szolgálat biztosítási tervét és majdani jóváhagyott működési szabályzatát. Nem elegendő a kivitelezés helyszínét biztosítani és megvédeni az esetleges elkövetőktől, a beépítésre váró anyagok folyamatos védelmére is legalább ugyanannyi erőt, ha nem többet kell fordítani ezen eszközök és alkatrészek összértékét figyelembe véve.

Egyáltalán nem mindegy ugyanis, hogy luxus szálloda építésére kerül sor, ahol minden felhasznált anyag prémium kategóriás vagy egy logisztikai csarnok létesítési folyamatát kell védeni ahol a méretek és anyagok felhasználása miatt kisebb mértékben számíthatunk az elkövetők megjelenésére a védelem tárgyának e területén.

Fontos kiemelni azon egységek biztosítását, ahol a csúcsminőségű gyártástechnológia miatt is a beszerelendő gépek, eszközök, berendezések, tovább nehezítik a rendészeti feladatok ellátását.

Az építőiparon belül hatalmas a különbség a védendő projektek között, nem elegendő egy sémát készíteni a vagyonvédelmi tervről, hanem minden egyes elemét a projektnek külön kell vizsgálni a projekt sajátosságai szerint.

ÉPÍTŐIPARI BERUHÁZÁSOK SAJÁTOSSÁGAI

Kivitelezett objektumok szerinti vizsgálatot a biztonsági szolgálat vezetőjének és annak közvetlen stábjának kell elvégezni. Pontosan tudni kell ehhez (a tervekből természetesen kiderül) az épület típusát, hasznosítását, és az oda beérkező anyagok mennyiségét és minőségét.

Az építőipari nagyberuházások biztosítási tervének kialakítása szempontjából le kell szögezni, hogy a funkcionálisan és más szempontból is stabil objektum általános védelmi követelményeivel szemben itt általános érvényességgel kijelenthető az objektum úgy térben,

mint időben történő folyamatos változása, így az élőerős védelem létszámának és feladatainak folyamatos bővülése.

A vagyonvédelem komplex rendszerének, és az azon belül elhelyezett élőerős védelem tervezése során is fegyelembe kell venni a fenti sajátosságot, ami a tervezést nagyban nehezíti.

Az ugyan nyilvánvaló, hogy a nagyberuházás során napról napra bekövetkezett változásokat a tervben lehetetlen ugyanebben az ütemben előre lekövetni, a változások rugalmas prognosztizálása érdekében szükséges és megvalósítható megoldásként kínálkozik a projektfolyamatok egy előre meghatározott vizsgálati szempontrendszer szerinti differenciálása kiemelt figyelmet fordítva többek között az alkalmazott munkafolyamatra, a ténylegesen igénybevett területre, az ideiglenesen letárolt anyagok mennyiségére és értékére, valamint a felhasznált és beépített anyagok értékére és „mozdíthatóságára".

Célszerű tehát a beruházás főbb és egyben jól körülhatárolható állomásait külön-külön kezelve megvizsgálni és értékelni. A vizsgálandó területeket képezik a földmunkák, mélyépítés, szerkezet építés, generál kivitelezés.

A földmunkák kockázati elemzése során első ránézésre talán egyszerűnek tűnik a helyzet, hiszen látszólag a védendő értékek köre szűk és jól behatárolt, komoly értékű anyag, berendezés nem kerül még letárolásra a területen.

Amennyiben azonban tüzetesen megvizsgáljuk az ekkor védendő eszközök körét (teherautó, föld-gyaluk, markológépek, egyéb nehéz gépek stb.), valamint azok alkatrészeit és a bennük lévő üzemanyag mennyiségét és értékét, a szükséges védelem külső körülményeit, világosan látszik, hogy ez az egyik legfontosabb és legkényelmetlenebb rendészeti feladat a projekt elindulásakor. Ebben az esetben mindegy, hogy városi vagy zöldmezős a beruházásról van szó, hiszen ekkor még gyakran nincs fizikai védelemmel ellátva az építési terület.

A biztonsági szolgálat kiemelt feladataként kell meghatározni a földmunkák esetében a kiszállított földmennyiség feljegyzését, a ki- és belépő gépjármű forgalom rendszám alapján történő ellenőrzését.

Itt az élőerő létszámának optimális kialakítása rendkívül fontos annak figyelembevételével, hogy az esetlegesen alulbiztosított védelem megerősítésére ebben a szakaszban technikai támogatás még ritkán biztosítható a fenti sajátosságok miatt. A legnagyobb problémát a felsorolt gépek és berendezések igen magas ára jelenti valamint a bennük található azonnal pénzre váltható üzemanyag.

Mélyépítés rendészeti szempontból viszonylag hálás építési szakasznak tekinthető, mert az alap kialakítása során történő földkitermelést követően az alaplemez elkészítéséhez valamint a résfal kialakításához minden anyagot és eszközt letelepítenek a munka helyszínére és a vasanyag valamint a beton szinte azonnal beépítésre kerül.

A rendészeti szolgálatnak könnyebb dolga van „mert csak" a munka gödörre kell vigyázni. A mélyépítés sajátossága, vasanyag felhasználás, betonozás, zsaluzati rendszerek használata. Ezek bármelyikének képviselt értéke egy nagy nagyberuházás során elérheti a több százmillió forintot, a védelmi szolgálat felelőssége tehát nem csökken.

Szerkezetépítés az alaplemeztől a záró födémig („koporsóig") tart, melynek során hatalmas mennyiségű vasanyag, beton kerül felhasználásra.

A szerkezet építők a ház szerkezetét zsalurendszerek segítségével építik ki, melynek ki-és beszállítás, felhasználása stratégiai jelentőségű, noha a beépítésre kerülő anyag maga a vasbeton,(effektív értéke nincs, az anyaga miatt szabotázs védett), a kivitelezés során felhasznált zsalurendszerek azonban milliárdos értéket képviselnek és azonnal értékesíthetők, így keresettek a feketepiacon.

A zsalurendszereket több beszállító biztosítja a projekthez melyeket bérbe adnak bizonyos munkák elvégzéséhez, és miután végeztek az érintett munkafázisokkal visszaszállítják a bérbeadó cég telephelyére. Ennek teljes körforgását kell a rendészetnek napra készen nyomon követnie és átlátnia. Ez kiemelt feladata kell, hogy legyen az élőerőnek, és a biztonsági vezetőnek a védelem tervezésekor megfelelő rálátással kell rendelkeznie eme sajátosságra, különösen annak tükrében, hogy a zsaluzat egyes elemei azok felhasználása során gyakran sérülnek és roncsolódnak.

Ha a biztonsági szolgálat itt pontatlanul és figyelmetlenül végzi e rendszerek biztosítását, akkor az építkezés végére csak ezeket az eszközöket tekintve több 100 milliós kár is keletkezhet.

A generál munkálatok gerincét a gépészet a villanyszerelés és a szárazépítés képezi, melyek jelentős kockázati tényezőt képviselnek rendészeti szempontból, hiszen az itt felhasznált vagy beépítésre kerülő anyagok mindegyike együttesen, akár külön- külön is ki van téve a vagyon ellenes cselekményeknek.

A lopásból származó kár ismételten elérheti több 100 millió forintot, mivel a probléma összetettebb, ekkor az előzőekhez képest komolyabb erőkoncentráció és komplex problémakezelés szükséges ahhoz, hogy ezeket a nem kívánt eseményeket elkerüljük. A generál munkálatok során például a konténerbázis őrzése kiemelt fontosságú feladat, ezzel egyidejűleg végzett humán ki-be léptetés, gépjármű ki-be léptetés és ezek együttes hiteles regisztrációja elengedhetetlen az eseménymentes feladat ellátáshoz.

Az épületbe telepített belső raktárak az alvállalkozók gépeinek eszközeinek védelme, az épületbe szerelt anyagok (gépészeit berendezések, villamos technikai eszközök, stb.) folyamatos biztosítása követeli meg annak a komplex védelmi struktúrának a kialakítását, melyet a biztonsági szolgálatnak követnie kell a kivitelezés során.

Az építőipari nagyberuházások sajátos körülményeik alapján történő megkülönböztetése lényeges az azok biztosítása során kiépítendő védelmi rendszer élőerős komponensének kialakítása érdekében. Az építőipari beruházások azonban számos szempont alapján differenciálhatók, így az optimális élőerő létszám meghatározásakor még további tényezők vizsgálata válik szükségessé.

Gyárak, gyáregységek, raktár épületek, logisztikai központokra a kivitelezésük hasonló technikája jellemző, az ami alapján gyakorlatilag egy kategóriába lehet sorolni e projekteket. A kivitelező vállalatok előre elkészített vasbeton szerkezetet alkalmaznak, az oldalfalakat és a tetőt pedig hőszigetelt panelekből alakítják ki. A belső teret rendszerint síkba betonozzák. A gépészetet és az elektromos rendszereket pedig a megrendelt igényekhez alakítják.

A különbség a gyárak és a raktárak között a gyárakba telepített technológia (gyártósor). Az ilyen típusú projektek alkalmával gyakran a rendészetnek nagyobb figyelmet kell fordítania a gyártósor letelepítésére, mint az épület kivitelezése során behozott előre legyártott épület alkatrészekre.

Szállodák, irodaházak sajátosságait vizsgálva egy közös pontot lehet felfedezni. Az épületek tagozódását valamint a beszerelendő prémium kategóriás alkatrészek mennyiségét.

Természetesen egy 4-5 csillagos szálloda kivitelezése rendészeti szempontból nagyon nehéz és összetett folyamat. A prémium kategóriás anyagok (kivételesen díszített szaniterek, pl. aranyozott csaptelepek, egyedi lámpák, stb.) érkeztetésétől kezdve azok letárolásán keresztül egészen a beépítéséig biztosítani kell az anyagok mozgását illetve védelmét.

Ugyanekkora figyelmet kell szentelni a hagyományosnál jóval drágább építő anyagokra (márvány, gránit lapok, ólomüvegek, egyedi tervezésű díszítő elemek). Szállodákban

természetesen mindig – de gyakran irodaházakban is – előfordul, hogy ezen épületeket felszerelik a legmodernebb konyhatechnikával és olyan légtechnikával, ami csúcstechnikai színvonalat képvisel a maga kategóriájában. Rendészeti szempontból az irodaházak esetében az információvédelem szintén jelentős figyelmet kap már a kivitelezés során is. Az ilyen kivitelezéseken tapintható ki igazán vagyonvédelemi feladatok komplexitása.

Üzletközpontok sajátosságai, hogy ötvözik a luxus, a prémium kategóriás anyagok és a tömegeket kiszolgáló strapabíró rendszereket.

Ezen épületekben a helységek funkcionálisan jól elkülönülnek egymástól, épp ezért már a kivitelezés során kellő rendészeti erőátcsoportosítással elejét lehet venni a vagyonellenes cselekményeknek.

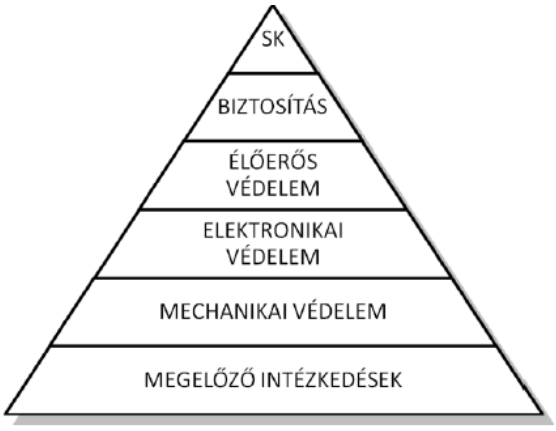
Itt nagyobbak a terek a szállodához képest, ugyanakkor a védhetősége nehezebb, mert jóval tagoltabb és összetettebb az ilyen épület együttes. Funkcióját tekintve egyszerre többféle anyag kerül beépítésre illetve kialakításra. Pl.: konyhák, bevásárló központ, nagyáruházak, kávézók, mozik, egyéb helységek.

A beérkező anyagokat biztosítani kell egészen a beszerelésig, ami azért összetett feladat, mert egy időben akár ezer munkás is dolgozhat az épületen. A munkájuk biztosítása rendészeti szempontból igen felelősségteljes és kockázatos feladat. Komolyan kell számolni a szabotázs lehetőségével és a szándékos károkozással is amellett, hogy az esetleges (rendszeres) gépeltűnések is hátráltathatják a munkát.

A másik komoly kihívás, hogy egy ilyen kivitelezés során a biztonsági szolgálatnak nem csak az épületre kell koncentrálnia, hanem a kisebb városnyi ember vagyontárgyaira is. Emellett biztosítani kell a belső rendet, a vagyonbiztonságot, mert egy szabotázs vagy lopás sorozat képes 200-300 milliós kárt is okozni, vagy akár a projekt leállítását is magába hordozhatja.

AZ ÉLŐERŐS VÉDELEM FELÉPÍTÉSE ÉS FENNTARTÁSÁNAK FELADATAI

A komplex vagyonvédelem egymásra épülő összetevőkből áll, melynek célja a kockázatok előfordulási valószínűségének és az egyes, mégis bekövetkező kockázati események káros következményeinek minél nagyobb mértékű csökkentése. [3] Összetevőinek kapcsolatát legérzékletesebben piramisban történő ábrázolással szokták kifejezni



1. ábra. A komplex vagyonvédelem összetevői[1]
(*forrás: Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései doktori (PhD) értekezés, 2009.*)

[1] A piramis csúcsán álló SK a „saját kockázat” rövidítése

A tervezés időszakában megkerülhetetlen tevékenység a komplex biztonsági rendszer komponensei arányának meghatározása. Ez a működés hatékony és zavarmentes biztosítása mellett, a szinergizmus jelenségét is biztosítja, az alrendszerek egymásra hatásának következtében a rendszer több lesz, mint a komponenseinek összege.

Az építőipari beruházások védelmi rendszerének mechanikai, illetve elektronikai elemei, főleg a kezdeti fázisokban gyenge hatásfokúak, esetenként hiányoznak, a kialakult aránytalanság következtében az élőerős védelemre ekkor nagyobb feladat hárul.

Éppen az építőipari tevékenységekre jellemző az, hogy a projekt előrehaladásával ezeken az arányokon beruházási szakaszonként változtatni kell. Ezeket a változásokat csak egy olyan védelmi rendszer képes követni, amelynek tervezésekor a tervező ügyelt a flexibilitás lehetőségének kialakítására. Ezt a rugalmasságot főleg az élőerő biztosítja. A flexibilitást képviseli a védelmi rendszer azon tulajdonsága is, hogy bármely elemének kiesésekor – ami egy építkezés során gyakran bekövetkezhet, a többi aktív képes lefedni a védelem területeit még, ha kisebb hatásfokkal is. [4] Az élőerős védelemnek ekkor is fontos szerepe van.

Építkezéseken jellemzően jelentős mind a személy, mind, pedig a gépjármű, valamint az anyagforgalom. A kerítésen belül az épülő objektumok a projekt befejezéséig nyitottak, szabad bejutás kínálkozik az épületekbe, az elektronikai védelem eszközei korlátozottan alkalmazhatók, ezért az élőerős védelem alkalmazása nagy jelentősséggel bír. Az élőerős védelem aktív komponensét képezi a komplex vagyonvédelmi rendszernek.

A személyi védelem képes ugyanis kezelni a bonyolult és váratlan helyzeteket, amelyeket az átlagos paraméterekkel rendelkező technikai eszközrendszer nem.[5] A humán elem szubjektivitása jelenti azonban annak gyenge pontját is. Az élőerős védelem elemei ugyanis forrását képezhetik az objektum belső veszélyeztetettségének, mely nehezen felderíthető, azonosítható és az ellene való védelem is meglehetősen nehéz. Az olyan jelenségek bekövetkezése, mint a szakszerűtlen feladat-végrehajtásból eredő kár, szabotázs, lopás vagy abban történő részvétel, esetleg a védelem szilárdságát biztosító fontos információk kiadása ugyanakkor az egész védelmi rendszert fenyegeti és a megelőzés roppant problémás.

A **munkaerő-kiválasztás** szempontjai között gyakran előkelő helyen találjuk a készségek és képességek igénye mellett a gazdaságosság szempontját.

Az élőerős védelem esetében nem a legolcsóbb a legjobb, hiszen mint, a már említett belső veszélyeztetettség forrása később igen sokba kerülhet. A kiválasztás folyamatában a szakmai kompetenciák mellett figyelmet érdemel a munkavégzési alkalmasság (fizikai – egészségügyi - pszichikai) vizsgálata. Emellett lényeges szempont a munkavégzési hajlandóság és az önálló fejlődés képessége. Az őrnek tudnia kell munkája során adaptálnia a tapasztalatokat, az egyes eseményekre reagálva tovább kell tudnia fejleszteni az egyéni módszereit. Szakszerűen kell kezelni a digitális beléptető rendszert, az őrjárat ellenőrző rendszert ellenőrizni kell a vagyonvédelmi-, tűzvédelmi eszközöket, azok üzemképességét. A képezhetőség is fontos, hiszen az új technikai eszközök bevezetése, a régiek korszerűsítése megköveteli az alkalmazó élőerő felkészítését.

A továbbképzésnek egyébként ki kell térnie a technikai eszközök mellett a jogszerű tevékenységet meghatározó jogszabályok ismertetésére is.

A komplex vagyonvédelem élőerős elemének fenntartása és „üzemeltetése” aktív jelenlétet kíván, a biztonsági vezetőnek folyamatos kontroll alatt kell tartani eme komponenst. Az közismert, hogy a vagyonvédelmi rendszer hatékonyságát a leggyengébb elemének hatékonysága determinálja. Nem kellő körültekintéssel felépített rendszereknek gyakorta az élőerős összetevője jelenti a leggyengébb láncszemet.

Az élőerős védelem felépítése során a hierarchikus struktúra kialakítása kívánatos számos okból. A hierarchia ugyanis a végrehajtás szervezettségét, a felelősség megállapíthatóságát, az őrök önállóságának behatárolását is biztosítja. [6]

Az élőerős védelem önmagában költséges és az emberi hibalehetőséget figyelembe véve szinte folyamatosan kockázatokkal terhelt komponens. Hatékonyságának megőrzése, valamint a működtetése során „betáplált" energia hasznosulása érdekében rendkívül fontos az élőerős védelem feladatainak pontos behatárolása. A feladatok meghatározásánál törekedni kell az adott projekt sajátosságainak figyelembe vételére, ami gyakorlatilag a biztonsági terv gyakorlatba történő átültetését jelenti.

A rendelkezésre álló információk és a biztonsági terv alapján kell tehát kialakítani és rögzíteni az élőerő feladatrendszerét. Mindezt természetesen közérthetően tömören, utasításokból felépítve, általában egy egységes szabályzatba foglalva. Ez nevezhető szolgálati utasításnak és vagy működési szabályzatnak. A szabályzatot úgy kell felépíteni, hogy az alkalmazó biztonsági szolgálat az egyes utasításokat követve el tudja látni az objektum és a hozzá tartozó terület őrzés-védelmét, idegenek behatolását képes legyen megakadályozni, és a belső rendet fenntartani. A napi irányítás igen hatékony eszköze, rögzíti a feladatokat úgy, hogy azok kikényszeríthetővé és ellenőrizhetővé váljanak. A hatékonyság érdekében a szabályzatnak tartalmaznia kell annak területi, személyi, időbeli hatályosságát, az őrzés-védelem, valamint a be-, és kiléptetés szabályait. A szabályzatnak egyebek mellett ki kell térnie a felelőségi viszonyokra, a műszaki követelményekre és a rendkívüli helyzetek kezelésére is.

A biztonsági szolgálat kiemelt feladata az építő ipari vállalat belső információinak védelme jó hírének megtartása, az ingatlan területén lévő anyagi javak őrzése a tűzvédelem és munkavédelem egyes szabályainak betartatása is.[7] A felelőségi körök megállapítása rendkívül lényeges az önálló tevékenység határainak megjelölésével.

Az élőerős szolgálat alapvető feladata a tulajdont károsító cselekmények megelőzése, felderítése, és annak meghiúsítása. Mindezek mellett az üzleti és vállalati titok védelme, az iratok és egyéb adathordozók (adatvédelmi rendszer) védelmére vonatkozó szabályok kidolgozása érvényesülésének elősegítése.

A vagyonvédelmi szolgálat tagjainak felelőssége van tehát a szolgálati utasításában meghatározott feladatok ellátása, a rábízott javak megőrzése, megvédése, valamint az őrszolgálat szabályos átvétele, ellátása területén, s nem utolsó sorban a technikai eszközök üzemképességének megóvása és a szolgálati okmányok szabályszerű vezetése területén.

Az élőerős szolgálat eredményes munkavégzésének alapvető követelménye a szükséges feltételek biztosítása, így többek között a működést alapjaiban meghatározó jogszabályok által megjelölt **jogkör behatárolása**. A jogkör meghatározásánál egyértelműen rendelkezik a jogalkotó, és ez iránymutató kell, hogy legyen a rendészet jogkörének meghatározásakor.

A biztonsági szolgálat vezetőjének kiemelt felelőssége az, hogy felhívja a kivitelező vállalat projekt vezetőjének a figyelmét a rendelkezésre álló jogszabályokra és az azok által biztosított mozgás-térre. A jogszabályok komplex ismerete és alkalmazása a biztonsági terv jogi hátttereként, mintegy biztosítéka a törvényes és hiteles (jogkövető) rendészeti munkának.

Sikeres munkavégzés alap feltétele a paragrafusok pontos ismerete és alkalmazása különösen a személyt érintő ellenőrzések és az adatok kezelésénél. Ugyanis a munka jelentős részét teszi ki az adatok kezelése és az építkezésen dolgozó személyi állomány teljes kezelése.(ki-, beléptetés kártyakészítés, adatainak kezelése, stb.), természetesen a fő tevékenység: az építkezés elleni vagyon ellenes cselekmények megakadályozása és az elkövetők elfogása mellett.

Kellő jogi ismeretek hiányában nem lesz sikeres az adott szolgálat. A jogszabályi környezetet változásainak nyomon követése szintén kiemelt feladata a biztonsági vezetőnek.

A védelmi filozófia és a védelmi stratégia, komplex védelem, így a kialakított élőerős védelem hatékonysága szempontjából elengedhetetlen a **tevékenységi célok meghatározása** és kitűzése. A legfontosabb feladat ennek érdekében, hogy pontosan ismerjük a projekt minden részletét úgy műszaki, mint humán erőforrás oldalról, de a közös célkitűzés az építőipari nagyvállalattal, stratégiai jelentőséggel bír. Több célkitűzés is lehet, pl.: egyes munkafolyamatok fokozott ellenőrzése, biztosítása. Lehet cél a prémium kategóriás építőanyagok biztosítása, lehet cél a biztonsági szolgálatnak a dolgozói állomány kiléptetésének precíz és hiteles regisztrálása.

A részfeladatok ellátása során elképzelhető ütközés a különböző célok megvalósítása érdekében ezért az építőipari vállalat és a biztonsági szolgálat céljainak közös platformra történő helyezése és a konfliktussal terhelt területek felderítése igen lényeges. Ennek megvalósulásának hiányában gyakran szembesülnek a kivitelezésen tevékenykedő építőipari alvállalkozók a biztonsági szolgálat korlátozott felelősség-vállalásával (pl. konténer feltörés, raktár feltörés, gép eltűnés, rongálás egyes eseteit illetően).

Az élőerős védelem tervezésénél előre kell gondolni néhány olyan, a későbbiekben megkerülhetetlen, és folyamatosan jelenlevő feladatra, mint az **állománnyal való foglalkozás**, humán erőforrás menedzselés: kiképzés, számonkérés, frissítések, melyek az élőerős szolgálat költségeit emelik. Ezek lehetnek azok az eszközök melyekkel a biztonsági szolgálat tagjait, a vagyonőröket motiválni is lehet. Ez folyamatos szakmai képzés formájában kell, hogy megvalósuljon. A képzések során a vagyonőröket meg kell ismertetni a legújabb technikákkal és eljárásokkal. A legújabb technológia felhasználása az Internet kezelése mellett a PC felhasználói szintű ismerete elengedhetetlen, különös tekintettel a rendészeti feladatokat támogató szoftverekre.

Az ismeretek szinten-tartása érdekében a képzéseket nem elég csupán egy vagy két alkalommal végrehajtani, folyamatosan kell képezni a kollegákat, a megfelelő szakemberek bevonásával. A biztonsági szolgálat munkatársainak a híradás biztosítása szempontjából fontos kommunikációs eszközök és berendezések új programjainak betanítása. Az online kommunikációs rendszerek probléma-mentes használata, az alkalmazott szoftverek üzemeltetése és a felmerülő problémák szakszerű kezelése napi feladatként jelentkezik.

A vagyonőröknek a számonkérések során kell a megszerzett tudásukról számot adniuk az őket kiképző szakembereknek. Természetesen mind ez a munka feladatuk ellátása mellett történik. Gyakran előfordul, hogy a már megismert szoftvert (kamera rendszert vezérlő szoftver, járőrútvonal ellenőrző szoftver, digitális képkezelő szoftver) adott esetben egy másik területre történő átvezénylés után elfelejti a vagyonőr, ebben az esetben az erre a feladatra kijelölt szakembernek újra fel kell frissítenie a korábban tanultakat.

A humán erőforrás menedzselés területéhez tartozó feladatok korrekt elvégzése a biztonsági vezető felelőssége, melynek hanyag ellátása az élőerős védelem hatékonyságának csökkenését eredményezheti exponenciális mértékben. Az emberekkel való foglalkozás egyik fő tevékenységi köre a rendezett munkaviszony biztosítása munkaszerződéssel, munkaköri leírással, szolgálati utasítással, hitelesen működő tb. ügyintézéssel, korrekt időben történő fizetéssel, pontos kiszámítható pályával. A vagyonőrökkel napi szinten a szolgálatvezetők, csoportvezetők és osztályvezetők kell, hogy foglalkoznak.



2. ábra. A mostoha körülmények között fontos az élőerő kellő motiválása

Napi operatív munka végrehajtása és annak ellenőrzése elengedhetetlen a pontos hatékony és eredményes rendészeti munka elvégzésében.

A napi operatív munka végrehajtását a biztonsági szolgálat működési szabályzata és annak rögzített változata a biztonsági szolgálat szolgálati utasítása adja meg. Ezen utasításokban pontosan meghatározásra kell, hogy kerüljenek a napi feladatok, a protokollok, eljárások, különböző szituációkra. A működési szabályzat biztosítja biztonsági filozófia megvalósulását, és pontosan leírja a rendkívüli események bekövetkezésekkor végrehajtandó feladatokat.

A napi munka egy vagyonőr életében jól összerakott rendészeti séma szerint zajlik, a feladatok és az eljárások nem változnak, a végrehajtásában azonban vannak különbségek. Építési területen gyakran előfordul, hogy a biztonsági szolgálat konténerét pakolgatni kell, át kell helyezni a technikai eszközöket is, ami bonyolíthatja a működést. A biztonsági őr napi munkája megkezdésekkor a szolgálat vezetőjétől kapja a napi utasításokat miután a szolgálatvezető átvette az előző váltástól a munkát. Feladatai közé tartozik a megrendelővel történő napi kapcsolattartás a gépjárműforgalmat, a dolgozók ki-be lépését, valamint az építési területen történt eseményeket, rendkívüli eseményeket illetően.

A napi munka főbb feladatai: a különböző nyilvántartások pontos vezetése, adminisztrációs tevékenység kamera rendszer kezelése, járőrfeladat ellátása és egyéb a szolgálattal összefüggő rendészeti munkák. A feladat tehát rendkívül összetett, ezért van szükség arra, hogy a vagyonőrök munkáját elsősorban segítve ellenőrizzék a vezetők.

Az ellenőrzés egy komplex rendszert kell, hogy alkosson, azaz az eredményesség miatt több lépcsősnek kell lennie. Az első lépcsőt a szolgálatvezető képviseli, aki kiadja az őrnek a napi feladatokat és azokat számon is kéri tőle.

A második lépcső a csoportvezető, aki a szolgálatvezető munkáját is ellenőrzi, és behatóan tanulmányozza a korábban kiadott utasítások végrehajtását, valamint azok eredményeit.

A harmadik lépcső az osztályvezető, aki a csoportvezetőt is ellenőrzi ugyanakkor közvetlenül foglalkozik a biztonsági őrök munkaügyi kérdéseivel, magánéleti kérdéseivel, tekintettel arra, hogy az osztályvezető készíti el a szolgálatok szervezését is.

Negyedik lépcső az éjszakai járőrszolgálat, akik kimondottan a vagyonőr éjszakai munkáját ellenőrzi. Az ellenőrzések célja az éjszakai mozgások figyelése az éjszakai szolgálati utasítások végrehajtásának ellenőrzése. És az esetleges szolgálattal nem összeegyeztethető cselekmények feltárása és megakadályozása.

Ötödik lépcső a 0-24 órás diszpécser szolgálat, aki az Internet segítségével digitális kamerákon keresztül folyamatosan nézi az adott területen történő mozgásokat, eseményeket,

emellett telefonos kapcsolatot tart fent az adott szolgálattal, akik meghatározott időnként leadják a központnak az addig történt eseményekről a jelentéseket.

Az öt lépcsős rendszer adja meg azt a hatékony ellenőrzési struktúrát, amit egy építőipari nagyberuházást biztosító vagyonvédelmi cég vezetőjének ki kell alakítania annak érdekében, hogy az élőerős szolgálat fenntartására fordított energia ne ablakon kidobott pénz legyen.

Az őr munkájának figyelemmel kísérése egyrészt ellenőrzés, másrészt az ennek során megvalósuló visszajelzés, esetleg értékelés a hatékony munkavégzés irányában motiválhatja az őrt.

Kooperáció, a megrendelővel és az alvállalkozókkal történő napi kapcsolattartás nagyon fontos, mert az épület napról napra változik, és ennek okán kell, hogy az élőerős szolgálat napra kész legyen.

A megbeszéléseket heti egy alkalommal kell tartani ahol a megrendelő az építőipari nagyvállalat képviselője tájékoztatja a biztonsági szolgálat vezetőjét az alvállalkozók által elvégzett munkákról. Minél előrehaladottabb állapotba kerül a beruházás, annál több anyag kerül be az épületbe, annál inkább nő az épületben található műszaki berendezések száma.

A kooperáció során meg kell vitatni a bekövetkezett változásokat, a rendészeti feladatokat, hiszen a változásokkal együtt változik a kivitelezés védelmi képessége is. Egy jól működő biztonsági szolgálat hatékony és hiteles feladat ellátásához elengedhetetlen a napi kommunikáció a területen dolgozó alvállalkozó vezetőivel valamint a megbízó jelenlévő képviselőjével.

Az objektumok védelme összetett feladat. A védelmi komplexum bármely részelemének hiánya vagy gyengesége kihat a teljes biztonsági rendszer hatékonyságára. A komplex rendszer részelemei is bonyolult biztonsági alrendszerek (beléptető rendszer; biztonsági monitoring rendszer stb.). A zavarmentes működés követelményeinek biztosítása létfontosságú. Az elektronikai és mechanikai védelmi alrendszerek magas fokú integráltsága mellett továbbra is fontos szerepe van az azokat üzemeltető élőerő tevékenységének, felkészültségének. [7]

Irodalomjegyzék

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

[2], [5] Báthori B.- Bodrogi F. - Szili L.: Őrzés védelem, jegyzet, Pro Lex Oktató és Szolgáltató KKT, Budapest, 1995.

[3] Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései, Doktori (PhD) értekezés, 2009.

[4], [5], [6] Teke András: Az őrzés, mint rendészeti alaptevékenység VI., in: Rendvédelmi Füzetek 2000/45, a Rendőrtiszti Főiskola kiadványa, Budapest, 2000.

[7] Szolgálati utasítás az S.C. Kft. által biztosított területén működő fegyver nélküli vagyonőri szolgálat részére. S.C. Kft, 2009.

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

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Fialka György

A PÉNZINTÉZETEK BIZTONSÁGVÉDELMÉNEK LEHETSÉGES PARADIGMAVÁLTÁSA

Absztrakt

A pénzintézeti biztonság megvalósítása, több tényező együttes fenntartása esetén lehetséges. Ezek a biztonságtechnika eszközei, az élőerős védelem személyi, szabályzási, és tárgyi elemei, a szabályozás keretei, a biztonsági szolgáltatások minősége, és az együttműködés különféle válfajaiban rejlő lehetőségek. Ezen tényezők egy része bizonyos okok mentén kezd zsákutcába torkolni a körülmények és lehetőségek szűkülése miatt. A cikk a paradigmaváltás lehetőségeit kívánja bemutatni, a környezeti mikró és makró hatások mentén.

The security of financial institutions can be guaranteed only with a permanent support of more factors. These are the tools of safety engineering, the personal, regulatory, and objective elements of live force defense, the frame of regulation, the quality of security services, and the possibilities in he different types of co-operation. A part of these factors starts to impasse because of the narrowing of circumstances and opportunities the article wants to introduce the potentials of changing paradigms, alongside the surrounding micro and macro effects.

Kulcsszavak: *ügyfél, paradigmaváltás, magánbiztonság, törvény, biztonságtechnika, együttműködés, EU-s irányelvek ~ customer, change paradigm, personal safety, law, safety engineering, co-operation, EU standards*

BEVEZETÉS

Ahhoz, hogy a magyar pénzintézetek biztonságának jövőjét elemezhessük, mindenképen szükséges a jelen időszak történéseit és elért eredményeit megvizsgálnunk.

A biztonsági jövőkép megfogalmazásában, mikro és makró környezetünk jelentős befolyással bír. A globális behatások makró környezetünk meghatározó elemei, egyre intenzívebben formálják át közvetlen életterünket is.

A magyar pénzintézetek működés biztonságának értelmezésében is, ennek hatására jelentős átalakulások mennek végbe.

E változások felismerhető okai a következők:

- A változtatások, amelyeket a működésbiztonság előírt szintjének fenntartása érdekében szükséges végrehajtani, folyamatossá váltak, állandósultak!
- Az egyedi, magyar országra jellemző bűnmegelőzési megoldások, melyek a magyar pénzintézeti bűncselekmények megismert, jellemző típusainak elhárítási módszereit tartalmazták, elégtelennek bizonyulnak napjainkban, mivel megjelentek, és elszaporodtak az európai és a globális mintát követő pénzintézeti bűncselekmények.
- A védekezési lehetőségek és azok eredményeinek értelmezése, megoldásának nézőpontjai, forrásai teljesen eltérőek, még a feladat meghatározó szakértői körökben is. (Pl.: a 2010. Adatbiztonsági napon Dr. Kerezsi Klára: fejtegette véleményét a térfigyelő rendszerek bűnmegelőzési értékéről. A panacea, vagy placebó ellentét fejtegetésében a térfigyelő kamera rendszerek szakmai használati értékét kétségbe vonja. Vagy ugyanezen alkalommal: Dr. Jóri András a térfigyelő kamerarendszerek kialakult (nyilván eredményes) alkalmazásai, és a törvényi szabályozás személyiségi jogi ütközéseinek kérdéseiről beszélt.)

Nyilvánvaló, hogy a magánbiztonság egyes alapvető kérdései egységes szabályozási elvek, törvények, törvénymódosítások kialakítására várnak, melyet többirányú behatások figyelembe vétele mentén sürgősen el kell végeznünk. A magánbiztonság teljes területét átfogó, értelmező, szabályozó törvény igénye fogalmazódik meg, ezen feszítő problémák megjelenésével.

A nemzetközi és nemzeti gazdaságok működésének vizsgálata valamint fenntartásának tudományos elemzése során kialakult a **kritikus infrastruktúrák**, mint a működés feltételei alapegységeinek **elmélete**. Ennek a kritikus infrastruktúra csoportnak a pénzintézetek meghatározó alapelemei.

A PÉNZINTÉZETEK MINT A KRITIKUS INFRASTRUKTÚRÁK ALAPELEMEI

A kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak, és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működképesség, közegészségügyi és környezeti állapot fenntartásában.

A kritikus infrastruktúrák működésének meghatározó eleme a pénzintézeti szektor, mivel a gazdasági működés fenntartásának alapfeltétele, a pénzforgalom biztosítása az alapegységek között. Ennek híján bármely szektor működése megbénulhat, ezzel kihatva a többi rendszerelem alapműködésére is helyi és globális szinten egyaránt. Ezért a pénzintézeti szektor működését, biztonságát e kérdéscsoportra kialakult vizsgálati elvek szerint is elemezni szükséges.

Megállapítható, hogy a Magyar Pénzintézetek, mindazokkal a globális kihívásokkal, kockázatokkal, és veszélyekkel, valamint ezek következményeivel is szembenéznek, amelyek a fejlett világ többi pénzintézetét éri.

Ezek a következők:

- Globális kihívások:
  Demográfiai robbanás, energiahordozók kimerülése, víz, élelem, és a természeti erőforrások problémája, környezetszennyezés, globalizáció, társadalmi egyenlőtlenségek.
- Globális kockázatok:
  Migráció, Fegyverkereskedelem, vallási ellentétek, nacionalizmus, tömegpusztító fegyverek terjedése.
- Globális fenyegetések:
  Szervezett bűnözés, terrorizmus, kábítószer maffia.

Pénzintézeti szempontból a fentiek összehangolt, egységes nemzetközi irányelvek mentén kezelendők.

A fentiek részelemeikben, vagy következményeikben megjelennek a pénzintézeti biztonság védelmének, célterületei között, ezért praktikusan egységes fellépési irányelveket szükséges megfogalmaznunk.

Az Európai Unió tanácsa ezen globális kihívások, kockázatok fenyegetésekkel szemben közös fellépést tervez és szervez egységes irányelvek és közös intézkedések bevezetésével.

A BŰNMEGELŐZÉSNEK AZ ERÓAI TANÁCS ÁLTAL MEGHATÁROZOTT 2001.05.28-I IRÁNYELVEI

Az Európai Tanács a bűnmegelőzés kiemelt fontosságának jelzése érdekében tanácskozást folytatott, melynek következtetéseiről az alábbi irányelveket bocsátotta ki 2001. 05. 28-án:

- Csökkenteni kell a bűnalkalmakat, növelni kell annak valószínűségét, hogy a bűncselekmény elkövetőjét elfogják, és méltón megbüntetik,
- Redukálni kell a bűnismétlés lehetőségét
- Csökkenteni kell az áldozattá válás lehetőségét
- Terjeszteni kell a jogkövetés kultúráját, országon belül
- A prevenció lehetőségeit ki kell fejleszteni, technikai és intézkedési szinten bevezetni

Ezek az irányelvek a pénzintézetek bűnmegelőzési tevékenységét is döntően meghatározzák, hiszen a védekezés, és a bűnmegelőzés alapjait jelentő irányelveket határoz meg.

A fentiek gyakorlati megvalósítása megköveteli, a globális elkövetési módok folyamatos megismerését, a kimunkált preventív megoldások adaptív átvételét, és ezek alapján a pénzintézeti szabályzások szükséges módosítását.

INTÉZETBIZTONSÁG = ÜGYFÉLBIZTONSÁG

A biztonság egy állandó gerjesztéssel létrehozott és fenntartott szükséges, és elvárt állapot jelent, egy meghatározott és körülhatárolt térre vonatkoztatva. Fő iránya mindig személyre mutat, vagy a személy életteréhez köthető. A pénzintézetek az élettér részei, a végzett tevékenység tartalma alapján, mind az alkalmazottak, mint a ügyfelek szempontjából.

Ezért a pénzintézetek biztonságos működtetése szempontjából meghatározó szempont, az ügyfelek és az alkalmazottak biztonsága, és biztonságérzete. Ennek megteremtése több feltétel együttes teljesülése esetén következhet be.

Technikai feltételek:

- mechanikai, fizikai szilárdság megteremtése és a védelmi eszközök alkalmazása
- elektronikai jelző és dokumentáló eszközök telepítése, szakszerű alkalmazása
- banki folyamatok szabályozása, és a szabályzati elemek következetes alkalmazása

Élőerős őrzés:

- a készpénzforgalom biztosítására
- a bankfiókok működési rendjének támogatására
- az intézet belső és külső rendjének biztosítása

A fentiekben felsorolt rendszerek, eszközök, és módszerek valamint a mechanikai védelem eszközei és módszerei alkotják közösen a pénzintézeti védelem tárgyi eszközcsoportját. A pénzintézeti fizikai védelem további feladatait a *biztonsági élőerős őrzés* tevékenysége foglalja magába.

A technika és az élőerő együttes alkalmazása, tevékenységük egymáshoz illesztése, valamint a szabályzati rend következetes alkalmazása határozza meg a biztonsági, védelmi tevékenység hatékonyságát.

A SZOLGÁLTATÁSOK SZÍNVONALI KÖVETELMÉNYRENDSZERE

A biztonsági szolgáltatásokat nyújtó vállalkozásokkal kötendő szerződéseknek tartalmaznia kell az alábbiakat:

- a feladatok, és az elvárások szakszerű meghatározása;
- a szolgáltatói tevékenység elvárt minőségének pontos, részletes meghatározása;
- a végrehajtás ellenőrzési normáinak meghatározása;
- a SZERZŐDÉS minőségbiztosítási melléklete.

A szolgáltatás színvonalának minőségbiztosítási rendszerének kialakítása és fenntartása érdekében ezek kulcsfontosságúak.

A PÉNZINTÉZETI BIZTONSÁGI PARADIGMAVÁLTÁS LEHETSÉGES IRÁNYAI

A múlt és a jelen pénzintézeti biztonságának fejlődési sebességét döntően az elkövetésekből levont konzekvenciák és azok gyakorisága vezérelte. Érzékelhető, hogy az alkalmazott eszközpark technikailag még fejleszthető, finomítható, de igazi áttörést csak a paradigmaváltás okozhat a pénzintézeti biztonságvédelemben. A kérdéshez érdemes a tudományos elemzéseket és eredményeket figyelembe venni ahhoz, hogy a lehetséges új irányokat megfogalmazzuk. A vizsgálatok egy része az elkövetői magatartások, minták értékelésével foglalkozik, mások a beavatkozás eszközei és módszerei körül keresik a megoldást.

A kutatások eredményei adhatják azt a bizonyos paradigmaváltást, mely a védekezés új korszakát jelenthetik.

A rablás elkövetőivel szemben például alkalmazható pszichikai gátló eszközök a következők:

- a nyilvánosság bevonása a felderítésbe;
- a törvények erős szigorítása az elkövetőkkel szemben;
- a büntetés végrehajtás szigorítása az elkövetőkkel szemben;
- a fentiek részletes kommunikálása a médeákban, valós elkövetőkön keresztül;
- kiváló minőségű, nagyszámú dokumentáló eszköz használata az elkövetés helyszínén;

- időzárak alkalmazása a lehetséges helyeken;
- tájékoztató tábla a bejáratnál, mely a folyamatos képrögzítésről, és az időzárak alkalmazásáról is tájékoztatja a belépőket;
- az intézkedési rend demonstrálása.

Az eszközpark tekintetében is látszanak eredmények, melyek lehetőségeket kínálnak a paradigmaváltásra. Ezek a következők:

- az érzékelés kiterjesztése, és az érzékenység növelése újabb mérhető paraméterek megjelenése;
- intelligens értékelő, elemző szoftverek fejlesztése, az elkövetési mintákból kinyerhető adatok alapján;
- a biometrikus érzékelés határainak kiterjesztése, érzékenységének fejlesztése, az elkövetési mintákból kinyert irányvonalak mentén;
- a beavatkozás eszközeinek fejlesztése, a lehetőségek megismerése mentén;
- robbanó patron, felcsapódó hang és átlövés álló elem, füstágyú, a Terra Hz-s tartományban működő felderítő eszközök alkalmazása a beavatkozási módszereknél.

Az őrszolgálat szervezése is átalakításra vár, mivel jelenlegi formájában nem hatékony a bankrablások elhárításában. Több alternatíva is felvetődött az őrök elhelyezése, mozgatása, és alkalmazása tekintetében, de ezek valós értéke még nem látható.

A MAGYAR ÉS EURÓPAI BANKSZÖVETSÉGEKBEN REJLŐ LEHETŐSÉGEK

A hazai illetve a külföldi elkövetési minták és gyakoriságok elemzése, prevenciós egyeztetések, közös prevenciós döntések erősíthetik a védekezés módjait.

Az ORFK-val kötött Bankszövetségi együttműködési megállapodás, a gyors esemény feldolgozás és adatcsere személyek eszközök tekintetében a megelőzés másik lehetséges eszköze.

Magyarországi és EU-s bankok közötti információcsere a bankszövetségeken keresztül, a statisztikai adatok cseréjével és feldolgozásával, előjelzések, terjedési irányok és tendenciák megállapítását teszi lehetővé.

A pénzintézetek biztonsága, egy ország biztonságának meghatározó tényezője értékmérő eleme. Állandó fejlesztése biztonsági színvonalának növelése ezért kötelező. Tudományos bázisa, oktatási alapja és rendszere a kulcsa a védelmi szint fenntartásának, növelésének. Lényeges ezért mielőbb létrehozni egy önálló kutatóbázist, valamely szakirányú felsőfokú intézmény keretein belül, akik a fenti kérdések kezelését, karbantartását, valamint tudományos szintű feldolgozását végzik.

Ennek a bázisnak lenne feladata, a felsőfokú képzés szervezése is, a pénzintézeti biztonsági szakemberek részére.

FELHASZNÁLT IRODALOM

1. Vasvári György: Vállalati biztonságirányítás – informatikai biztonságmenedzsment, Info-Szakkönyv Bt., 2007
2. Vasvári György: Bankbiztonság, Információs Társadalomért Alapítvány, 2008.

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Körmendi Krisztina
krisztina.kormendi@gmail.com

Földi László
foldi.laszlo@zmne.hu

Solymosi József
solymosi.jozsef@zmne.hu

A KRITIKUS INFRASTRUKTÚRÁK ÉRINTETTSÉGE ÉS A KATASZTRÓFAVÉDELEM FELADATAI EGY ESETLEGES VILLAMOSENERGIA KRÍZIS HELYZET ESETÉN A 2003. ÉVI „NAGY ÉSZAK-AMERIKAI ÁRAMSZÜNET" TAPASZTALATAI ALAPJÁN

Absztrakt

A folyamatos villamosenergia ellátás a 21. századi modern társadalom alapvető szükséglete. Az ellátás kimaradása számos problémát vethet fel és rendkívüli helyzetekhez vezethet életünk számos területén, mint ahogy ezt a 2003. évi „nagy amerikai áramszünet" esetében is látható volt. Fogyasztók milliói maradtak áramellátás nélkül; számos, a mindennapi élethez alapvetően szükséges szolgáltatás nem volt elérhető. Mindez olyan rendkívüli helyzetet teremtet, melynek megoldása - az áramellátás és más alapvető szolgáltatások helyreállításán dolgozó szervezetek munkáján kívül vagy éppen annak segítésére - a katasztrófavédelemben, polgári védelemben érintett szervezetek közreműködését is igényelte. Jelen közleményben a 2003. évi „nagy amerikai áramszünet" példáját, mint esettanulmányt felhasználva arra keressük a választ, hogy a viszonylag tartós áramkimaradás milyen hatásokkal járt, hogyan érintett más kritikus infrastruktúrákat, a kialakult rendkívüli helyzetben milyen katasztrófavédelmi, polgári védelmi feladatok mutatkoztak, milyen szervezetek vettek részt a kialakult helyzet kezelésében illetve hogyan kezelték azt. Áttekintjük a katasztrófavédelem, polgári védelem és villamosenergia-krízis kezelés magyarországi szabályozását és megkíséreljük feltárni a hasonlóságokat és különbözőségeket. Végül megvizsgáljuk, hogy milyen szerepe lehetne egy újfajta intézménynek, az ún. energiabiztonsági központnak egy esetleges hosszan tartó, más kritikus infrastruktúrák működésére valamint a lakosság életére jelentős hatás gyakorló áramkimaradásra történő felkészülésben.

The continuous electricity supply is essential for the 21th century's modern society. Outages of the supply raise several problems and can lead to extraordinary situations in many aspects of our life, such as it happened during the North American blackout of 2003. Millions of customers remained without power, several basic services were not

available. That induced an extraordinary situation, the management of which required the contribution of disaster management and civilian defence institutions beside – or even for the help of - the organizations worked on the restoration of the supplies. In this publication we examined the effects of a relatively long-term power outage to other critical infrastructures, the disaster management and civilian defence tasks occurred due to the outage, the institutions involved and the manner they managed these problems in the example of the great North American blackout of 2003. We outline the Hungarian legislation of disaster management, civilian defence and electricity-crisis management, attempt to find similarities and dissimilarities. Finally we examine the possible role of a novel institution called Energy Security Centre in the management of a long lasting power outage, which has serious effects to other critical infrastructures and to the life of the population.

***Kulcsszavak**: villamosenergia krízis, katasztrófavédelem, kritikus infrastruktúra ~ electricity crisis, disaster management, critical infrastructure*

A 2003. AUGUSZTUSI NAGY ÉSZAK-AMERIKAI ÁRAMSZÜNET HATÁSAINAK ÁTTEKINTÉSE

2003 augusztusában a villamosenergia-ellátó rendszer összeomlása következtében jelentős áramkimaradás lépett fel az USA észak-keleti és középnyugati államaiban és a kanadai Ontario tartományban. Az áramkimaradás több Egyesült Államokbeli és Kanadai nagyvárost is érintett: pl. New York, Detroit, Cleveland, Connecticut, New Jersey, Michigan (USA), Ottawa, Toronto, Montreal, Quebec (Kanada). Mintegy 50 millió lakos maradt áramellátás nélkül, a kiesett szolgáltatás mennyisége 61800 MW volt. Míg a villamosenergia rendszer kaszkádszerű összeomlása néhány perc alatt lezajlott, a rendszer teljes helyreállításához több mint egy hét kellett. [1]

A villamosenergia rendszer összeomlásának eseményeit és okait egy korábbi publikációban [1] dolgoztuk fel. Jelen közleményben azt vizsgáljuk, hogy az áramkimaradás milyen hatást gyakorolt más alapvető szolgáltatásokra, kritikus infrastruktúrákra illetve mindez hogyan érintette a lakosság életét, milyen lakosságvédelmi feladatok léptek fel és hogyan kezelték ezeket.

Ez a konkrét eset is rámutat arra, hogy a villamosenergia rendszer, mint a kritikus infrastruktúra része kiemelt fontossággal bír, kiesése számos problémához vezet és más a kritikus infrastruktúrának minősülő rendszereket is súlyosan érinthet. A nagy-észak amerikai áramszünet esete azt mutatja, hogy az áramkimaradás kihatott

- a távközlési hálózatok, szolgáltatások (vezetékes és mobil telefonhálózatokat, televízió és rádióállomások, kábeltelevízió rendszerek, internet szolgáltatás)
- vízellátó és szennyvízkezelő rendszerek
- a közúti, vasúti és légi közlekedés, városi tömegközlekedés, az üzemanyag termelés és utánpótlás
- a pénzpiacok
- gyárak, ipari üzemek (áram és anyag utánpótlási problémák, normál működésnél több szennyezés, káros anyag kibocsátás)
- kórházak, egészségügyi létesítmények működésére illetve elérhetőségére.

Mindez egy rendkívül meleg nyári napon következett be, a hőmérséklet a nagyvárosokban meghaladta a 33 ^{o}C-ot, mely körülmények között az áramkimaradás és következményei még súlyosabban érintették a lakosságot. Számosan rekedtek a leáll liftekben, a két megállóközt leállt metró és vonatszerelvényeken. Estére lakosság világítás nélkül maradt, áram nélkül nem működtek a légkondícionáló berendezések, a meleg mellett néhány helyen a víz hiányával is meg kellet küzdeni. Az emberek nehezen vagy nem tudtak haza jutni munkahelyükről, New Yorkból az ingázók nagy része nem jutott haza, parkokban és középületek lépcsőin töltötte az éjszakát. A mobiltelefonok nem működtek, az emberek sorban álltak az utcai telefonfülkék előtt. A tűzoltókat számos gyertya okozta tűzesethez riasztották. Néhány területen a segélyhívó szám (911) elérhetősége nem volt folyamatos. Összesen 8 halálesetet jelentettek, melyek az áramkimaradás hatásainak következtében léptek fel. [2]

Több területen felszólították a lakosságot az árammal és vízzel való takarékoskodásra, Cleveland-ben a 18 év alatti lakosság számára kijárási tilalmaz rendeltek el. Michigan, New York és Ontario államokban rendkívüli helyzetet rendeltek el. [2]

Az Amerikai Egyesült Állomokban számos a lakosság védelmét érintő feladatot a tűzoltóságok végeznek, így volt ez a 2003.-as áramszünet esetén is. Az „International Association of Fire Chiefs IAFC)" nevű szervezet a tűzoltóság által a 2003 évi áramszünet alatt gyakorolt tevékenységét vizsgáló jelentés [3] 31 a tűzoltóságok által az áramszünet idején végzett feladat típust nevezett meg, melyek a tűzoltási és különböző műszaki mentési feladatok mellett olyan tevékenységeket is tartalmaztak, mint

- az áramellátás biztosítása kritikus állami és egyéb létesítményekben; generátorok kihelyezése, javítása;
- vízosztás a lakosság körében; hűsölők átmeneti „menedékek" kialakítása a lakosság számára, lakosság tájékoztatása;
- bűnüldözési, rendfenntartási tevékenységek, forgalomirányítás segítése;
- kórházak és egészségügyi szolgáltatók segítése; gyógyszerek hűtésének biztosítása, légzőkészüléket használók segítése;
- veszélyhelyzet kezelés vezetésének ellátása és/vagy közreműködés a helyi „veszélyhelyzet kezelő központok" Emergency Operational Centers) tevékenységében;
- szomszédos körzetek számára felszerelés és személyzet biztosítása stb.

A jelentést a társaság tagjainak részvételével készített felmérés alapján készítették, melyben különböző méretű hivatásos, önkéntes és „vegyes" tűzoltóságok munkatársai vettek részt. A jelentés szerint annak ellenére, hogy a tűzoltóságok számos nehézséggel néztek szembe, megfelelően teljesítették feladataikat. A siker sarokköve a megfelelő tervezés és felkészítés volt. A kidolgozott kölcsönös segítségnyújtási tervek; az áram, a víz és a kommunikációs rendszerek kimaradására vonatkozó készenléti tervek, eljárásrendek kidolgozása és alkalmazása valamint a személyzet megfelelő felkészítése mind hatékonyan hozzájárult a helyzet sikeres kezeléséhez. Ugyanakkor a jelentés szerint a helyzet által megkívánt eszköz, emberi és fizikai erőforrás igény számos tűzoltóság esetén meghaladta a rendelkezésre álló erőforrásokat, mely nehezítette a sikeres fellépést. További nehezítő tényezőként jelent meg a magánszektor felkészületlensége a veszélyhelyzetek kezelésére, a megfelelő eszközök és tervek hiánya valamint a (víz, áram stb.) szolgáltató vállalatok alacsony együttműködési hajlandósága a tűzoltóságokkal és más a veszélyhelyzetek kezelésében érintett szervezetekkel. [3]

ESETTANULMÁNY MICHIGAN ÁLLAM PÉLDÁJÁN

Mint az a fentiekben említettük a tartós és nagy területet érintő áramkimaradás hatásai miatt több államban rendkívüli helyzetet rendeltek el. A következőekben a Michigan Állami Közszolgáltatási Bizottság (Public Service Commission) beszámolója [4] alapján bemutatjuk az állami válsághelyzet kezelés szervezetét és a 2003. augusztusi áramkimaradás során elrendelt intézkedéseket. Michigan államban történtek jó példát nyújtanak a kritikus infrastruktúrák közötti interdependenciák bemutatására is.

A válsághelyzeti tervezés és elhárítás rendszere

Michigan államban a Közszolgáltatási Bizottság (Public Service Commission, PSC) felelős annak biztosításáért, hogy a lakosság és a vállalkozások megfelelő energia ellátáshoz juthassanak versenyképes áron. A Bizottság hivatott jóváhagyni a szolgáltató vállalatok által földgáz vagy áramellátási problémák esetén alkalmazandó eljárásrendeket illetve a szolgáltató vállalatok beszámolási kötelezettséggel tartoznak a Bizottság felé az általuk megtett intézkedésekről. Amennyiben az esetlegesen kialakuló ellátási válsághelyzet kezelésére kötelező érvényű állami intézkedésekre van szűkség, az állam kormányzója – saját hatáskörében vagy az ún. Energetikai Tanácsadó Bizottság (Energy Advisory Committee, EAC) javaslatára – „energia válsághelyzetet" (State of Energy Emergency) rendelhet el és kötelező érvényű intézkedéseket írhat elő. Ha az energia ellátási probléma súlyosbodik vagy egyéb esemény pl. természeti katasztrófa vagy terrortámadás is fellép, a kormányzó katasztrófahelyzetet (State of Disaster) rendelhet el. Ebben az esetben a védekezés elsődlegesen az „állami rendőrség veszélyhelyzet kezelési osztálya" (Emergency Management Division [EMD] of Michigan State Police [MSP]) hatáskörébe kerül át. Az osztály munkáját a Bizottság munkatársai támogatják. Ezen felül valamennyi állami minisztérium köteles kijelölni egy ún. „Veszélyhelyzet Kezelési Koordinátort" (Emergency Management Coordinator, EMC), aki képviseli az adott minisztériumot a veszélyhelyzet kezelés folyamatában illetve az koordinálja az adott osztály a helyzet kezeléséhez szükséges erőforrásainak rendelkezésre bocsátását. [4]

Az „energia válsághelyzetről szóló törvény" (Energy Emergency Act) széles hatáskörrel ruházza fel az állam kormányzóját energia válsághelyzet esetén. A törvény értelmében válsághelyzet esetén a kormányzó:

1. Rendkívüli korlátozásokat rendelhet el többek között pl.
    a. középületek, kereskedelmi-, ipari létesítmények és iskolák nyitvatartási idejét, fűtését, világítását
    b. az energiaforrások értékesítési körülményeit
    c. magángépjárművek használatát vagy a sebességhatárokat, tömegközlekedést illetően. [4]
2. Utasíthatja az energia (forrás) szolgáltatót, hogy biztosítsa alapvető egészségügyi, biztonsági és jóléti szolgáltatásokat nyújtó létesítmények, intézmények, szolgáltatók energia ellátását. [4]
3. Felfüggesztheti egyes jogszabályok, rendeletek rendelkezéseit, amennyiben ezek megakadályozhatják vagy késleltethetik a válsághelyzet kezelésére szolgáló intézkedéseket. (Nem függeszthetőek fel bűnügyi eljárások vagy a törvényhozást érintő rendelkezések.) [4]

A törvény előírja egy ún. Energetikai Tanácsadó Bizottság (Energy Advisory Committee, EAC) felállítását. Az EAC rendeltetése, hogy folyamatosan figyelemmel kísérje és értékelje az energiahelyzetre jellemző információkat, és felhívja a kormányzó figyelmét egy esetleges energia válsághelyzet kialakulásának veszélyére. Az EAC elnöke a Közszolgáltatási Bizottság elnöke, tagjai a Fogyasztóvédelmi és Ipari Szolgáltatások (Department of Consumer & Industry Services), Mezőgazdasági (Department of Agriculture), Közegészségügyi (Department of Community Health), Közlekedési (Department of Transportation) minisztériumok és a Michigani Állami Rendőrség igazgatói. [4]

Energiaügyi válsághelyzet esetén illetve ilyen helyzet kialakulásának veszélye esetén a Közszolgáltatási Bizottság (PSC) elnöke ún. „Energia Válsághelyzet Kezelési Munkacsoportot" (Energy Emergency Management Team, EEMT) állíthat fel az Energetikai Tanácsadó Bizottság (EAC) munkájának segítségére. A Munkacsoport folyamatosan figyelemmel kíséri a fejleményeket, értékeli a kialakult helyzetet és javaslatokat dolgoz ki annak kezelésére. A Munkacsoport tagjai a Közszolgáltatási Bizottság vezetői, a Bizottsági Műveletek (Commission Operations Division) és az Energiaügyi Műveletek (Energy Operations Division) Osztályok munkatársai. [4]

Az állami kormányzati szervek veszélyhelyzet esetén érvényes feladat és felelősségi körét Michigan állam Veszélyhelyzet Kezelési Terve (Emergency Management Plan) rögzíti. Az „általános terv" mellett az egyes veszélyhelyzet típusok (nukleáris baleset, ellenséges támadás, természeti katasztrófa, technológiai katasztrófa) esetére külön terveket dolgoztak ki. (Az áramkimaradás esetére a technológiai katasztrófa esetekre kidolgozott terv vonatkozik). A Veszélyhelyzet Kezelési Tervek mellett az egyes minisztériumok feladataikat részletesen meghatározó további tervekkel rendelkeznek. A terveket rendszeresen felülvizsgálják és frissítik, naprakész állapotban tartják. [4]

Az egyes minisztériumokban a Veszélyhelyzet Kezelési Koordinátor feladata, hogy gondoskodjon arról, hogy az adott osztály képes legyen a Veszélyhelyzet Kezelési Tervekben meghatározott feladatai ellátására. A Koordinátor többek között gondoskodik a veszélyhelyzet kezelésben érintett személyzet felkészítéséről, a veszélyhelyzeti feladatok ellátása eljárásrendjeinek kidolgozásáról és felülvizsgálatáról, valamint a szövetségi hivatalokkal és magánszektorral történő kapcsolattartásról. [4]

A veszélyhelyzeti tervezéséért és veszélyhelyzeti beavatkozások megtételéért elsősorban a Bizottsági Műveletek (Commission Operations Division) és az Energiaügyi Műveletek (Energy Operations Division) Osztályok felelősek. Ezek az osztályok

- figyelemmel kísérik a michigan-i energia ellátó rendszer működését, feladatuk, hogy azonosítsák az esetleges energia válsághelyzethez vezető problémákat és értesítsék erről az illetékes állami hivatalokat, tisztviselőket;
- felelősek a veszélyhelyzeti tervek kidolgozásáért, koordinálásáért és irányításáért;
- kommunikációs középpont szerepét töltik be a szövetségi-, állami- és helyi energia válsághelyzeti tervezési és kezelési tevékenységek során;
- folyamatos kapcsolatot tartanak fent a kőolaj-, földgáz- és villamosenergia-ipari szereplőkkel. [4]

Az áramkimaradással kapcsolatos események és intézkedések

Michigan államban 6 millió lakos maradt áram nélkül, az áram kimaradások mintegy 2 napon keresztül tartottak. A villamosenergia rendszer összeomlása következtében 2003. augusztus

14.-én délután 4:15-re 2,3 millió fogyasztó maradt áramellátás nélkül. Az érintett áramszolgáltató vállalatok ezt követően még aznap este illetve másnap - augusztus 15.-e folyamán - újabb fogyasztói kieséseket jelentettek. A villamosenergia rendszer helyreállításának előrehaladtával egyre több fogyasztót tudtak visszakapcsolni, augusztus.16.-án reggel 6:30-ra valamennyi fogyasztónál helyreállt az áramszolgáltatás. [4]

Augusztus 15.-én hajnali 12:44-kor a detroiti Marathon olajfinomító jelentette az üzem leállását, az olajfinomító a következő 8 napban üzemen kívül maradt és csak augusztus 23.-án állt újra üzemben. A termelés kiesése jelentős problémákat okozott a térség motorbenzin utánpótlásának biztosításában. [4]

Az áramkimaradás észlelésekor a Michigan-i Közszolgáltatási Bizottság (Michigan Public Service Commission, PSC) személyzetének egy része haladéktalanul megkezdte az áttelepülést az „állami veszélyhelyzeti műveleti központban" (State Emergency Operations Center, SEOC, a továbbiakban: Központ). A Központ saját tartalék áramforrással rendelkezik, világítás, számítógépes hozzáférés és telefonrendszert biztosított a személyzet részére. A személyzet másik része a Közszolgáltatási Bizottság – áramellátás nélküli – irodáiban maradt sötétedésig, mobiltelefonon voltak elérhetőek. [4]

Az áttelepülő személyzet augusztus 14.-én 4:30-kor foglalta el helyét a veszélyhelyzeti műveleti központban és kapcsolatba lépett az érintett áramszolgáltató vállalatokkal valamint az „Energiaügyi Minisztérium" (U.S. Department of Energy, DOE) washington-i „veszélyhelyzeti műveleti központjával" (Emergency Operations Center) adatgyűjtés céljából. [4]

Először az üzemzavar okát és kiterjedését vizsgálták. A Védelmi Minisztérium tájékoztatta a Központot, hogy az áramkimaradás nem terrortámadás következménye. Az üzemzavar okát és eredetét illetően többféle híradás jelent a médiában, a Központ személyzete ezeket próbálta igazolni. Az internetes hírportálokon próbálták nyomon követni az áramszünetről kiadott információt, azonban ez a másod és harmadkézből származó információ nem minden esetben bizonyult hasznosnak. A legfontosabb információforrásnak az „Észak-Amerikai Villamossági Megbízhatósági Tanács" (North American Electric Reliability Council, NERC[1]) bizonyult. [4]

A Központ személyzete folyamatos kapcsolatot tartott a helyi és szövetségi állami és egyéb hivatalokkal, az Energiaügyi Minisztériummal (Department of Energy) és Belbiztonsági Minisztériummal (Department of Homeland Security) illetve a Szövetségi Katasztrófavédelmi Ügynökséggel (Federal Emergency Management Agency, FEMA). Rendszeres volt a kapcsolattartás a michigani Környezetminőségi Minisztérium (Department of Environmental Quality), a Michigani Közszolgáltatási Bizottság, a Michigani Nemzeti Gárda (National Guard), valamint az Amerikai Egyesült Államok Környezetvédelmi Ügynöksége (U.S. Environmental Protection Agency, EPA), az Energiaügyi Minisztérium (Department of Energy) és a Nemzeti Gárda Iroda (National Guard Bureau) között. [4]

Bár alapvetően a kommunikáció jól működött, a tapasztalatok az államok és a szövetségi hivatalok közötti információ megosztás és koordinációs eljárások fejlesztésének, valamint az

[1] A NERC az 1965. évi áramszünetet követően alakult nem-kormányzati szervezet. Feladata az Észak–Amerikát ellátó villamosenergiai-rendszer megbízhatóságának támogatása. A NERC a villamosenergia-ellátó rendszer megbízható üzemeltetését biztosító szabályok, szabványok kidolgozását, fejlesztését és betartását ösztönzi. (2007. január 1-el a Megbízhatósági Tanács (North American Electric Reliability Council) és az Észak-Amerikai Villamossági Megbízhatósági Társaság (North American Electric Reliability Corporation) egyesült. A NERC Társaságot az USA Szövetségi Energiaügyi Szabályozási Bizottsága, (U.S. Federal Energy Regulatory Commission, FERC), 2006. július 20-án „villamossági megbízhatósági szervezetnek" ismerte el) [1]

Energiaügyi Minisztérium és a Belbiztonsági Minisztérium feladat és hatáskörének élesebb elkülönítésének szükségességére mutattak rá. [4]

A kommunikációval kapcsolatos legfontosabb tapasztalatok a jelentés szerint:

- Mind a Belbiztonsági Minisztériumtól (DHS), mind a Katasztrófavédelmi Ügynökség területi szervétől (FEMA Region V) kapott jelentések nem voltak elég lényegre törőek, egymással átfedők voltak, ugyanazokat az információkat tartalmazták.
- A szöveg alapú dokumentumok email-en való küldése hatékonyabb és gyorsabb információ megosztást tett lehetővé, mint faxon történő küldésük.
- A telefonos kommunikáció számára olyan rendszer kell kialakítani – illetve a meglévő rendszert továbbfejleszteni – mely a kereskedelmi telefon rendszerektől független, nem érinti azok esetleges kiesése.
- Az államon belüli kommunikáció kitűnően működött, köszönhetően a Michigan állam által létrehozott 800 MHz-es digitális rádiórendszernek, a „Michigan-i Közbiztonsági Kommunikációs Rendszernek" (Michigan Public Safety Communication System). A rendszerirányító központja és összes antennája saját, független áramellátással rendelkezik, így a rendszerben nem okozott kiesést az áramkimaradás. A rendszert mintegy 374 állami hivatal használja elsődleges rádió kommunikációra is és mintegy 90 hivatal csak veszélyhelyzet kezelési célokra, összesen mintegy 11.000 rádióval. [4]

Az Energiaügyi Minisztérium „Energia Biztosítási Hivatala" (Office of Energy Assurance, OEA) megkezdte egy olyan kommunikációs eljárásmód kidolgozását, mely szisztematikus, gyors és pontos információ megosztást tesz lehetővé az állami és szövetségi kormányok között energia ellátási zavarok esetén. [4]

Augusztus 14.-én délután 6:00-kor a kormányzó és személyzete megérkezett a Központba. Az este folyamán a Közszolgáltatási Bizottság személyzete a kialakult helyzet értékelésén, a helyreállítás időszükségletének megbecslésén dolgozott, valamint az állami kormányzat weblapján megjelentetendő lakossági tájékoztatásokat dolgoztak ki. Folyamatosan tájékoztatták a kormányzati hivatalokat a hatáskörükbe tartozó eseményekről, intézkedésekről, felmerült problémákról. [4]

Augusztus 15-én 10:00-kor a Közszolgáltatási Bizottság kérésére a Detroit Edison – a rendszerösszeomlásban leginkább érintett – áramszolgáltató vállalat képviselői megérkeztek a Központba, ezt követően a Központ személyzete és a Detroit Edison munkatársai folyamatosan figyelemmel kísérték a rendszer helyreállításának folyamatát. Az áramszolgáltatást augusztus 16.-án reggelre valamennyi fogyasztónál helyreállították, de továbbra is önkéntes terheléskorlátozásra volt szükség a rendszeregyensúly megtartásához, mindaddig, amíg elegendő számú erőmű újra nem indult. Amennyiben az aktuális igény meghaladta volna az aktuálisan elérhető erőművi teljesítményt, könnyen újabb kiesések következhettek volna be a villamosenergia rendszerben. Ezért a Központ augusztus 16.-án folytatta működését, fő feladata a rendszeregyensúly helyreállításának figyelemmel kísérése volt. Az egyensúly helyreállítását követően a központ augusztus 17.-én befejezte működését. [4]

Augusztus 18.-án a Közszolgáltatási Bizottság vizsgálatot rendelt el a michigani lakosságot érintő áramkimaradás lefolyásának, időtartamának és okainak kivizsgálására. [4]

A Közszolgáltatási Bizottság és az állam kormányzata a lakosság folyamatos tájékoztatására törekedett. A lakossági tájékoztatás irányelveit a Michigani Energia Válsághelyzeti Műveletek Kézikönyv (Michigan Energy Emergency Operations Manual) rögzíti, ennek megfelelően tájékoztatták a lakosságot a kialakult helyzetről, a helyreállítás

érdekében megtett intézkedésekről valamint arról, hogy a lakosság hogyan és miben segítheti a helyreállítási munkát. Tájékoztatókat helyeztek el a kormányzat honlapján, a kormányzó televíziós beszédben tájékoztatta a lakosságot, a kormányzó és a Közszolgáltatási Bizottság elnöke sajtótájékoztatót tartott valamint a Közszolgáltatási Bizottság sajtóközleményt adott ki, hogy felhívja a lakosságot az árammal való takarékoskodásra. Az áramszünet ideje alatt a kormányzati sajtóiroda kérésére a Közszolgáltatási Bizottság kezelte a sajtómegkereséseket valamint információt tett közzé honlapján. [4]

Augusztus 15.-én délelőtt 9:30-kor az állam kormányzója „rendkívüli állapot" (State of Emergency) kihirdetését rendelte el több megyében (Macomb, Monroe, Oakland, Washtenaw, Wayne). A „rendkívüli állapot" elrendelését augusztus 21.-én vonták vissza. [4]

Augusztus 20.-án az „Energetikai Tanácsadó Bizottság" (Energy Advisory Committee, EAC) elnöke közeledő energia válsághelyzetre hívta fel a kormányzó és a Bizottság figyelmét, a Marathon olajfinomító leállása miatt ugyanis jelentősen lecsökkent az elérhető motorbenzin utánpótlás mennyisége. [4]

Augusztus 21.-én délután 4:00 órakor a kormányzó rendeletében visszavonta az augusztus 15.-én elrendelt rendkívüli állapotot és „energia válsághelyzetet" (Energy Emergency) rendelt el, tekintettel arra, hogy az olajfinomítók leállása miatt veszélybe került Michigan állam motorbenzinnel történő megfelelő ellátása. 7 nappal az olajfinomító üzemének újraindítását követően, szeptember 30.-án, a kormányzó rendeletben visszavonta az „energia válsághelyzetet". [4]

Kritikus infrastruktúrák érintettsége

Michigan államban történtek jó példát nyújtanak a kritikus infrastruktúrák közötti interdependenciák bemutatására is. A továbbiakban – a teljesség igénye nélkül - bemutatunk néhány példát az áramkimaradás a telekommunikációra, az olajiparra és üzemanyag utánpótlásra, víz és szennyvíz ellátásra, élelmiszer ellátásra valamint a közlekedésre gyakorolt hatására. [4]

A mintegy 3 millió ügyfelet kiszolgáló helyi telefonrendszer működőképes maradt, annak ellenére, hogy a hívások mennyisége a normál körülményekhez képest 149%-al megnövekedett, csupán mintegy 50.000 vevő maradt telefonszolgáltatás nélkül valamivel több mint egy órán keresztül. A telefonrendszert üzemeltető SBC társaság tartalék generátorok és akkumulátorok üzembe helyezésével oldotta meg az áramellátás folyamatosságát létesítményeiben. Mintegy 120 iroda és 2.300 távközlési alállomás villamosenergia-ellátását kellett biztosítania átlagosan 28 órán keresztül. [4]

A SBC társaság két nagyobb pótkocsira szerelt generátorral és számos kisebb hordozható generátorral rendelkezett, ezenkívül két nagyobb generátort vett bérbe egy helyi gyártól. A távközlési alállomások akkumulátorait időszakosan újra kellett tölteni. Ezt úgy oldották meg, hogy a technikusok sorra járták az alállomásokat a hordozható generátorokkal és feltöltötték a lemerült akkumulátorokat. A feladatot nehezítette, hogy számos alállomás településektől távol helyezkedik el, melyeket főleg éjszaka nehézkes volt megtalálni. [4]

A generátorok üzemanyag utánpótlása mellett tehát gondoskodni kellett az alállomásokra, vidéki telephelyekre kivonuló hibaelhárító járművek üzemanyag utánpótlásáról is. A megnövekedett üzemanyag igényt a SEOC segítségével tudták biztosítani, a SEOC segítette az üzemeltetőt az elérhető üzemanyag források azonosításában. Az üzemeltető mintegy 650.000 dollár értékben vásárolt 320.000 gallon üzemanyagot. [4]

Tekintettel a helyi telefonhálózatok működőképességének fenntartására a távolsági hívásokban sem jelentkeztek problémák, mivel ezen szolgáltatások elérhetősége a helyi telefonhálózatok működőképességétől függ. Emellett a távolsági hívásokat szolgáltató társaságok mindegyike rendelkezett üzletfolytonossági tervvel és megőrizte működőképességét. [4]

Néhány mobiltelefon-szolgáltató társaságnál volt rövid idejű szolgáltatás kiesés. A generátorok üzemanyag utánpótlása nem jelentett problémát, tekintettel arra, hogy még az üzemanyag kimerülése előtt helyreállt az áramszolgáltatás. [4]

A számítógépes rendszerek – a tartalék áramellátással rendelkező rendszerek kivételével - az áramkimaradás következtében leálltak. A szerverek áramellátásának biztosításán túl a szervertermek hűtéséhez szükséges légkondicionáló rendszerek áramellátásáról is gondoskodni kellett a normál üzem fenntartása érdekében. Az áramkimaradás az állami számítógépes rendszerek többségét érintette, az Informatikai Osztály (Department of Information Technology) irányító központja szintén áramellátás nélkül maradt, ezért beindították a tartalék irányító központot, mely áramellátását tartalék generátorokkal oldották meg. A jelentés hangsúlyozza a katasztrófa-helyreállítási tervezés (disater recovery planning) fontosságára a számítógépes rendszerek esetében. [4]

Az áramkimaradás súlyosan érintette a vízellátó és szennyvízkezelő rendszereket is, leálltak a szennyvíztisztító és víztisztító üzemek, szivattyú állomások, a rendszer ellenőrző telemetria. A michigani „Ivóvíz Biztonsági Törvény” (Michigan Safe Drinking Water Act) előírja, hogy a normál villamosenergia ellátás kiesése esetén is biztosítani kell az ivóvízellátás fenntartását. Ennek érdekében a létesítmények minimum két egymástól független villamosenergia-ellátási útvonallal és/vagy tartalék áramfejlesztőkkel és/vagy megfelelő gravitációs tárolási lehetőséggel kell rendelkezzenek. A térség villamosenergia rendszerének teljes összeomlása miatt azonban a független másod vagy harmad ellátási útvonalak sem működtek, így csak a tartalék áramfejlesztővel rendelkező üzemek tudtak – néhány órán belül – újraindulni. A leginkább érintett térségekben vízkorlátozási intézkedéseket kellett bevezetni. [4]

A szennyvíz elvezető és tisztító rendszerek áram hiányában szintén megbénultak. A tartalék áramfejlesztővel rendelkező rendszerek újra tudtak indulni illetve az áramellátás nélkül maradt létesítményekben a gravitációs gyűjtőkben tudták tartani a szennyvizet. Miután a szennyvíz csatornák és tárolók megteltek, az üzemeltetők két alternatíva közül választhattak: vagy engedik a szennyvizet visszafolyni a lakossági épültekbe, ami számos nagyon súlyos egészségügyi következménnyel járt volna, vagy a fogadó természetes vizek felé engedi „kiönteni” a felesleget. (A kiöntés előtt általában részlegesen kezelni illetve fertőtleníteni tudták a szennyvizet). [4]

A Detroit Marathon olajfinomítót mind az áramkimaradás, mint a vízellátási problémák érintették. Az áramkimaradás kezdetekor az üzemben vészleállítást hajtottak végre. Az eljárás részeként a feldolgozás alatt levő kőolaj származékokat biztonságos módon elégették, ennek lángja jól látható volt a térségben. A vészleállás alatt robbanás történt az egyik szén-monoxid kazánban, mely szénhidrogén keverék és gőzkibocsátással járt. Bár az olajfinomító vizsgálatai alapján a kibocsátás nem tartalmazott mérgező anyagot, benzol és hidrogén-szulfid jelenlétét kizárták, a környező lakosságot kitelepítették és az olajfinomító közelében futó főutat átmenetileg lezárták a kitelepítés megkönnyítése érdekében. A szénhidrogén szivárgást másnap (2003. augusztus 15.) reggelre megszüntették, a Környezetvédelmi Ügynökség (EPA) levegőminőségi méréseit követően a lakosság a délután folyamán visszaköltözhetett. [4]

A Marathon olajfinomító naponta 74.000 hordó nyersolajat dolgozott fel és többfajta kőolajszármazékot állított elő, leginkább motorbenzint. A becslések szerint a finomító a

detroit-i körzet motorbenzin igényének 38%-át fedezte. Az áramkimaradás következtében a több kisebb olajfinomítójában szintén 1-2 napra leállt a termelés. A kiesett motorbenzin termelés Michigan állam napi felhasználásának 2/3 részének felelt meg, mindezek következtében üzemanyag hiány alakult ki. [4]

A térség benzinkutjainak mintegy 9%-a tudott üzemben maradni az áramszünet ideje alatt. A lakosság valósággal megrohanta ezeket. A benzinkutak egy része – a személyzet és a berendezések biztonságát féltve – éppen a lakossági roham miatt zárt be. A nyitva tartó benzinkutak sem tudták a benzin utánpótlást biztosítani, mivel a benzinszállító járműveket nem indították el a veszélyes közúti helyzet miatt. A tömeg és a forgalom kezelése jelentős rendőri erőket kötött le egészen az áramellátás augusztus 16-i helyreállításáig. [4]

A lakossági élelmiszer ellátás számára a romlandó élelmiszerek hűtésének megoldása jelentette a legnagyobb kihívást az áramszünet ideje alatt. A nagyobb élelmiszer kereskedelmi hálózatok – üzletfolytonossági terveik szerint – boltjaikban a hűtést megoldották, a kisebb hálózatok boltjaiban és az éttermekben azonban nem. A hűtés hiányában megromlott élelmiszerek elszállítása sem volt megoldott, egyrészt azért, mert a hulladékszállító társaságok nem vállalták a szerződéses kötelezettségeiket meghaladó szállításokat, másrészt a hulladéklerakók a hétvége folyamán nem voltak elérhetőek. (Az áramkimaradás augusztus 14-én csütörtök este kezdődött, az áramellátás augusztus 16-án szombaton reggelre állt csak helyre teljesen). [4]

A közlekedési rendszerekben szintén jelentős fennakadásokat okozott az áramkimaradás:

- Nem működtek a közlekedési lámpák, a forgalmasabb kereszteződésekben rendőrök irányították a forgalmat.
- A mélyebbe fekvő autópályák mentén szivattyúkat használnak a vízátfolyások megakadályozására. Az áramszünet ideje alatt a szivattyúk áramellátását hordozható áramfejlesztőkkel oldották meg, mely az üzemeltető személyzet folyamatos munkáját igényelte. Az egyidejű heves esőzések miatt több autópályát így is átmenetileg le kellett zárni.
- A „Michigani Intelligens Közlekedési Rendszer Központ” (Michigan Intelligent Transportation System Center) áramellátása teljesen megszűnt. A video kamerák és az elektronikus „üzenőfalak” lekapcsoltak, a Központ weboldala nem volt elérhető. A kommunikáció az autópálya járőrökkel, a médiával és a Michigani Közlekedési Minisztériummal (Michigan Department of Transportation) gyakorlatilag megszűnt.
- Egyes alagutakat a szellőztető rendszer leállása miatt le kellett zárni.
- Az USA legforgalmasabb kereskedelmi szárazföldi kikötőjében torlódás alakult ki a számítógépes rendszerek leállása miatt.[2]
- A Metropolitan Detroit Airport repteret augusztus 14-én éjfélig lezárták. [4]

[2] Az amerikai vámhatóság számítógépei csak néhány másodpercre álltak le, majd a tartalék áramfejlesztőkről újraindultak. A kanadai vámhatóság számítógépein azonban megszűnt az adatkapcsolat és ezzel a teherszállítási rakományjegyzékek elektronikus ellenőrzése is. Vizuálisan és manuálisan kellett megvizsgálniuk az rakományjegyzéket és szükség esetén a rakományt is. Mindez jelentősen lelassította a forgalmat, az amerikai oldalon mintegy 4 mérföldes sor alakult ki csaknem 24 órán keresztül. [4]

Az esettanulmány tapasztalatainak összefoglalása

A vizsgált esettanulmány alapján az alábbi főbb tanulságokat emelhetjük ki:

- A tartós áramkimaradás következtében előállt helyzet kezelésében érintett szervezeteknek két alapvető problémakörrel kellett megküzdeniük:
    - a lehető legrövidebb időn belül helyre kellett állítani a kiesett szolgáltatásokat,
    - gondoskodni kellett a lakosság biztonságának fenntartásáról.
- A helyzet sikeres kezeléséhez kulcs fontosságú a kritikus infrastruktúrák közötti inderdependenciák figyelembe vétele, lehetséges kölcsönhatások ismerete.
- Alapvető fontosságú a személyzet megfelelő felkészítése a veszélyhelyzetek kezelésére mind az érintett állami szervek, mind a kritikus infrastruktúrákat üzemeltető magáncégek esetében. Különösen fontos az állami és az üzemeltető magán cégek együttműködése mind a veszélyhelyzeti tervezés mind a beavatkozás szintjén.
- A veszélyhelyzet kezelésben érintett állami szervezetek részére biztosítani kell a tervezéshez és beavatkozáshoz szükséges erőforrásokat, a megfelelő finanszírozást, a szükséges felszerelés rendelkezésre állását.
- A veszélyhelyzeti eljárásrendek, tervek, útmutatókat rendszeresen felül kell vizsgálni és naprakészen kell tartani. Fontos a veszélyhelyzet kezelésben érintett állami szervezetek, üzemeltető vállalatok veszélyhelyzetben értesítendő munkatársai elérhetőségi adatainak rendszeres felülvizsgálata és naprakészen tartása is.
- A veszélyhelyzet kezelésben résztvevő személyzetet előzetes ki kell jelölni és fel kell készíteni a veszélyhelyzeti eljárásrendek ismeretére és alkalmazására.
- Fontos az események pontos és teljes körű dokumentálása mind az események nyomon követéséhez, mind az utólagos kiértékeléshez.
- Kulcs fontosságú a veszélyhelyzet kezelésében résztvevő intézmények, szervezetek feladat, felelősség és hatáskörének egyértelmű megszabása.
- Az energia ellátási válsághelyzet sikeres kezeléséhez elengedhetetlen, hogy a helyzet kezeléséért felelős szervezetek számára naprakész háttérinformáció álljon rendelkezésre az energia ellátási válsághelyzetben és kezelésében esetlegesen érintett rendszerekről és infrastruktúrákról. Célszerű ezeket az anyagokat mind elektronikus, mint nyomtatott formában előállítani, tekintettel arra, hogy az elektronikus információ elérhetősége áramszünet idején nem feltétlenül biztosított.

KATASZTRÓFAVÉDELEM, POLGÁRI VÉDELEM, VESZÉLYHELYZET KEZELÉS ÉS VILLAMOSENERGIA-KRÍZIS KEZELÉS SZABÁLYOZÁSA MAGYARORSZÁGON

E rövid és teljesség igényét nélkülöző betekintés alapján számos párhuzamot vélhetünk felfedezni a 2003. évi nagy amerikai áramszünet következtében kialakult helyzet kezelésében Michigan állam példáján bemutatott és a magyarországi, a katasztrófavédelemben, polgári védelemben és villamosenergia krízis kezelésében érintett szervek között.

Magyarországon a katasztrófák elleni védekezés irányításáról, és szervezetéről az 1999. évi LXXIV. törvény (továbbiakban: Katasztrófavédelmi törvény) [5] rendelkezik. Ez a törvény, illetve a végrehajtásáról szóló 179/1999 (XII.10) kormányrendelet [6] határozza meg a katasztrófák elleni védekezés irányításának szervezetét, a Kormány feladatait és intézkedéseit,

a védekezés irányításában résztvevő szervek valamint a katasztrófavédelem végrehajtását végző szervek feladatat és hatáskörét. A katasztrófavédelmi feladatok tárcák közötti koordinációját a Kormányzati Koordinációs Bizottság (továbbiakban KKB) látja el. A KKB állandó jelleggel Titkárságot, Veszélyhelyzeti Központot, valamint katasztrófahelyzetben Operatív Törzset és védekezési munkabizottságot működtet.

Az esettanulmányból láthattuk, hogy a legkorábbi beavatkozó szerv a tűzoltóság volt. Hazánkban ehhez hasonlóan a tűzoltóság kezdi meg az elsődleges beavatkozási és mentési feladatokat. az áramkimaradás következtében kialakult helyzet kezelése során a rendőrségi erőkre is számos feladat hárult, hasonló helyzetben nem lenne ez másképp hazánkban sem. A rendőrség és a tűzoltóság katasztrófavédelmi feladatait hazánkban a 48/1999. (XII.15.) BM rendelet [7] rögzíti.

A polgári védelemről szóló 1996. évi XXXVII. törvény [8] értelmében veszélyhelyzet[3] esetén a lakosság védelmével kapcsolatos feladatok a polgári védelem feladatkörébe tartoznak, végrehajtásukban államigazgatási szervek, önkormányzati és hivatásos (területi, települési, munkahelyi) polgári védelmi szervek, valamint közreműködőként a Magyar Honvédség és rendvédelmi szervek vesznek részt.

Az IAFC vizsgálata alapján készült tanulmány [3] szerint a 2003. augusztusi áramszünet következtében kialakult helyzetet sikeres kezelésének egyik alapja a megfelelő tervezés volt. A hazai szabályozás szintén nagy hangsúlyt fektet a tervezésre. A polgári védelmi és veszélyhelyzet elhárítási tervezésről a 20/1998 (IV.10.) BM rendelet [9], az ún. Riasztási és Segítségnyújtási terv készítéséről a 32/2009. (XI.30) ÖM rendelet [10] rendelkezik.

Michigan állam példáján bemutattuk, hogy a Kormányzó rendkívüli események esetén „veszélyhelyzetet", energia ellátási problémák esetén „energia válsághelyzetet", illetve katasztrófához vezető események fellépése esetén „katasztrófahelyzetet" rendelhet el. Ezen helyzetekben a Kormányzó rendkívüli intézkedések rendeletben történő előírására jogosult. Hazánkban hasonló módon a Katasztrófavédelmi törvény értelmében veszélyhelyzet kihirdetését igénylő méretű katasztrófahelyzetben a Kormány rendeletben hirdeti ki a veszélyhelyzetet és a Magyar Honvédségről szóló 2004. évi CV. Törvény (továbbiakban: Honvédelmi törvény) 149. § (3) bekezdésében meghatározott rendkívüli intézkedéseket vezethet be. A törvény végrehajtási rendelete (179/2009. Korm. r.) értelmében katasztrófa esetén szintén a Kormány jogosult az érintett területet katasztrófa sújtotta területté nyilvánítani.

Az esettanulmány alapján a michigani állami minisztériumok mindegyik részt vesz a fent nevezett rendkívüli helyzetek kezelésében, a minisztériumok ún. Veszélyhelyzet Kezelési Koordinátort jelölnek ki. Ez a magyar Kormányzati Koordinációs Bizottságra emlékeztet, amelyben a minisztériumok és az állami hatáskörű szervek vezetői vesznek részt. Megjegyzendő, hogy a michigani Veszélyhelyzet Kezelési Koordinátoroknak jóval szűkebb a feladat és hatásköre mind az a KKB esetében.

Az esettanulmányban említett Szövetségi Katasztrófavédelmi Ügynökség illetve regionális szervezetei az Országos Katasztrófavédelmi Főigazgatóság központi, területi és helyi szerveihez hasonlóak.

Az esettanulmányban bemutatott energia válsághelyzet fogalomhoz képest a magyar szabályozás – legalábbis a villamosenergia-ellátás tekintetében - a villamosenergia-ellátási zavarokat több fokozatban kezeli. A Krízisrendelet jelentős zavar, válsághelyzet veszélye és válsághelyzet fogalmakkal dolgozik, melyeket együttesen krízisnek nevez, a különböző

[3] A veszélyhelyzet fogalmát a törvény 2. §. (2) bekezdése határozza meg.

fokozatok esetén eltérő rendelkezések alkalmazását írja elő. Az alkalmazandó intézkedések szabályait, az alapvető feladatokat, felelősségi és hatásköröket a villamos energiáról szóló 2007. évi LXXXVI. törvény valamint a villamosenergia-rendszer jelentős zavara és a villamosenergia-ellátási válsághelyzet esetén szükséges intézkedésekről szóló 285/2007. (X. 29.) Kormányrendelet (továbbiakban: Krízisrendelet) állapítja meg. A Krízisrendelet - többek között – az intézkedéseket részletező ún. Krízisterv elkészítését és ún. Krízis Munkabizottság működtetését írja elő. A Krízis Munkabizottság munkájában mind a villamosenergia-ipar szereplői mind állami szereplők részt vesznek. [11]

Érdekes, hogy a michigani esettanulmányban nincs – vagy legalábbis a PSC jelentése nem említi – olyan testület létezését, melyben a villamosenergia-ipar szereplői és állami szereplők együttesen vesznek részt a villamosenergia krízisek megelőzése, kezelésére történő felkészülés és elhárítása érdekében. Az esettanulmányban bemutatott Energetikai Tanácsadó Bizottság feladatköre – legalábbis a villamosenergia-ellátás tekintetében – emlékeztet a Krízis Munkabizottságéra, azonban ebben nem vesznek részt ipari szereplők.

A két szervezet különbözőségeit vizsgálva megemlítendő, hogy míg az esettanulmány szerinti Energetikai Tanácsadó Bizottságban tag a Közegészségügyi Minisztérium igazgatója, a Krízis Munkabizottságban az állami szervek részéről nem jelenik meg közvetlenül az egészségügyi terület. Egy esetleges (villamos)energia-krízis, az esettanulmányban bemutatott hosszan tartó áramkimaradás akár közvetlenül, akár más kritikus infrastruktúrák működésében kiváltott zavarokon keresztül számos egészségügyi feladatot[4] vethet fel, mint ahogy azt az esettanulmányban láthattuk, így talán az egészségügyi terület – a többi állami minisztériumhoz hasonló módon – tanácskozási illetve tájékoztatási joggal történő részvétele indokolt lehetne a Krízis Munkabizottság munkájában, vagy legalábbis annak a területet érintő vonatkozásaiban.

További, részletesebb következtetések levonására a jelen tanulmány készítése keretében megvizsgált adatok alapján nem vállalkozhatunk, az a jelenleginél sokkal részletesebb vizsgálatot igényelne. Ez az igencsak lényeges és érdekes kérdés egy újabb tanulmány témája lehetne.

AZ ENERGIABIZTONSÁGI KÖZPONT LEHETSÉGES SZEREPE A HOSSZAN TARTÓ ÁRAMKIMARADÁSOKRA TÖRTÉNŐ FELKÉSZÜLÉSBEN

A vizsgált esettanulmány is rámutat arra, hogy a villamosenergia ellátás egy esetleges hosszan tartó kimaradása milyen szerteágazó, egymással kölcsönhatásban álló és összetett problémákat vett fel, melyek kezelésében számos különböző szervezet érintett. Az ilyen események megelőzése és kezelésére történő felkészülés összetett feladatinak ellátására olyan új típusú intézményre van szükség, mely a problémamegoldás minőségileg új képességeit tudja biztosítani. Az energia ellátási problémák kezelése terén ilyen új intézmény lehet egy ún. Energiabiztonsági Központ (továbbiakban Központ).

Meggyőződésünk, hogy e komplex problémák megoldásához szükséges szaktudás akár hazai, akár nemzetközi szinten rendelkezésre áll, így a Központ feladata nem a különböző kapcsolódó szaktudások megteremtése, hanem azok olyan módon történő „összefogása”, hogy a fellépő szinergiák révén minőségileg új tudás és képességek alakuljanak ki.

[4] pl. egészségügyi létesítmények villamosenergia ellátásának biztosítása áramkimaradás esetén; elektromos árammal működő, az egészség vagy az élet fenntartásához szükséges egészségügyi eszközt használó betegek kezelése, villamosenergia ellátásának biztosítása áramkimaradás esetén; a hűtés nélkül maradt romlandó élelmiszerek, a vízellátás és szennyvízkezelés zavarai következtében kialakuló fertőzésveszély stb.

A Központ koncepciójának [12] alapulvételével a villamosenergia-ellátási krízishelyzetek kezelésére történő felkészülés terén a Központ az alábbi alapfunkciókat valósíthatná meg:

1. Villamosenergia-krízisre történő felkészüléshez, tervezéshez, helyzetértékeléshez és felkészítéshez valamint mindezek szabályozásának kialakításához szükséges ismeretek, információ hatékony, gyors előállítása.

   Ezen funkció megvalósításához a Központban elemző-értékelő kapacitásokat kell kialakítani. A Központ feladata lehetne pl.:

   - esettanulmányok, szimulációk elemző értékelése, legjobb gyakorlatok azonosítása;
   - adatbázisok felállítása, tervezéshez szükséges információk begyűjtése, rendszerezése, rendelkezésre bocsátásának biztosítása a tervezésben érintett szervezetek részére;
   - elemzési, tervezési és felkészítési módszertanok fejlesztése;
   - a megfelelő szabályozás kidolgozásához illetve továbbfejlesztéséhez szükséges információ előállítása, rendszerezése és közvetítése a szabályozó hatóságok felé.

2. A villamosenergia-krízis helyzetek kezeléséhez szükséges tapasztalati tudás megszerzésének felgyorsítása.

   A tapasztalati tudás megszerzésének alapvető eszközei a különböző modellezési eljáráson alapuló szimulációs módszertanok. A Központ feladat lehetne olyan modellek, modellezési eljárások fejlesztése, melyek lehetővé teszik

   - a villamosenergia-ellátás különböző mértékű zavarainak más kritikus infrastruktúrák működésére illetve más kritikus infrastruktúrák zavarainak a villamosenergia-ellátásra, valamint mindezek a lakosság életére gyakorolt hatásainak vizsgálatát;
   - a hatások vizsgálatát extrém (pl. időjárási) körülmények között és/vagy több olyan rendkívüli esemény egyidejű fellépése esetén, melyek önmagukban nem, együttesen azonban súlyos zavarokhoz vezethetnek vagy ellehetetlenítik a helyreállítási érdekében szükséges intézkedések végrehajtását;
   - ezen hatások megelőzését és következményeinek csökkentését célzó intézkedési tervek eredményességének és hatékonyságának „tesztelését”, a különböző beavatkozási, intézkedési tervek megvalósításának feltételeinek illetve lehetőségeinek vizsgálatát a villamosenergia ellátás különböző mértékű zavarai esetén;
   - különböző, a feladatok végrehajtásában érintett szervezetek, szakemberek hatékony felkészítését célzó gyakorlatok lebonyolítását.

3. Hatékony tudástranszfer kialakítása, fenntartása, folyamatos továbbfejlesztése, krízishelyzet kezeléséhez szükséges tapasztalatok, ismeret átadás minőségileg új alapokra helyezése, a legjobb gyakorlat közvetítése.

   Ennek keretében pl.:

   - széleskörű tudástranszfer szervezése a különböző állami, ipari és krízishelyzet kezelésben érintett egyéb szereplők között;
   - tudástranszfer szervezése a témában érintett hazai, európai és nemzetközi szervezetek között;
   - tudományos konferenciák szervezése a tapasztalatok kiértékelésére, legjobb gyakorlat közvetítésére

- közös gyakorlatok szervezése a témában érintett állami és ipari szereplők között, egymás feladat és hatáskörének megismerése, megértése érdekében

ÖSSZEFOGLALÁS

A 2003 augusztusában Észak-Amerikában bekövetkezett áramszünet tapasztalatai is igazolják, hogy egy esetleges tartós és nagy kiterjedésű áramkimaradás milyen rendkívüli helyzethez vezethet. Az ilyen sajnálatos események vizsgálata, elemzése számos tanulsággal szolgálhat az ilyen események elkerüléséhez illetve kezeléséhez.

A 2003 augusztusában Michigan államban történtek példáján áttekintettük az áramszünet hatásait, más kritikus infrastruktúrák érintettségét, a felmerült lakosságvédelmi feladatokat, a válsághelyzet kezelésben résztvevő szervezeteket, a legfontosabb intézkedéseket és tapasztalatokat.

A teljesség igénye nélkül bemutattunk néhány párhuzamot és eltérést a válsághelyzet kezelés michigani és magyarországi szabályozásában, néhány érdekesség kiemelésén túl részletes következtetések levonására jelen közlemény keretében nem vállalkoztunk.

Az esettanulmány alapján megmutattuk, hogy a helyzet kezelésében kulcs fontosságú

- a kritikus infrastruktúrák közötti inderdependenciák figyelembe vétele, lehetséges kölcsönhatások ismerete.
- a megfelelő tervezés és felkészítés mind az érintett állami szervek, mind a kritikus infrastruktúrákat üzemeltető magáncégek esetében.
- az állami és az üzemeltető magán cégek együttműködése mind a veszélyhelyzeti tervezés mind a beavatkozás szintjén.
- a tervezési és beavatkozási tevékenységhez szükséges erőforrások biztosítása.

A fentiekkel kapcsolatos komplex feladatok megoldásához hatékony segítséget nyújthatna az ún. Energiabiztonsági Központ a feladatok megoldásához szükséges új ismeret előállításával, tapasztalati tudás megszerzésének felgyorsításával és tudástranszfer megvalósításával.

Irodalomjegyzék

[1] Körmendi Krisztina – Solymosi József: A villamosenergia-ellátás zavarának kialakulása és okai a 2003. augusztusi „nagy észak-amerikai” áramszünet példáján. Hadmérnök III. évfolyam 1. szám – 2008. március http://www.hadmernok.hu/archivum/2008/1/2008_1_kormendi.html, letöltés ideje: 2010.05.21

[2] Knowledgerush: 2003 North America blackout http://www.knowledgerush.com/kr/encyclopedia/2003_North_America_blackout/ letöltés ideje: 2010.05.21

[3] International Assiciation of Fire Chiefs: Performance of the Fire Service during the 2003 Northeast Blackout and the Implications for Critical Infrastructure Protection. 2003. November http://www.iafc.org/associations/4685/files/NE_blackout_report.pdf letöltés ideje: 2010.05.22

[4] Michigan Public Service Commission: Report on August 14th Blackout. November 2003

http://www2.tech.purdue.edu/eet/courses/eet331/blackout/Michigan_blackout_report.pdf letöltés ideje: 2010.05.22

[5] 1999. évi LXXIV. törvény a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről (https://kereses.magyarorszag.hu/jogszabalykereso a jogszabály 2010.06.01-én hatályos változata)

[6] 179/1999. (XII.10.) Korm. rendelet a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 1999. évi LXXIV. törvény végrehajtásáról (https://kereses.magyarorszag.hu/jogszabalykereso a jogszabály 2010.06.01-én hatályos változata)

[7] 48/1999 (XII.15) BM rendelet a belügyminiszter feladatairól és a védekezés végrehajtásának rendjéről, valamint e szervek irányítási és működési rendjéről (https://kereses.magyarorszag.hu/jogszabalykereso a jogszabály 2010.06.01-én hatályos változata)

[8] 1996. évi XXXVII. törvény a polgári védelemről (https://kereses.magyarorszag.hu/jogszabalykereso a jogszabály 2010.06.01-én hatályos változata)

[9] 20/1998 (IV.10.) BM rendelet a polgári védelmi tervezés rendszeréről és követelményeiről (https://kereses.magyarorszag.hu/jogszabalykereso a jogszabály 2010.06.01-én hatályos változata)

[10] 32/2009. (XI. 30.) ÖM rendelet a tűzoltóságok legkisebb erő- és eszközállományáról, a Riasztási és Segítségnyújtási Tervről, a működési területről, valamint a tűzoltóságok vonulásaival kapcsolatos költségek megtérítéséről (https://kereses.magyarorszag.hu/jogszabalykereso a jogszabály 2010.06.01-én hatályos változata)

[11] Körmendi Krisztina – Solymosi József: A villamosenergia-krízis kezelés szabályozása Magyarországon. Hadmérnök III. évfolyam 2.szám – 2008 június http://www.hadmernok.hu/archivum/2008/2/2008_2_kormendi.html (letöltés ideje: 2010.06.01)

[12] Nagy Károly: Energiabiztonsági központok. Hadmérnök III. évfolyam 1. szám – 2008. március http://www.hadmernok.hu/archivum/2008/1/2008_1_nagy.html (letöltés ideje 2010.05.31)

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Pántya Péter
panpet1@freemail.hu

INEXPENSIVE DRILL-CONTAINER FOR FIREFIGHTERS

Absztrakt / Abstract

A tűzoltók gyakorlati képzése elsőrendű fontosságú terület minden tűzoltóságnál, jogviszonytól (hivatásos, önkéntes, létesítményi) és országtól függetlenül. A gyakorlati képzéshez az éles, tűz közeli lehetőségek biztosítják a legjobb alapot. A már kiépített gyakorlati pályák használata viszonylag magas költséggel oldható meg, ehhez járul a viszonylag kötöttebb szimulációs lehetőség. A cikkben egy, már több országban kipróbált, egyszerű, olcsó, de hatékony gyakorlati kiképzési forma ismerhető meg, házilag építhető szimulációs konténer formájában. Az akár minden tűzoltóság területén kis költségből felépíthető építmény újszerű kiképzési lehetőségeket is kipróbálni enged.

The practical training of firefighters is of primary importance at all fire departments of all employment types (career, volunteer and on-site) in any country. The best basis for practical training is given by opportunities to be in near-fire situations. Use the practice facilities, which have already been built up can only, at a relatively high cost combined with the limited possibilities for simulation. The article describes a simple, cost-effective, yet efficient practical training method that has already been tested in several countries and can be home-built in the form of a container simulator. This facility, which can be built even on the area of all fire department at a low cost, allows the testing of novel practical possibilities.

Kulcsszavak/Keywords: *tűzoltó, gyakorlat, szimulációs konténer ~ fire fighter, drilling, container simulator*

No firefighter organization of any country is overfunded. Of course, there are differences in this regard, yet, resources are never unlimited. Finances greatly influence many fields of the profession including training possibilities; however, a firefighter is essentially ingenious and tries to make the most of less. I will describe below a low cost solution for examining closed area-fires as well as practicing methods of intervention.

There are large-scale, high-standard, high-quality training centers with different training tracks in many countries. The different intervention methods – from technical rescue, fire extinguishing to high altitude rescue - can be taught on these training tracks. Certainly, this is the most expensive and most effective way of training; on the other hand, this is not available all the time on an unlimited basis to the entire firefighter troop of the given country. Therefore, we are faced with a demand.



Pictures 1-2. Container simulators of Hungarian Disaster Recovery Learning Center - outer superstructure and inner area during operation,
(Source: www.langlovagok.hu, 2009.)

Today, mobile container fire-simulators have become available (such as Fire Dragon), which are excellent tools for examining closed area fires and methods of intervention. Their use, compared to fixed facilities, are a lot more versatile, have unlimited mobility, and their operation is more efficient, cost-effective.





Pictures 3-6. Container fire-simulators from different manufacturers at Interschutz 2010 (Own pictures)

The systems of exercises ensure the skills-maintenance of the emergency standby troop. There can be no question about their necessity for those who work in the field and as I talk to people in professional circles and read the professional literature, I see that there is a demand for such exercises on the part of those concerned.

All commanders hold the practice of fire extinguishing - and to have fire extinguishing practiced - of primary importance. Similarly significant is the examination of induced fire events and those occurring in real-life. I do not deny that the training possibilities on mobile container simulators or built premises facilitate conducting the largest-scale exercises; however, they take larger organizing efforts to and require greater input of funds.

Here is an alternative:

Home-built training course



Picture 7. "Fire-cell" built for examining closed area fire (Source: Fire Department, Pécs, Hungary, 2009.)

Those who need to make due with less (especially the carrier and volunteer fire departments of modestly funded local governments) may find the buildable drill-house advantageous which can be build in the yard of any barracks in a few days and can be optionally designed. Fire events can be created and examined within or outside of it repeatedly. Intervention drills can be held applying different methods even for the entire troop any day of the year. Cooperation exercises can be organized with partner law enforcement organizations according to needs in a constructed environment. This does not necessitate major funding.

A great advantage of "home constructed" drill-courses is that the standby personnel will not miss out on the different events either, because even if the building is not put up in the barracks yard, most probably it can be constructed in the vicinity of the fire station.

Members of the Pécs Fire Department personnel in Hungary made great use of the "home built drilling course" in question. A light structure, couple of square meter drilling house has been built and tested there on several occasions. This article was inspired by this simple training possibility (special thanks to lieutenant-colonel Péter Handbauer). Materials recommended for use and other ideas were taken from here. Before someone should embark on the building attention must be paid to environmental concerns during construction and use. However, it may be unnecessary to call the reader's attention to the importance of environmental considerations in the year of 2011.

Similar solutions are used for drilling purposes by the firemen of the United States of America and drawing on their experience, in a significantly more cost effective fashion, for about 200-300 Euros – not counting living labor – the construction of a smaller, one or two room hut can be implemented. It is easy to build a street section in the environment of the drilling-house using car-wrecks from the salvage yard, fire hydrants and other accessories which do not significantly increase costs, although, largely expand utilization possibilities.

The so called "flashover" phenomena, that is, the almost simultaneous ignition of objects found nearby with very rapid flame-spreading can be simulated at the constructed house. [2] It is also possible to examine the "rollover" that is, the phenomena occurring before flashover with arching flames.



Pictures 8-9. Light-structure fire drilling facility with initial fire and forming of "fire-blanket" at the Berettyóújfalu Fire Department, Own picture

When creating the fire event using distant reading thermometer and/or heat camera the various stages of fire development can be examined, the different behavior of the pieces of furniture in fire. For those working in the fire-prevention field many possibilities open for conducting different experiments and fire examination methods.

As part of an open day, representatives of fire departments (carrier, volunteer, on-site), partner organizations, institutions involved, students from schools - for recruitment purposes people wanting to join the department - the media and of course the residents living in the nearby area can be invited to practice, analyze and examine events taking place within or in the vicinity of the drilling house. Fire department propaganda can be a very useful tool.

Here are a couple pieces of useful advice from experience for those who are planning on building:

- Prior inquiries about environmental permissions
- Thoroughly treated and protected wood frame can last longer than metal ones.
- During furnishing it is important to keep in mind that the exercise/demonstration should be smooth and realistic. Attention must be paid to positioning and materials of the furniture.
- The facility can easily be built of OSB boards, sheetrock, although, if the facility is intended for repeated use, the protection of heat-exposed areas and screw heads should be taken into consideration.
- Deficient, second class, salvaged materials will suffice in unimportant parts for construction.
- The recommended place for fire ignition is one of the corners, where it is advisable to hide further ignition materials for the sure success of the demonstration.
- The face opening is more than sufficient in case of construction based on the provided data. Cutting further apertures in this kind of implementation is not practical.
- A more spectacular effect can be achieved using wall to wall carpets.
- It is recommended to fill with water the plastic bottles used as furnishing articles.
- Placing pictures and tapestry on the wall also increase the effect.
- In case of a fire examination exercise very visible marks may be left if the facility is realistically furnished.
- For smoke creation use of foam sponge and synthetic materials is justified.
- There can be a great loss of heat if simple sheet walls are used which can adversely affect the exercises, experiments.
- It is strongly recommended to hold a rehearsal before major demonstrations.

SUMMARY

Creating the conditions for closed area “near fire” training of fire department personnel entail very high costs. I recommend the construction of low-cost low-labor drilling house described in this article for all fire departments (whether career or volunteer) which have an appropriate place for this and can implement the construction of the drilling house to a greater or smaller extent, with possible add-ons. This is highly recommended for fire departments located relatively far from the available drilling courses. If all fire departments had similarly implemented facilities local conditions special to the area could be tested, tried at any given time of the year or day without separate outside organizing.

LITERATURE

[1] Pimper, László: Fire drilling course at MOL Nyrt’s Danube Refinery. (Tűzoltó gyakorlópálya a MOL Nyrt. Dunai Finomítójában), www.vedelem.hu, ISSN: 1218-2958. (downloaded: 04. January 2010.)

[2] Grimwood, Paul T. : Flashover: a firefighter´s worst nightmare. Journal "Fire&Rescue" p. 21-23. April. 2003., ISSN: 0964-9727

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Szalkai Attila
aszalkai@hotmail.com

SECURITY POLITICAL ANALYSIS OF FRESHWATER POLLUTION IN VIEW OF HYDROCOOPERATIONS

Absztrakt/Abstract

A vízszennyezés napjaink egyik legsúlyosabb környezetvédelmi problémája. Tekintettel arra, hogy a víz minőségének romlása a felhasználható édesvíz mennyiségének csökkenését okozza, vízhiányos régiókban fontos biztonságpolitikai tényezőként jelenhet meg. A vízszennyezés azonban nem kizárólag a vízhiánnyal küszködő területeken jelent kihívást. A Földön egyre kevesebb ember jut egészséges ivóvízhez, és ezzel arányosan nő a szennyezett vízhez kapcsolható megbetegedések és halálesetek száma. Több ország által birtokolt vízbázisok esetében a vízszennyezés elterjedésének megakadályozása, és a probléma mielőbbi megoldása kizárólag közös együttműködések révén valósítható meg. Az édesvíz készletek minőségének megőrzése érdekében létrehozott hidrokooperációk elengedhetetlen feltételei a közös vízfelhasználás biztonságának.

Water pollution is one of the most oppressive environmental problems in these days. Regarding that the ruin in water quality leads to the diminution in the amount of freshwater, it can emerge as an important factor in security policy in areas short of water. However, water pollution means a challenge not only in such areas. Access to healthy drinking water is constantly decreasing on the Earth, and parallel to this phenomenon, the number of diseases and casualties related to polluted water increases pro rata. In case of water bases owned by several countries, prevention of the spread of water pollution and the earliest elimination of the problem can only be feasible by means of mutual cooperation. The hydrocooperations established to support the conservation of freshwater stocks' quality are indispensable provisos of the security of common water use.

Kulcsszavak/Keywords: *vízszennyezés, hidrokooperáció, hidroszolidalitás, környezetvédelem, vízhiány ~ water pollution, hydrocooperation, hydrosolidarity, conservation, water shortage*

INTRODUCTION

Water shortage, which has affected an increasing part of the Earth, has been becoming a more and more dominant risk factor for the security of the endangered regions. The problem of freshwater shortage is not solely represented by the practical lack of water. Living organisms, mostly humans can only preserve their health by consuming water of defined clearness: so besides quantitative conditions, claims on water from global water stocks also have qualitative conditions. The disproportionately vast appearance of polluted freshwater inadequate for human and animal consumption or agricultural utilization can result in the development, spread or deepening of water shortage risks.

According to UNICEF's survey, the number of people who have no access to healthy drinking water is more than 884 million in the developing countries, which gives more than 39 per cent of the population in Middle and Western Africa. [1] Regular consumption of polluted water can lead to various diseases. According to the standpoint of World Health Organization and United Nations, almost half of the Third World's population suffer from any of the contaminated water borne diseases. The different diseases having evolved due to of the lack of clear drinking water and the related basic hygiene affect almost 3, 34 billion people annually all over the world. [2] Nearly fifty per cent of the casualties are caused by infections, and thirty per cent of them are generated by diseases derived from parasites. Data and results are included in the Table 1.

The growing demand for water that has arised along with the population boom and urbanization, and beyond this, the fact that most of the developing countries still lack the basic water infrastructure network, all contribute to a great extent to the increase of water pollution. According to forecasts, in the next twenty-five years the number of those who lack adequate drinking water and drainage network can become doubled and the excessive environmental pollution will result in the becoming of a growing part of the seriously decreasing water stocks to be unusable. It is important to make the remark that water contamination means a security political risk factor not only as a possible root cause of water shortage. Two or more nations have to share most of our planet's surface and under-surface water stocks. In such a case, the qualitative conservation of the water resources is out of the sovereign state competence; thus the defence and safekeeping of the connected water bases become a common interest. Water pollution, which generally affects most or the whole of the given water networks, can influence water quality and the quantity of the utilizable drinking water of not only the polluting country, but also of the adjacent countries. The pollution of water bases can cause significant international problems even in areas rich in natural resources, and where they are scarcely present; it becomes a dominant security political factor.

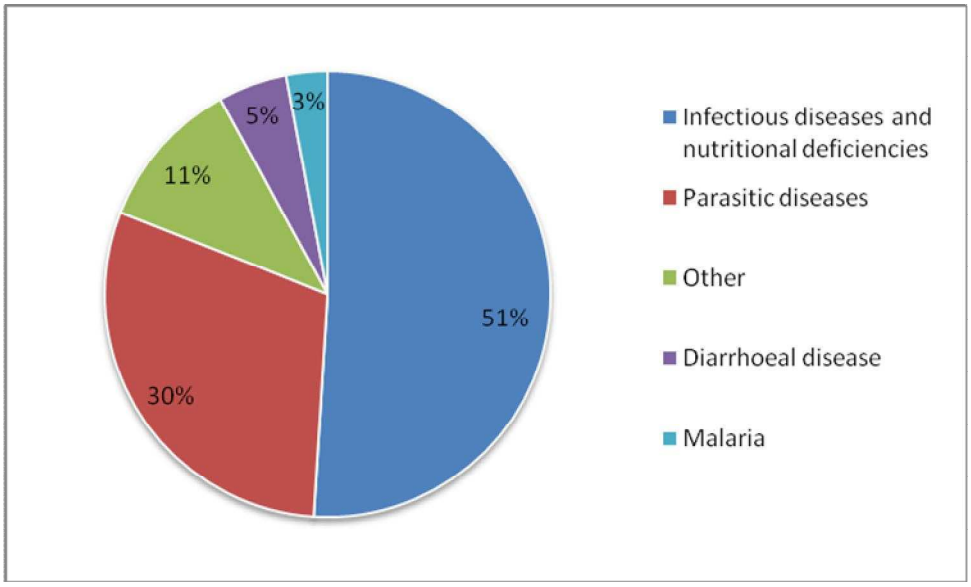


Table 1. Death rates from water-associated diseases in 2001
(Source: http://www.un.org/waterforlifedecade/pdf/waterforlifebklt-e.pdf downloaded 2010-06-20)

THE NOTION OF WATER POLLUTION AND ITS SECURITY POLICY APPROACH

There exist several conceptual definitions of water pollution. In security political approach and analysis, several elements of different definitions are worth heightening. Based on these, one of the most important determinants of water contamination is that it evolves as a result of anthropogenic functions, so they are induced directly or indirectly by humans themselves. It means such a negative change in the natural water's quality which besides increasing the concentration of dangerous materials also has a harmful effect on its consumability for humans. Water contamination can expand to each and every natural form of water appearance, i.e. still and running waters and also under-surface water stocks. Accordingly, in case of the commonly owned water bases, water pollution can be a phenomenon fraught with serious threats. Regarding the fact that it is induced by anthropogenic functions and thus human intervention can be ascertained, the responsibility of the polluting country becomes obvious. In dependence of the extent of pollution and the hydrological conditions, it can expand to most of or to the entire water basis and the deterioration of water quality may threat other natural water bases. In this sense, it may be practical to approach the classification possibilities of water pollution firstly in view of the size of the affected water bases. By reason of this, local, fluvial (affecting the given aquifer), regional and continental extensions of water pollution can be distinguished. [4] With most of the countries, local water pollution is the one that can affect the natural water's quality of the neighbouring countries in the least. At this level, the developed problem can be solved on state or even on local authorities' level, as far as possible. In cases of fluvial, regional and continental contamination, along with the growth of the expansion, the number of the affected countries may grow in direct ratio. The common water monitoring, environmental and disaster recovery agreements of the countries constrained to share the water basis have come to the front; these play an important role in the finding the earliest possible solution to the problem. In case of countries that are not on friendly terms or even hostile with each other due to other reasons the security risk of water pollution grows worse. It can emerge as

an aggravating factor if the catastrophe appears on water-scarce areas, or if the lack of adequate financial conditions ends up in operational incapacity.

Other important defining elements of water contamination are the various human activities. The anthropogenic processes that contribute directly or indirectly to the decay of freshwater quality may be derived mostly from communal, industrial and agricultural functions. Due to the effect of population boom and the urbanizational process, near half of the world's population dwell in cities today. High population clustered in disproportionately small area severely burdens the environment of the affected settlements. Due to poor drainage network and the unbuilt status of sewage farms, certain proportion of megalopolis' communal wastewater gets in the environment uncleared; and thus back to the natural water bases.
A good example to the above mentioned facts is that in Mexico City, that of population over 20 million, despite having twenty-seven different sewage works only ten per cent of all communal wastewater is cleaned. [5]

The population boom and the urbanization have also resulted in the growth of industrial and moreover in agricultural productivity. Industrial functions take the greatest responsibility in terms of decay in freshwater quality. Industrial sewage, oil and radioactive pollution and contamination resultant of the leakage form undersurface pipelines and containers considerably endanger the quality of freshwater stocks. For air pollution and the consequent acid rains, which are also fundamental elements of our planet's water circulation, industrial emission is to take the blame in the highest degree. The chemicals applied in order to increase agricultural productivity get into the natural water systems mostly by means of wash-off and erosion. The eutrophication process which intensifies due to the effects of fertilizers and other substrates endangers the lakes in the following rates: 54 percent in Asia, 53 per cent in Europe and 48 per cent in North-America. [6]

Water political approach requires to mention also the geographical classification of natural body of water. Previously the fact that water pollution affects the quality of both surface and under-surface water bases was already referred to. The two forms of appearance of the surface water stocks, i.e. the running waters and stagnant waters react to water pollution in very different ways; however, in the present case, examining how the pollution spreads is the matter of prime importance. Regarding surface freshwater stocks, certain water flows can reach most of the countries, eminently, considering that in the river systems, any of the tributaries can convey the contamination to the main river flow. In this respect, the most severe risk policy factors of water flow systems are the fast spread of the pollution and expansion of the affected area. Surface still waters and water courses are in close hydrological relationship with each other. Many countries can share one common stagnant water; however, in the spread of the pollution the feeding and downcomer rivers play the most important roles.

The pollution of under-surface water stocks can run various risks. On the one hand, under-surface water stocks, that give a significant amount of the Earth's drinking water reserve, may appear under such geographical areas which hold under-surface water stocks scarcely or do not hold at any all. On the other hand, due to their locations, such water stocks are now examined whose cleaning and neutralization from contamination is difficult or is far not soluble. Further problems arise from the fact that these water bases run under several countries' borderlines and they may be in direct contact with surface water stocks, so they can have an impact on their quality, too.

In the following sections, the possible security political factors of water pollution are presented by enumerating specific examples, principally emphasizing the importance and necessity of hydrocooperation and hydrosolidarity in the affected regions.

PROBLEMS WITH WATER POLLUTION IN THE RUSSIAN FEDERATION

Basically, the Russian Federation does not belong to those countries that suffer from water shortage. However, certain peculiar economical, sociological and political processions and changes have their effects on the water circulation and water stocks' quality of the water circulation even in the largest country on Earth. Above it is demonstrated that the high rate of urbanization entails significant burdens for the cities' environment. In 2000 the Russian Federation 110,9 million people out of the population of 147,7 million in the Russian federation were urban citizens and according to certain estimates, this number will have been increased to 122,8 million by 2020. [7] The situation is worsen by the fact that the population does not spread evenly in the country, but 80 per cent of them are concentrated in the European areas and nearby the Caspian Sea. Consequently of this, industry and agriculture are also concentrated to these areas, which is clearly shown by the fact that almost 70 per cent of the the watered areas lie on the European parts. On the urbanized and industrialized areas, there can only 8 per cent be found of the natural water flows that otherwise provide the preponderant amount of the country's water stock. In both terms of water pollution and water taking may the affected rivers be regarded as threatened ones, mainly knowing that in case of certain water flows even half of the water runoff gets exploited. [8]

Up to these days, water pollution has become one of the crucial environmental problems of the Russian Federation. Quasi fifty per cent of the surface waters does not meet the basic water quality requirements, and 30 per cent of the under-surface water stocks is intensely contaminated. Less than half of the Russian population have access to healthy drinking water so the need for a solution to this problem has been becoming more and more urgent at all levels. [10]

Since 1991, when The Soviet Union collapsed, springs and tributaries of many natural water flows of the new Russia have come to the territories of the newly independent countries and has had to share some proportion of the surface stagnant waters and the under-surface water stocks. The prevention of occasional water contaminations affecting the water bases has grown from being a home affairs problem to be a joint foreign affair interest, which raised the question of the necessity of establishing hydrocooperations. The previous cooperational contracts between the former Soviet Union and its neighbours affected in the above mentioned matter generally involved different water policy issues; so did the agreement between U.S.S.R and the government of Turkey in 1927 and the 1964 Soviet-Polish agreement. The water treaty that was signed by Hungary, Romania, Yugoslavia and the Soviet Union in Szeged in 1986 intended to prevent the quality decay and contamination of the entire Tisza River.

The first multilateral water agreement after the dissolution of the Soviet Union was established among Kazakhstan, Uzbekistan, Tajikistan and Turkmenistan in 1992, with the help of which the Middle Asian hydrocooperation was successfully founded. Besides the agreements, the water stocks divided by the new borderlines generated several debates in the affected region. The industrial fields and water power-plants set on the upper flow of the water may cause such a grade of contamination that makes field watering impossible on the lower part of the waterflow. In case of Kura River that enters the Caspian Sea, for the similar situation that has evolved among Azerbaijan, Armenia, Georgia and Turkey, the establishment of hydrosolidarity hasn't been managed yet; which fact, by lacking the development of the adequate monitoring system, may denote the aggravation of the problem. [11]

Towards the protection of interboundary natural water stocks the most significant breakthrough was the agreement in Moscow in 1998 which was established among the

Russian Federation, Belarus and Tajikistan. Under the terms of the cooperation, regarding the environment, a common provisional system was introduced and the signing countries assumed an obligation to avoid any further activity that may negatively influence the quality of the water bases that are in dispute. However, Russia has to endeavour to enter into similarly good water political relations even with those of its neighbours that were not parts of the former Soviet Union.

In my opinion, the water and environmental series of agreements made during the 1990s apropos of the transboundary Khanka Lake running alongside the Russian-Chinese borderline clearly indicate the line of bearing that the Russian Federation has to follow towards the protection of the common water bases' quality. Khanka Lake is the largest surface freshwater in North-East Asia, which is fed by fifteen and eight rivers from the Russian Federation and China, respectively. [12] In the immediate sorroundings of the lake sensitive and unique for its hydrological features and natural flora and fauna there live 620 000 people, almost 70 per cent of whom are urban citizens. The freshwater stock is utilized with various purposes, however, a crucial part, almost ninety-five per cent of it serves watering. [13] Several factors played their roles in the qualitative decay of Khanka Lake's water. In the cities built in its sorroundings besides the low degree of sewage treatment and the different washed-in and infiltrated chemicals the industrial and mining functions on the Russian side contributed to a great extent to the contamination of the stagnant water. The fast degradation that got under way both in water's quality and biodiversity caused serious problems on both sides. At first, the parties handled the critical decay in natural still water's quality in their own scopes of authority. Later they had to realize that solely within their own borders, at state level they would not be able to treat this problem.

In order to avoid the conflict, the Chinese and the Russian party agreed on establishing a common program for water defence so as to sustain Khanka Lake as a usable freshwater stock for the inhabitants. On the Russian side the industrial and agricultural operations became reduced, towards less population resettlements were carried out and 80 % less water was used for watering. [13] Parallelly with this, the Chinese tried to moderate the further pollution of stagnant water by building sewage farms and the connected drainage system, allocating reservations, and also by means of stricter legal regulation. The appropriate monitoring stations were established, among which the adequate and regular flow and exhchange of information also mean an important part of the efficient cooperation.

The Russian Federation has to give priority to the conservation of its natural water stocks' quality. The country's population figures show a decreasing tendency to which, besides low standard of living and other setbacks, and to a certain extent unfavourable environmental circumstances also contribute. The water policy agreements made among the former states have to be renewed so thus enabling them to manage their current problems, too; and with the other neighbours, efforts have to be made for setting a similarly functioning hydrocooperation.

TIBERIAS LAKE: THE NECESSITY OF HYDROSOLIDARITY IN THE NEAR EAST

In the Near East region, on the territory of Israel and its neighbouring countries, due to the the scant freshwater bases the fresh drinking water sources gain a valorized role.
In the areas of water scarcity the decay of water's quality and the spread of the dross may denote critical secure political risk. In case of Israel and its neighbours, the situation is worsen by the fact that due to serious historical conflicts, the relationship of Israel and its surrounding countries have become quite disaffected. The necessary establishment of hydrosolidarity is further complicated by the fact that previously Israel got into such military

conflicts in which the seizure of strategic water stocks played its role. I suppose in the Palestinian West Bank issue there have been certain water political controversies still present, which contribute to the block of the peace processes.

As for water pollution, it is important to heighten the water policy issues related to Israel's sole extended surface stagnant water, namely Tiberias Lake. The lake's water stock provides almost fifty per cent of the Jewish state' drinking water, so conservation of its quality is a task of high importance. [14] In view of the fact that the main source of Tiberias Lake is Jordan River, whose tributaries originate from Lebanon, Syria, and Jordan; Israel by all means has to found certain water political cooperations. After the 1949 allocation of the armistice demarcation lines Tiberias Lake got entirely to Israeli territory, so the multinational hydrocooperations should be set primarily as confined to the feeding rivers.

In the affected area hydrocooperation had been rendered more difficult by earlier water strategic oppositions. In the 1950s and 60s Syria and Israel made several efforts to divert the flow of River Jordan's tributaries, thus significantly cutting down on the amount of freshwater that empties in Tiberias Lake. Israel, which had to supply its growing population and economy, in the early 1960s, started to build its water transfer network that extends to the southern Negev Desert; whose water-taking offended the northern neighbours' interests. The oppositions that sharpened in small conflicts and in the six day war of 1967; during which the Jewish state managed to strengthen its water strategic positions in the Middle Eastern region. In view of Lake Tiberias it seems to be fundamental to emphasize that during the war Israel gained the control over the Golan Heights, so Jordan River and its main tributaries got under its authority. Seizing the water bases owned great significance not only for the sustenance of water stocks but also for the assurance and control of their quality.

One of the most important tributaries of the Jordan River that feeds Tiberias Lake is Yarmouk River which is shared by three countries: Israel, Syria and Jordan. There were agreements established on Yarmouk River between Jordan and Israel in 1953 and 1987, but these targeted mainly the importance of the building the barrage over the river, the utilization of the water for plant watering and the common water share. Conservation of water quality also got to the background, most notably, if considering that in terms of the agreements several industrial facilities and brrages were built along the river. [15] The 1994 Israel-Jordan Treaty of Peace, a separate Article of whose includes the agreements on water resources of Jordan River and Yarmouk River, involves projects regarding the quality of water. The assurance of the exchange of environmental information, the establishment of monitoring stations, the protection of common water bases and the defence of the other party's water network were discussed in the treaty of peace; which was a significant development in the region. [16] The importance of the agreement is proven by the fact that in 2009 Jordan claimed a compensation to be paid by the Jewish state, viz. considerable oil and other contamination had been noticed in Yarmouk River, which had originated demonstrably from the Israeli banks. [17]

The quality of Tiberias Lake and the related water systems is threatened by several anthropogenous processes. The agriculture, communal sewage and litter, fishing and vast tourism of the sorroundings all contribute to a significant extent to the contamination of stagnant water. The situation is worsen by Jordan River being not only feeder but also by-passer of Tiberias Lake whose water is utilized by both Jordan and Israel. Towards South the river empties into The Dead Sea, towards the protection of whose clearness and environmental assets a bilateral cooperation have already been made among Israel, Jordan and the Palestinian Authority. As for the utilization of Tiberias Lake it is momentous to note that the Israeli Water Authority indicated the lake's critical tides with red and black lines. The red line means the moderation or suspense of water-taking, and in case the tide of the lake

declines under the black line, it would draw irreversible environmental disasters as a consequence. [18]

The water networks of Tiberias Lake and Jordan River are indispensable water resources for Israel and the neighbouring Arab states. Besides the agreements affecting water-taking and water division, by all means, regarding also the protection of the quality of the water, significant improvements are necessary to be made. The technologically and institutionally more developed Israel has to strive for its enhancement of the environmental development of the surrounding countries; in which the establishment of the common-interest based cooperations play a significant role.

CONCLUSION

Besides the quantitative regulation of the global freshwater stocks, more and more emphasis should be laid on the conservation of the quality of the existing water bases. The different forms of contamination can make the resources unhealthy and unusable, which may result in new risks to evolve. Considering that most of the water bases are bliged to be shared by several countries, in most cases water pollution is a source of risk affecting a part or the whole of the given water system. In areas of water-scarcity the given problem appears revalued, since the defence and protection of the scant resources is an important risk factor, principally if other areas show different conflicts of interest. In the future an increased attention should be paid to the appointment and configuration of these countries' adequate preventional and cooperational projects, whose basis will be the common interests and hydrosolidarity.

Moreover, in the future, besides the division of water stocks, the hydrocooperations will have to be extended also to other projects related to the issue of water pollution. Beyond the establishment of common monitoring stations, the continuous exchange of information and the common damage prevention taks, the prospects for sanctions should also be drawn onto legal basis. As far as possible, the water polical cooperations should be extended to the entire water system that is affected, since the non-signing country may be able to cause a pollution in most of the water base. A good example to this is the Nile Basin Initiative that was established for the division and the protection of Nile's water stock and which can take substantive steps only through a cooperation of all of the Nile countries.

Water pollution may be a source of risk not only in the regions scarce in water. As for Hungary, the Austrian pollution of Rába River or the diplomatic conflict that evolved when Tisza River was polluted with cyan in 2000 is an instance to recall. Both instances clearly show that in a region similar to Hungary's great attention is to be paid for the protection of the common water bases, and to the opportunity to effect the evolved problem in the early phase of its spread. The bases of reducing risk are the recognition of own responsibility and the indroduction and installation of joint cooperations for prevention and averting, in pursuance of which the conservation of freshwater stocks' quality will be a global project in the future.

REFERENCES

[1] http://www.unicef.org/wash/ (2010-06-18)

[2] http://www.gdrc.org/uem/water/water-crisis.html (2010-06-18)

[3] http://www.indepthnews.net/news/news.php?key1=2010-03-22%2002:13:23&key2=1 (2010-06-18)

[4] Thyll Szilárd – Vízszennyezés – vízminőségvédelem (Egyetemi jegyzet) - http://gisserver1.date.hu/thyll/vizszenny-vizmin/tartalomjegyzek.html (2010-03-16)

[5] http://casestudies.lead.org/index.php?cscid=146 (2010-06-20)

[6] Wilhelm Rodhe – Crystallization of Eutrophication Concepts in Northern Europe – Washington, 1969. – ISBN: 309-01700-9

[7] Ward Kingkade – Intarnational Brief Population Trends: Russia – http://www.census.gov/ipc/prod/ib96-2.pdf (2010-06-20) U.S. Department of Commerce, 1997.

[8] https://docs.google.com/viewer?url=http://www.icid.org/v_russia.pdf (2010-06-27)

[9] http://www.country-data.com/cgi-bin/query/r-11390.html (2010-07-03)

[10] http://www.dni.gov/nic/special_russianoutlook.html (2010-06-27)

[11] Ministry For Natural Resources Of The Russian Federation – Transboundary Water Cooperation In The Newly Independant States – Moscow-Geneva, 2003.

[12] http://www.worldlakes.org/lakedetails.asp?lakeid=8619 (2010-07-03)

[13] Jin Xiangcan – Lake Xingkai/Khanka - http://www.ilec.or.jp/eg/lbmi/pdf/28_Lake_Xingkai_Khanka_27February2006.pdf (2010-07-03)

[14] Moshe Gophen - Water quality management in Lake Kinneret (Israel): hydrological and food web perspectives - http://www.iii.to.cnr.it/pubblicaz/JL_62_supl/11_Gophen.pdf (2010-07-03)

[15] Advocate Jitzchak P. Alster - Water in the Peace Process: Israel-Syria-Palestinians - http://www.intjewishlawyers.org/main/files/Justice%20No.10%20September1996.pdf (2010-07-04)

[16] Treaty of Peace Between The Hashemite Kingdom of Jordan And The State of Israel - http://www.kinghussein.gov.jo/peacetreaty.html (2010-07-04)

[17] http://www.greenprophet.com/2009/03/20/7695/israel-jordan-polluted-rive/ (2010-07-04)

[18] Jerusalem Post - Lake Kinneret water level dips below 'Lower Red Line' - http://www.jpost.com/Home/Article.aspx?id=106767 (2010-07-05)

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Vágföldi Zoltán
vagfoldi@hotmail.com

Földi László
foldi.laszlo@zmne.hu

KORSZERŰ TELEPÍTHETŐ LABORATÓRIUMOK ÉS ANALITIKAI MÓDSZEREK MÉRGEZŐ HARCANYAGOK ÉS VESZÉLYES IPARI ANYAGOK AZONOSÍTÁSÁRA

Absztrakt

A cikkben ismertetjük a telepíthető laboratóriumok kialakítására és működtetésére vonatkozó NATO szabványt (STANAG 4632), röviden bemutatjuk néhány NATO tagország telepíthető vegyi laboratóriumát. Ezen alapokra támaszkodva áttekintjük a magyarországi fejlesztési elképzeléseket. Elemezzük a laboratóriumi szabványos konténerbe építhető analitikai berendezések (műszerek) alkalmazhatóságát, mobilitását és meghatározzuk a szabványos analitikai azonosítási szintekhez tartozó megfelelő laboratóriumi kiépítést/műszerezettséget.

In this paper we make an overview on the NATO STANAG 4632 related to deployable laboratories and we analyse briefly existing deployable laboratories of some other NATO member states. Based on this we also overview the ongoing Hungarian research and development (R&D) projects for establishing a deployable laboratory. We investigate the suitability and mobility of different analytical equipment (instruments) can be mounted into a standard laboratory container, and determine the adequate instrumental equipment configuration needed to fulfil the standardized levels of analytical identification.

Kulcsszavak: *telepíthető laboratórium, mérgező harcanyag, kromatográfia, veszélyes ipari anyagok ~ deployable analytical laboratory, chemical warfare agents, chromatography, toxic industrial chemicals*

BEVEZETÉS

A címben megjelölt témával kapcsolatos angol szakirodalom viszonylag kevés, magyar nyelvű tudományos publikációt nem találtunk, ezért a telepíthető laboratóriumokra vonatkozó NATO STANAG és személyes tapasztalataink alapján, - főként tanulmányok, telepíthető laboratóriumokat bemutató szakmai előadásokon elhangzottak alapján - hiánypótlásként állítottuk össze a cikket.

A mérgező harcanyagok körét és fogalmát a Vegyifegyver Tilalmi Egyezmény (angolul: Chemical Weapons Convention, CWC) és a NATO AAP-21 (B verzió) is definiálja. [1] Az AAP-21 definíciója szerint *„mérgező harcanyag (chemical warfare agent): olyan mérgező anyag, melyeket katonai műveletekben használnak azzal a céllal, hogy halált, súlyos sérülést, vagy harcképtelenséget okozzon sajátos fiziológiai hatásai miatt. Nem tartoznak a mérgező harcanyagok közzé az ingerlő anyagok, ha azt rendfenntartó céllal alkalmazzák, a növényzetpusztítók (herbicidek), a ködanyagok és a gyújtóanyagok”*. A Vegyifegyver Tilalmi Egyezmény (a továbbiakban Egyezmény) az anyagokat listákba sorolja és a potenciálisan mérgező harcanyagnak alkalmas vegyületeket részletesen felsorolja. [2]

Vegyifegyverrel történt csapás („vegyi hadviselés”) vagy terrortámadás (pl. a tokiói metróban 1995-ben szarinnal végrehajtott támadás) esetén az elsődleges beavatkozás, a mentesítés, a sérültek ellátása és a további jogi lépések szempontjából alapvető fontosságú az anyagok gyors minőségi (esetlegesen mennyiségi) azonosítása. A Vegyifegyver Tilalmi Szervezet (angolul: Organization for the Prohibition of Chemical Weapons, OPCW) ellenőrei az Egyezmény felhatalmazása alapján rendszeresen ellenőrzik a részes országok létesítményeit és laboratóriumi összehasonlító körméréseket (OPCW Proficiency Test) rendeznek, melynek célja az egyes laboratóriumok felkészültségének minősítése. A követelményeknek megfelelő laboratóriumokból stabil laboratóriumi hálózatot hoztak létre a mérgező harcanyagok, prekurzoraik (a mérgező harcanyagok gyártásának kiindulási vegyületei) és bomlástermékeik egyértelmű azonosítása érdekében. Ezeket nevezzük kijelölt OPCW referencia laboratóriumoknak.

Megjegyezzük, hogy a NATO tagországok védelmi céllal fenntartott és az OPCW kijelölt stabil laboratóriumai között jelentős az átfedés, amely érthető is, hiszen a cél (illetve eszközpark, szaktudás) azonos: a mérgező harcanyagok azonosítása.

Másrészről a NATO 2002-es prágai csúcstalálkozóján döntés született a NATO Reagáló Erők felállításáról (továbbiakban: NRF), amelyben váltásban komplett vegyivédelmi képesség és többnemzetiségű erők is kijelölésre kerültek. A többnemzetű vegyivédelmi zászlóalj állományában ABV[1] felderítő és mentesítő képesség, telepíthető ABV laboratóriumok (benne SIBCRA[2] mintavevő csoport, vegyi-, biológiai-, radiológiai laboratóriumok, vegyivédelmi-tűzszerész csoport és parancsnoki csoport) és a parancsnoki döntéstámogatást biztosító Hadműveleti Értékelő Csoport (Joint Assessment Team, JAT) is megtalálható. Az NRF váltásokban nemzeti felajánlás alapján folyamatosan tevékenykednek a telepíthető VBR laboratóriumok, a Magyar Köztársaság a Mobil Biológiai Laboratóriumi Komplexum (továbbiakban MH MBLK), ABV felderítő képesség és a JAT állományának felajánlásával vesz részt. A következő fejezetekben bemutatjuk a mérgező harcanyagok azonosítására kifejlesztett telepíthető vegyi laboratóriumokat és a fejlesztés magyarországi előzményeit. Az MH MBLK-ról a későbbiekben teszünk említést.

---

[1] ABV: atom-, biológiai- és vegyi (angol szakirodalomban: CBRN)

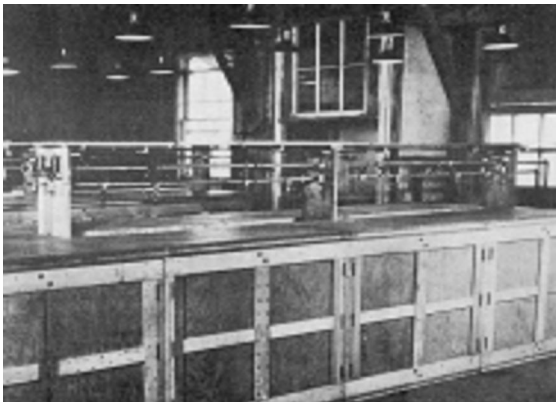
[2] SIBCRA: Sampling and Identification of Biological, Chemical and Radiological Agents (Biológiai, vegyi és radiológiai harcanyagok mintavételezése és azonosítása) – NATO ABV védelmi munkacsoport.

TELEPÍTHETŐ VEGYI LABORATÓRIUMOK

Napjainkban az elsőrendű fenyegetést a terrorizmus eszközeiként is könnyen alkalmazható vegyi fegyverek, valamint a potenciális vegyi fegyverekként számon tartott veszélyes ipari mérgező anyagok (angolul: TIC - toxic industrial chemicals) jelentik. Ebből fakadóan mind a mérgező harcanyagok, mind a veszélyes (mérgező) ipari anyagok esetében fontos, hogy olyan analitikai képességekkel rendelkezzünk, melyek birtokában a lehető legrövidebb időn belül képesek vagyunk megfelelő választ adni egy felmerült fenyegetésre. Kiemelendő, hogy ilyen esetekben az azonosítás feladata messze túlmutat a vegyifelderítő szervezetek által alkalmazott kimutató eszközök képességein, így a helyszíni mintavétel és a mielőbbi azonosítás szükségessége vitathatatlan. Emiatt rendkívül fontos, hogy vegyi szennyezettség gyanúja esetén a műveleti területhez a lehető legközelebb elérhető legyen egy megfelelő képességekkel rendelkező laboratórium. Ehhez mobil-, szállítható- és telepíthető kémiai analitikai laboratóriumokat lehet igénybe venni.

A telepíthető és mobil kémiai analitikai laboratóriumok története több mint hatvan éves múltra tekint vissza. Fejlődését elsősorban az Amerikai Egyesült Államok hadseregében rendszeresített eszközökön keresztül mutatjuk be.

Az Egyesült Államokban az első telepíthető kémiai analitikai labort, az M2-es Kémiai Laboratórium Bázist [1. ábra] a második világháború idején 1944-ben fejlesztették ki. Mintegy 10 tonna súlyú, 65 csomagolási egységből álló szállítmányként érkezett a műveleti területre, majd került összeszerelésre. A 60-as években módosított új változata az M2A1 – mely idegmérgek, és radioaktív anyagok detektálására, és biológiai harcanyagok mintavételezésére is képes volt – 1986-ig állt szolgálatban. [3] [4]



1. ábra. M2 kémiai laboratórium bázis



2. ábra. M3 mobil kémiai laboratórium

Még szintén 1944-ben került kifejlesztésre az M3-as Mobil Kémiai Laboratórium, [2. ábra] amely az M2-eshez képest csökkentett képességű volt, viszont standard tehergépjárműveken szállíthatták. [5] Az M3-ast a koreai háború alatt váltotta le az E4-es Mobil Kémiai Laboratórium [3. ábra], mely már képes volt a teljes önellátásra, a kémiai és radiológiai anyagok, majd később – a megfelelő technológia kifejlesztését követően – biológiai ágensek kimutatására is. Mobilitását 27 láb hosszú, 8 láb széles alumínium falú konténerben szállítva biztosították.



3. ábra. E4 mobil kémiai laboratórium



4. ábra. XM93 felderítő rendszer

A következő lépés a mobil kémiai laboratóriumok fejlődésében a komplex XM87-es Felderítő Rendszer volt, melynek három féle járműre – pl. M113 páncélozott gyalogsági harcjárműre – való telepíthetőségével 1987-ig kísérleteztek, azonban 1988-ban a hadsereg vezetői inkább a német FUCHS páncélozott vegyifelderítő gépjármű megvásárlása mellett döntöttek. [6]

Ezt követően 1990-ben állították szolgálatba az első XM93-asokat a Sivatagi Pajzs ideje alatt [4. ábra]. Rendkívül gyors és mobil volt, valamint a szennyezett területen keresztül haladva, menet közben is képes volt az ABV kimutató, riasztó és mintavevő felszerelései révén a hadszíntéren a vegyi szennyezés lokalizálására és megjelölésére. A négy fős személyzetet túlnyomásos fedélzeti kollektív védelmi berendezés védte. 1998-ban – az első 24 jármű kivételével – az összes XM93-ast áttervezték és felújították.

1996-ban állították rendszerbe az M93A1-et [5. ábra], melyek első éles bevetésére valójában már 1995-ben Boszniában sor került. Ez már rendelkezett M21-es mérgezőharcanyag távfelderítő készülékkel is. A különböző szenzorokról érkező jeleket a jármű riasztás esetén azonnal integrálta a fedélzeti navigációs jelekkel (GPS koordinátákkal), valamint meteorológiai paraméterekkel és továbbküldte a műveletirányító központba. [7] [8] [9] [10] [11]



5. ábra. M93A1 NBC felderítő rendszer (FUCHS/FOX)



6. ábra. JSLNBCRS

A jövő fejlesztési iránya a JSLNBCRS (Joint Service Lightweight NBC Reconnaissance System) rendszer felé mutat [6. ábra], mely a járműre szerelve, fejlett szoftvere révén, képes lesz felismerni, illetve megjelölni a vegyi és mérgező anyagokat és ABV veszély esetén valós idejű terepi felderítési adatokkal kiegészítve továbbküldeni az információkat a műveleti központ felé. Két hordozó járműhöz teszik alkalmassá – egyfelől könnyű páncélozott harcjárműre, másfelől nagy mozgékonyságú gumikerekes járműre –, melyek ugyanazt a felszerelést fogják hordozni.

A nem is oly távoli jövőre tekintve az amerikai fejlesztők további célja egy olyan ABV felderítő, megfigyelő, detektáló és azonosító rendszer létrehozása, mely tovább fogja növelni a bevetett erők harcértékét és minimalizálja az erők harcértékének csökkenését ABV környezetben. A rendszert úgy tervezik, hogy még különböző kiegészítő elemeket tudjon befogadni, mely révén képes lesz például levegő minták vegyi összetételének menet közbeni mérésére, integrált vegyi-biológiai detektálására, valamint menet közbeni mikro-meteorológiai adatok mérésére. Ezen adatok birtokában pedig képes lesz a parancsnoki vezetési rendszert teljes mértékben kiszolgálni.

A mobil laboratóriumok történetének magyar vonatkozását tekintve a VLG–66 vegyivédelmi laboratórium-gépkocsit emeljük ki, mely rendeltetése a különféle haditechnikai eszközökről, fegyverzetről és felszerelésről vett minták, valamint levegő- és talajminták mérgező anyag tartalmának és radiológiai szennyezettségének vizsgálata volt. Továbbfejlesztett változatai (VLG–71 és VLG–71 CS vegyivédelmi laboratórium gépkocsik) [7. ábra] már idegmérgek automata kimutatására is képesek voltak (Automata Vegyi Jelző, Folyamatos Vegyi Jelző és Gyorsműködésű Vegyi Jelző berendezésekkel és klasszikus analitikai vizsgálatokkal). [12]

A laboratóriumi járművek hazai fejlesztése során a Haditechnikai Intézet (HTI) az 1990-es évek elején elkészített egy Rába alvázon futó kísérleti vegyi laboratóriumi (konténeres) gépkocsit (a hozzá kapcsolt utánfutóban pedig radiológiai labort) VLG-90-es névvel, de az eszköz nem jutott túl a csapatpróba fázisán. Az említett eszközöket kivonták a rendszerből, hasonló képességű eszköz jelenleg nincs a Magyar Honvédségben. Korlátozott ABV felderítő képességeivel a vegyivédelmi zászlóaljnál szolgálatot teljesítő VSBRDM-2 vegyi-sugár felderítő járművek [8. ábra], illetve a napjainkban ezeket leváltó, BTR–80 típusú harcjármű alvázára épített vegyi-sugár felderítő jármű (VSBTR) és a MH Havária Laboratórium készenléti szolgálatának vonuló gépjárműve (málházott eszközei) jöhetnek számításba.



7. ábra. VLG–71 és VLG–71 CS vegyivédelmi laboratórium [12]



8. ábra. VS BRDM-2 vegyi- és sugárfelderítő harcjármű [12]

Telepíthető Vegyi Laboratóriummal (NATO terminológiával Deployable Analytical Laboratory, D-Al) több NATO és PfP[3] tagország rendelkezik. Eddigi ismereteink szerint abc sorrendben: Amerikai Egyesült Államok, Cseh Köztársaság, Finnország, Franciaország, Kanada, Nagy-Britannia, Németország, Olaszország, Szlovákia, Szlovénia, Svédország. Ezek közül NRF váltásba eddig csak a cseh, német és olasz laboratóriumokat ajánlották fel. A telepíthető laboratóriumok képességeinek, felszereltségének egységesítése érdekében 2005-

[3] PfP: Partnership for Peace (Partnerség a Békéért)

ben kiadták a „Telepíthető ABV Analitikai Laboratórium” szabványt, a 4632-es STANAG-et[4]. [13]

A finn hadsereg laboratóriuma megfelel a NATO AEP-49 (SIRA)[5], valamint a NATO AEP-10 (SICA) Kézikönyv[6] előírásainak, a laboratórium képes analizálni vegyi anyagokat, biológiai ágenseket, toxinokat, valamint ipari mérgező anyagokat (Toxic Industrial Compounds, TIC). A svéd haderő külön járművekre szerelten működtet radiológiai, kémiai, illetve biológiai laborokat. A kémiai analízisekhez gázkromatográffal (rövidítve: GC) kapcsolt tömegspektrométert használnak (rövidítve: GC-MS), valamint Fourier Transzformációs infravörös spektrométert (FT-IR) és Raman spektrométert. A folyadékminták – különösen a víz minták – analizálásához UV-VIS spektrofotométert használnak, és CMS analízis szettet (Chip Measurement System, Dräger, Németország) alkalmaznak a gőzök és az ipari toxikus vegyületek beazonosításához. A kanadai hadsereg mobil laboratóriuma GC-MS-el (EI/CI ionizációs módban is alkalmazható) és folyadékkromatográffal kapcsolt tömegspektrométerrel (HPLC-MS) van felszerelve, valamint infravörös spektrométert alkalmaz. A britek Bagdadban 3 db ‘Silver Standard’ ISO konténerben működő laboratórium komplexumot üzemeltettek 2003-2004-ben, mely laboratóriumokból (vegyi, biológiai- és radiológiai), irodából és raktárból állt. A laborok többek közt GC-MS-t, infravörös spektrométert (IR), Dräger csöveket, gyors teszteket és radiológiai szennyezettséget jelző képességgel is rendelkeztek.

A szlovén telepíthető laboratórium alapműszere egy Agilent gyártmányú GC-MS, míg a szlovák vegyi konténerben 2 db GC-MS (Bruker Daltonics gyártmányú EM-640 és Inficon gyártmányú HAPSITE), egy HPLC-ESI-MS[7] van elhelyezve a mintaelőkészítéshez és elemzéshez szükséges eszközökkel, vegyszerekkel és műszerekkel. [14]

Magyarországon is van elképzelés a meglévő biológiai mellett (MH MBLK) külön vegyi- és radiológiai laboratóriumi konténer kialakítására, de jelenleg forráshiány miatt ez eddig még nem került megvalósításra.

A hazai vegyi konténer tervezésnél és beépítésénél körültekintően figyelembe kell venni a már meglévő telepíthető laboratóriumokat, azok előnyeit és hátrányait. Egy ilyen telepíthető, konténeres kialakítású vegyi laboratórium beszerzése, üzemben tartása komoly szakmai (személyzet) és anyagi erőforrást igényel (éves üzemeltetése mintegy. 20-50 millió Ft-ba kerül). A telepíthető laboratóriumhoz célszerűnek látjuk stabil laboratóriumot hozzárendelni, amelyben a személyzet kiképzése, módszerek és eljárások fejlesztése, a konténer tárolása (illetve egy komplexummá történő összekapcsolása) történhetne.

Hazai példaként említenénk a MH MBLK-t, amely maga nemében világszínvonalat képvisel és létrehozása pillanatában a NATO-n belül egyedi képesség volt, ez jó példája az igényeket megelőző hazai fejlesztéseknek. Azonban, míg ez a komplexum korábban a MH Pápa Bázisrepülőtéren hangárban volt elhelyezve, később az MH Dr. Radó György Honvéd Egészségügyi Központ Tünde utcában lévő raktárbázisára költözött Budapestre, ahol szabad égen található egész évben jelenleg is. Az MH MBLK-nál további gondnak ítéljük meg azt, hogy a konténer, személyzet és műszerpark rendelkezésre áll ugyan, de a hozzá optimális infrastruktúra csak részben van kiépítve (konténernek fűtött-fedett tároló stb.). A tervezésnél és megvalósításnál a kapcsolódó infrastruktúra „kimaradt”. Ez sajnos rossz példa arra, hogy egy világszínvonalat képviselő fejlesztés hogyan válhat a rövidlátó, kizárólag költségvetési, de a szakmai szempontokat nélkülöző szemlélet „áldozatává”.

---

[4] STANAG: Standardization Agreement (Szabványosítási Megállapodás)
[5] Sampling and Identification of Radiological Agents (SIRA) Handbook -AEP-49
[6] Sampling and Identification of Chemical Agents (SICA), Handbook - AEP-10
[7] High performance liquid chromatograph-electrospray ionization-mass spectrometer

Telepíthető laboratóriumokkal szemben támasztott követelmények a STANAG 4632 előírásai alapján

Már az atom-, biológiai- és vegyivédelmi felszerelésekről (a minimális ellátás követelményei) szóló STANAG 2352 meghatározza a telepíthető kémiai analitikai laboratórium rendeltetését és fogalmát, mely szerint a laboratóriumnak képesnek kell lennie a mérgező harcanyagok kimutatására, és az anyagok azonosítására is. [15]

2005-ben kiadásra került a 4632-es STANAG, melynek célja a telepíthető laboratóriumokra vonatkozó képesség alapkövetelmények rögzítése. A fejezetben kizárólag a telepíthető vegyi laboratóriummal foglalkozunk.

A telepíthető vegyi analitikai laboratórium (angolul rövidítve: D-AL, magyar rövidítése: T-AL) rendeltetése, hogy a világ bármely pontján álljon készen mintavételi és analitikai feladatok magas szintű végrehajtására, vegyen részt a hadműveleti szintű vegyi fenyegetés felmérésében annak érdekében, hogy a műveleti parancsnokok képesek legyenek a szükséges intézkedések időbeni meghozatalára.

A szabvány alapján a laboratóriumnak az alábbi általános képességekkel kell rendelkeznie:

- Legyen alkalmazható a katonai földi-, légi- és tengeri műveletek teljes skáláján.
- Minden eleme légi úton is szállítható legyen.
- Az analitikai labor legyen alkalmazható a várható vegyi fenyegetéshez igazított feladat végrehajtására.
- 5 nap alatt érje el a készenlétet[8].
- A vegyi analitikai labor minden eleme független áramellátással (aggregátor) rendelkezzen.
- Legyen képes 72 órán keresztül utánpótlás nélkül önállóan végrehajtani feladatát, miután eljuttatták a feladat végrehajtásának helyére.

A telepíthető analitikai labor felépítését tekintve a következő elemekből kell, hogy álljon:

- Laboratórium parancsnoki elem (HQ), amely a parancsnoki (vezetési) elemmel együtt települ, műveleti kapcsolattartó rendszere a JAT (Joint Assessment Team). A parancsnoki (vezetési) elem koordinálja az T-AL egyedi műveleti (operatív) és logisztikai ellátási igényeinek biztosítását.

- Telepíthető vegyi laboratórium műszereivel azonosítja a potenciális veszélyt, továbbá hitelesen megállapítja, vagy kizárja vegyi anyagok, illetve a vizsgálandó (kijelölt) veszélyes ipari anyagok jelenlétét. Minimális követelmény, hogy a labor legyen képesek kimutatni és azonosítani a STANAG 4632 „A" és „D" mellékletében felsorolt valamennyi vegyületet. A labor hajtja végre a környezetből vett minták vizsgálatát (emberi eredetű mintákat nem kell elemezniük). A laboratóriumi elemzést és azonosítást gyors módszerekkel kell végrehajtani (4–6 órát nem meghaladó idő alatt). A feladat fontossága magasan képzett személyzetet és jó állapotban levő felszerelést követel meg. A laboratóriumi eljárásoknak és a felszerelésnek meg kell felelniük az AEP-10-ben és az AEP-49-ben foglaltaknak. Szükség esetén a labor elkülöníti és előkészíti a mintákat a nemzetek által biztosított referencia laborban történő ellenőrző (pl. OPCW referencia laboratóriumok) azonosításhoz.

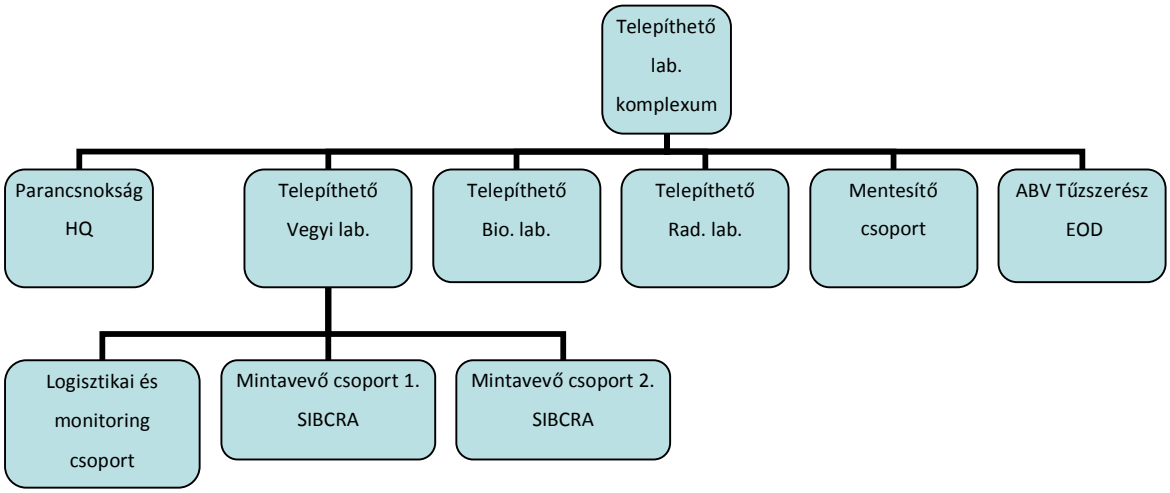
- ABV tűzszerész/robbanószerkezet és aknamentesítő csoport (CBRN EOD/IEDD), mely egy vegyi fegyverekre kiképzett (specializálódott) tűzszerész szakértő csoport.

---

8 a riasztástól 5 nap alatt legyen kész feladat végrehajtásra (kijelölt gyülekezési helyen vagy alkalmazás helyén az NRF készenléti állapotnak megfelelően).

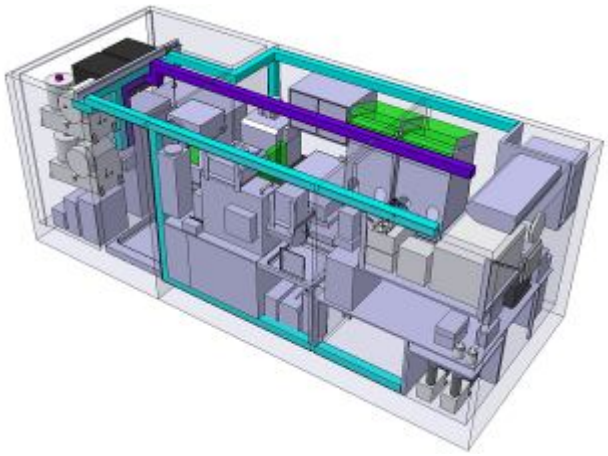
- Az ABV tűzszerész csoport tűzszerész támogatást biztosít valamennyi laboratóriumi SIBCRA mintavevő csoport[9] részére. A feladatuk, hogy megtisztítsák a robbanószerkezetektől a területet, ahol a mintavevő csoportok mintákat vesznek és segítsék a mintavevő csoportokat az aknákból és más robbanószerkezetekből történő mintavétel végrehajtásában.
- A SIBCRA mintavevő csoportoknak képeseknek kell lenniük a SIBCRA szabványnak megfelelő mintavétel végrehajtására. A mintavevő csoport(ok) fogja végrehajtani a minták biztonságos beszállítását a telepíthető laboratóriumba. A mintavevő csoportnak szigorúan be kell tartani a hiteles (törvényszéki) mintavételre vonatkozó szabványokat és eljárásokat a mintavétel, a szállítás és a minták őrzése folyamán.
- Mentesítő csoport (laboratórium részére), amely felelős a laboratórium minden részlege személyzetének, anyagainak és felszerelésének mentesítéséért.

A fentiekből látható, hogy a NATO követelmény sokkal több, mint „pusztán" egy jól felszerelt vegyi laboratórium, a megfelelő működés érdekében a labor speciális támogató képességeket is megkövetel. A SIBCRA Kézikönyv szerint a vegyi laboratórium minimális létszáma (mintavevő csoport nélkül minimum 10 fő. A szlovák telepíthető laboratóriumi komplexum (ABV-AL) felépítését a 9. ábrán, látványtervét a 10. ábrán szeretnénk példaként bemutatni (létszám 32 fő!):



9. ábra. A szlovák hadsereg telepíthető laboratóriumainak szervezeti felépítése [15]

[9] A „SIBCRA szabvány" és elfogadott azonosítási eljárás részletes leírása az AEP-10-ben és az AEP-49-ben található, melyet az AEP-66 fog felváltani



10. ábra. A Szlovák vegyi konténer látványterve [15]

A telepíthető laboratórium egyéb követelményei a következőkben kerülnek bemutatásra.

A laboratórium személyi állományának képesnek kell lennie minden alkalmazott védőeszköz használatára (beleértve az egyéni védőeszközöket, védőoltások és egyéb megelőző módszerek alkalmazását is, ahogy azt a feladat kívánja).

A személyzet és a felszerelés alkalmas kell, hogy legyen extrém időjárási körülmények között is tevékenységének ellátására (hideg, meleg, párás környezet). Ehhez légkondicionált munkahelyek kialakítása szükséges.

A környezet védelme érdekében a veszélyes hulladékok gyűjtése, kezelése során be kell tartani az érvényben levő jogi szabályozást.

Kommunikáció vonatkozásában is szigorúak a követelmények. Például a laboratórium parancsnokságának képesnek kell lenni kapcsolódni a települt és az állandó kommunikációs rendszerekhez (védett kommunikációs csatornán is). Hozzáférhetők kell, hogy legyenek a nyílt információforrások (az Internet) és az adott téma szakértői. A labor részlegein és csoportjain belüli kommunikáció nemzeti felelősség alá tartozik (így a mintavevő csoport tagjai közti kapcsolattartás).

A NATO műveletekben alkalmazott hivatalos nyelv az angol, ezért minden dokumentumot és jelentést angol nyelven kell elkészíteni (mérési eredményeket is angolul kell megadni). A nemzeteknek biztosítaniuk kell, hogy a csoporttagok megfelelő angol nyelvtudással bírjanak.

A téma szempontjából a STANAG 4632 szabványban két fő mellékletet kell megemlíteni. Az „A”mellékletében a telepíthető analitikai laboratórium alapképességébe tartozó mérgező harcanyagok és toxinok felsorolása található, míg a „D”mellékletében azok a veszélyes ipari anyagok (TIC) és a hozzájuk tartozó kimutatási eljárások, amelyeket a laboratóriumnak ki kell tudnia mutatni. [13]

A foszgént (fojtó mérgező harcanyag) és hidrogén-cianidot (általános hatású mérgező harcanyag, „vérméreg”) a veszélyes ipari anyagok (TIC) közé sorolja és a „D” mellékletében sorolja fel.

NATO rövidítés	*Típus/ megnevezés(ek)*	*Kimutatási módszer*
Hólyaghúzók		
H	HD, Kénmustár, Bisz(2-klóretil)szulfid	GC-MS
Q	Seszkvimustár, Bisz-(2-chloroethylthio)ethane,	GC-MS
T	O-mustár, Bisz-(2 klóretil-tioetil-éter)	GC-MS
N1	HN1, Nitrogénmustár, Bisz-(2-klóretil etil-amin)	GC-MS

NATO rövidítés	*Típus/ megnevezés(ek)*	*Kimutatási módszer*
Hólyaghúzók (folytatás)		
N2	HN2, nitrogénmustár, bisz(2 klóretil)-metil-amin	GC-MS
N3	HN3, nitrogénmustár, trisz(2 triklór-etil)-amin	GC-MS
L1	Lewisite I, 2-klórvinil-diklór-arzin	származékképzés, GC-MS
L2	Lewisite II, 2 klórvinil-klór-arzin	származékképzés, GC-MS
L3	Lewisite III, trisz(2-klórvinil)-arzin,	GC-MS
Idegmérgek		
DFP	diizopropil-foszforofluoridát	GC-MS
GA	Tabun	GC-MS
GB	Szarin, o-izopropil-metil-foszfonofluoridát	GC-MS
GD	Szomán, o-pinakolil-metil-foszfonofluoridát	GC-MS
GF	Cikloszarin, o-ciklohexil-metilfoszfonofluoridát	GC-MS
VX	VX, o-etil S-2-diizopropil-aminoetil-metilfoszfonotiolát	GC-MS

1. táblázat. T-VAL[10] alapképességébe tartozó MHA-ok felsorolása „A" melléklet [13]

Az AEP-66 (SIBCRA Kézikönyv) tervezet „E" mellékletében is megtalálhatóak a fenti táblázatban megnevezett vegyi anyagok, kissé más csoportosításban. A kézikönyv a vegyi anyagokat három listába sorolja (1. lista mérgező harcanyagok, 2. lista prekurzorok, 3. lista veszélyes ipari anyagok). [16]

Telepíthető vegyi laboratóriumban alkalmazható kémiai analitikai módszerek

Az olyan minták vizsgálata, amelyeknél felmerül a gyanú, hogy mérgező harcanyagot tartalmaznak, különösen, ha a harcanyag bonyolult mátrixban található, csak jól felkészült és ilyen téren komoly gyakorlattal rendelkező laboratóriumban végezhető el. A NATO AEP-10 (SICA) szerint három olyan analitikai eljárásrendszert ismerünk és alkalmazunk a laboratóriumi gyakorlatban, amelyek kielégítik a mérgező harcanyagok egyértelmű azonosításának kritériumát. Ezek a következők: [17]

- Tömegspektrometria (MS)
- Infravörös (IR) spektrometria
- Mágneses magrezonancia spektroszkópia (NMR)

A mérgező harcanyagok elválasztására, kimutatására és azonosítására jelenleg használt legalkalmasabb kapcsolt technika a GC-MS és a HPLC-MS, az NMR készülék nem mobilizálható és alkalmazható telepíthető laboratóriumban.

Az azonosításnak három szintje definiált a növekvő bizonyosság sorrendjében, amely alapvetően meghatározza a szükséges műszerezettséget.

Előzetes azonosítás (első szint, detektálás):

A mérgező harcanyag előzetesen azonosítottnak tekintendő az alábbi kritériumok valamelyikének teljesülése esetén:

- A mérgező harcanyagról két különböző kísérleti körülmények között felvett kromatográfiás retenciós adatok megegyeznek egy ismert mérgező harcanyagéval (pl. GC-FID[11],)

[10] T-VAL: telepíthető vegyi analitikai laboratórium

- A mérgező harcanyagról specifikus detektorral felvett retenciós adatok megegyeznek egy ismert mérgező harcanyagéval (pl. GC-ECD, NPD detektorral).

Bizonyított azonosítás (kettes szint, mennyiségi vagy minőségi analízis):

A mérgező harcanyag bizonyítottan azonosítottnak tekintendő az alábbi kritériumok valamelyikének teljesülése esetén:

- A harcanyagról egyedi spektroszkópiás módszerrel felvett teljes spektruma (TIC) megegyezik egy ismert mérgező harcanyag adatbázisban található referencia spektrumával. A gyakorlatban pl. GC-MS esetében ez azt jelenti, hogy ha a molekulaion nincs jelen a tömegspektrumban, akkor újabb mérést kell végrehajtani (például kémiai ionizációs technikával -CI, hogy a vegyület molekulatömegét meghatározzuk).
- A mérgező harcanyagról GC-MS-el SIM[12] üzemmódban (legalább 3 tömegű ion) felvett kromatográfiás retenciós adatok megegyeznek egy ismert mérgező harcanyagéval. A három ion arányának a referencia spektrumban található ionarányokkal 10%-on belül meg kell egyeznie. Az ionoknak a referenciával egybeeső maximumuk legyen, ugyanolyan félérték-szélességük, valamint a jel-zaj (Signal/Noise) arányuknak háromnál nagyobbnak kell lennie. Ez a feltétel csak kvadrupol tömeganalizátorú, elektron ütközéses (EI) ionizáció esetén biztosított.

Egyértelmű azonosítás (hármas szint):

A mérgező harcanyag egyértelműen azonosítottnak tekinthetjük az alábbi kritérium teljesülése esetén:

- A harcanyagról felvett kromatográfiás retenciós adatok és legalább két független spektrometriás módszerrel (MS, IR vagy NMR) felvett teljes spektrum megegyezik egy ismert mérgező harcanyag ugyanolyan körülmények között felvett, adatbázisban található referencia standardjával. Ha a molekula-ion nincs jelen a tömegspektrumban, akkor újabb mérést kell elvégezni például kémiai ionizációs technikával, hogy a vegyület molekulatömegét meghatározzuk.

Az AEP-66 szerint adott minta két kapcsolt kromatográfiás módszer egyidejű alkalmazásával kapott tömegspektrumának referencia anyaggal történő összehasonlítása is egyértelmű eredményt szolgáltat (GC-MS és HPLC-MS). [16]

A tervezett magyar telepíthető vegyi laboratórium főbb elemei

A HM Fejlesztési és Logisztikai Ügynökség Technológiai Igazgatóság telepíthető vegyi laboratórium megvalósítási tanulmányánál a cél az volt, hogy a laboratórium legalább kettes szintű azonosítást legyen képes elvégezni. Az azonosítási módszerek (MS, IR, NMR) közül a mágneses magrezonancia spektrometria nem mobilizálható, így a hármas szint elérése csak azon anyagok esetében várható, amelyek az MS és IR módszerekkel, főként pedig a hozzájuk kapcsolt elválasztási technikákkal (kromatográfia) megbízhatóan mérhetők.

A mobil rendszerekkel szemben támasztható követelmények alapján a kromatográfiás módszerek egyeduralkodók, kiemelve a GC-MS technikát. Az alapvető követelmény az analitikai eljárásokkal szemben az, hogy a települést követően rövid időn belül (max. 6 óra) meg lehessen kezdeni a tevékenységet.

---

[11] FID: lángionizációs detektor (Flame Ionization Detector)

[12] SIM: Szelektív ionkövetés (Selective Ion Monitoring)

Másfelől a konténerbe telepíthető eljárások ne igényeljenek bonyolult anyag, eszköz és időigényes mintaelőkészítési eljárásokat.

Az optimális GC-MS konfigurációt különböző típusú kolonnákkal (méret, filmvastagság, legalább 3 féle polaritás), kvadrupol tömegszelektív detektorral EI ionforrással, turbómolekuláris vákuumszivattyúval, CI opcióval célszerű választani.

Mivel a telepíthető laboratóriumban megvalósítható eljárások alapvetően a gyors adatszolgáltatás igényeit tarják szem előtt, a kalibrálásuk és a mérések reprodukálhatósága esetenként körülményesebb, ezért a specifikusságuk és érzékenységük általában nem éri el a laboratóriumban fixen telepített készülékekét. Az elválasztás és a mintaelőkészítés követelményei sem teljesíthetők maradéktalanul, így a nyomszennyezéseket tartalmazó minták detektálása sok esetben nem valósítható meg.

A telepíthető laboratórium működésének alapvetően a következőket kell biztosítania:

1. Mérgező harcanyagok és ipari veszélyes anyagok terepi mintavételezése,
2. Mintakonzerválás és szállítás a laborba, mintafogadás;
3. Laboratóriumi mintaelőkészítés;
4. Nagyműszeres analitikai mérés;
5. A mért adatok kiértékelése, interpretálása, jegyzőkönyv és jelentéskészítés;
6. A mérési eredmények továbbítása, nagytávolságú kommunikáció;
7. A feladatok végrehajtásához szükséges feltételek biztosítása az állomány részére:
   - Egyéni és kollektív védelem,
   - Mentesítő kapacitás,
   - Informatikai eszközök és kommunikáció (helyszíni és távolsági),
   - Egyéb vezetésbiztosító eszközök, laborkonténer infrastruktúra,
   - Szociális feltételek (WC, étkező, pihenő, stb.)

A vegyi laboratóriumi konténert fixen telepített 2 db C20-as konténerben tervezik megvalósítani, a rendszer telepítése daruzó gépkocsival történne. A szállítás megvalósítható közúton, vízi vagy légi úton. A telepíthető laboratóriumot konténerek és sátrakból összeállított komplexumként való építését javasolták. A szlovének megoldása szerint a konténerre szerelték a 4 db. hidraulikus emelőt, amely önmagát képes szintezni és a teherautóról leemelni, véleményünk szerint ez egy ötletes megoldás.

A veszélyes hulladékok gyűjtése elkülönítetten kell megoldani. Az elképzelések szerint a létesítmény minden eleme saját klíma és szellőzőrendszerrel rendelkezne, mindegyik szellőztetés befúváson alapulna. A konténerben helyet kapnak elszívó berendezések is. Ezeket az elszívó rendszereket egy ABV szűrön keresztül vezetnék ki, így biztosítva, hogy a veszélyes anyagok, amelyek a vizsgálati mintákból, keletkeznek, ne kerülhessenek vissza a környezetbe.

A mobil laboratórium feladatának ellátásához a következő műszerezettség képzelhető el:

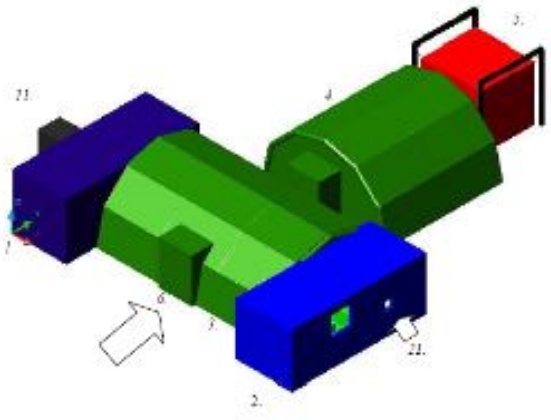
1. GC-MS hozzácsatolt FID detektorral.
2. GC-MS és NPD valamint EC detektorral.
3. GC-MS és HPLC-ESI-MS

Az LC/MS-MS-sel valamennyi kijelölt vegyület származékképzés nélkül vizsgálható, a mintaelőkészítés egyszerűbb, kevesebb lépésből áll. Hátránya, hogy a spektrumkönyvtár csak részben van meg a mérgező harcanyagokra és metabolitjaira (bomlástermékeire). A beüzemelés során ezért azt ki kell alakítani (le kell mérni).

A rendszer részletes képe a 11. ábrán látható. Kialakítását tekintve 5 fő egységből épül fel:

1. A: konténer (MHA)

2. B: konténer (TIC)
3. C: folyosó sátor
4. D: lakósátor
5. E: mentesítő sátor



11. ábra. T-VAL konténer látványterve

A konténerben alkalmazandó főbb mintaelőkészítési megoldások:
- szilárd fázisú extrakció (SPE C8, C18, PCX töltetű oszlopokkal) és szilárd fázisú mikroextrakció (SPME) különféle polaritású szállal;
- Mintakoncentrálás inert (nitrogén) gázzal, származékképzés (elsősorban szililezéssel).

A biztonság és független működés érdekében a konténerben ki kell alakítani az alábbiakat:
- izolációs és lamináris elszívó boxok/fülkék;
- mentesítő kamra a konténerben a ki-bejáratnál;
- hulladékgyűjtés;
- labor légtér monitoring (mérgező anyagokra);
- szellőzés, légkondicionálás;
- független levegős csatlakozási lehetőség (izolációs védőruha esetén).

A T-VAL tényleges megvalósításáig még számos részfeladatot meg kell oldani, a szükséges költségvetést biztosítani kell, de bízunk benne, hogy a fejlesztés a közeljövőben elkezdődhet.

ÖSSZEFOGLALÁS

A harctérre illetve kárhelyre telepíthető vagy mobil vegyi laboratóriumok tervezése és gyakorlati megvalósítása mintegy 40 éves múlttal rendelkezik. A NATO tagországainak a hidegháborút (1989-et) követő megváltozott biztonsági környezetben és fenyegetésekkel kell szembenézniük, számolni kell – elsősorban terrorista csoportok általi- mérgező harcanyag vagy veszélyes ipari anyagok alkalmazásával. A 2002-ben felállított NATO Reagáló Erők (NRF) és telepíthető laboratórium koncepciójának 2005-ös (STANAG 4632 szabványának) elfogadásával a tagországok rendszerbe állították korábbi tapasztalataikra alapozva a telepíthető laboratóriumukat.

Véleményünk szerint olyan „kis” országnak, mint Magyarország, a még meglévő szakmai és kutatás-fejlesztési alapokra támaszkodva olyan képességeket kell továbbfejlesztenie, ami

nagy hozzáadott hazai szellemi értéket képvisel és versenyképes nemzetközi viszonylatban is, mind a NATO, mind az EU keretein belül. Ilyen magas fokú szakmai tudást igényel például az egészségügy illetve a vegyivédelem.

A cikkben bemutattuk a telepíthető laboratóriumokra vonatkozó 4632-es NATO szabványt és a megvalósításra tervezett magyar tanulmányt, ismertettük a beépítésre tervezett műszereket a kettes szintű azonosítási követelménynek megfelelően. A magyar fejlesztésű vegyi konténer tervezésénél és felszerelésénél véleményünk szerint körültekintően figyelembe kell venni a már meglévő telepíthető laboratóriumok kialakítását, máskülönben a tényleges beépítésnél sok buktatóval kell majd számolni. A piacon sok gyártótól széles választékban kapható analitikai műszerek többségében alkalmasak a telepíthető laboratóriumokba való beépítésre, célszerű magyarországi szerviz háttérrel és referenciával rendelkező készülék típus kiválasztása.

A tervekben szereplő telepíthető vegyi konténer (konténerek) beszerzése, üzemben tartása (műszerek karbantartása, fogyóeszközök beszerzése) komoly szakmai (felkészült személyzet) és anyagi erőforrást igényel, melyet a jelenlegi költségvetési helyzetben is célszerű finanszírozni. A telepíthető vegyi laboratórium olyan, akár NRF-be is felajánlható képességet teremt, amely költséghatékonyság szempontjából az egyik ígéretes fejlesztés lehet hazánkban. A fejlesztés és a későbbi alkalmazás, illetve közös gyakorlatok során a szomszédos országokkal két vagy többoldalú nemzetközi katonai együttműködés keretében biztosítani lehet a külföldi tapasztalatok építő jellegű felhasználását és beépítését a laboratórium eljárásrendjébe.

FELHASZNÁLT IRODALOM

[1] AAP-21 (B): ABV védelmi terminológia és definíciók (STANAG 2367 NBC, NATO Glossary of NBC Terms and Definitions), a HM Hadműveleti és Kiképzési Főosztály kiadványa , (2009), p. 32.

[2] Vegyifegyver Tilalmi Egyezmény, A Vegyifegyverek kifejlesztésének, gyártásának, felhalmozásának és használatának tilalmáról, valamint megsemmisítéséről szóló, Párizsban, 1993. január 13-án aláírt egyezmény, 1997. évi CIV. törvény által kihirdetve

[3] Information Paper, CWTC Item 945, 17 Mar 1944

[4] Information Paper, AMCTC Item 3400, 22 Apr 1965

[5] Information Paper, CWTC Item 1120, 31 Aug 1944

[6] Michael J. J. Eddy, New Developments in Chemical-Biological Materiel, CRDEC-SP-86013, April 1986, 36; CRDEC, Annual Historical Review, FY88, 60-61.;

[7] U.S. Army Chemical and Biological Defense Command. AMC Accomplishments During General Ross' Period of Command. undated; “NBCRS Headed for Production,” The Catalyst 1, no. 2 (1995);

[8] Michael H. J. Eddy, New Developments in Chemical-Biological Materiel, CRDEC-SP-88014, 34; Information Sheet, M93A1 Fox NBC Reconnaissance System, 10 Nov 1998

[9] Information Paper, The Fox NBC Reconnaissance Vehicle, 29 Jul 1997

[10] Information Paper, M93A1E2 Block Modification Fox Nuclear, Biological, Chemical Reconnaissance System (NBCRS), January 1999

[11] Information Paper, The Fox NBC Reconnaissance Vehicle, 29 Jul 97; "The Fox Goes to Bosnia," Edgewood Quarterly, No. 8, June 1996

[12] Erdős József, Pintér István, Solymosi József: Magyar ABV védelmi technikai almanach, ZMNE, 2003., 142-147.o.

[13] STANAG 4632: Deployable NBC analitical laboratory (Telepíthető ABV Analitikai Laboratórium, NATO Standardization Agency (NSA), (2005)

[14] Ľuboš TRUDIČ szds., Milan BOŽOK hdgy.: MOBILE IDENTIFICATION CHEMICAL LABORATORY, Internatonal CBRN Worksop in the Slovak Republic előadás (2009.05.19)

[15] STANAG 2352 Nuclear, biological and chemical (NBC) defence equipment – operational guidelines (Atom-, biológiai- és vegyivédelmi felszerelések -a minimális ellátás követelményei), NATO Standardization Agency (NSA), (2006)

[16] Sampling and Identification of Chemical, Biological and Radiological Agents (SIBCRA), Handbook - AEP-66 (2009, ratification draft) E melléklet, 245-247. o.

[17] STANAG 4359 (LG/7) Sampling and Identification of Chemical Agents (SICA), Handbook – (AEP-10)

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Ágoston Tibor
agostontibor86@gmail.com

MŰHOLD ELLENI FEGYVEREK

Absztrakt

Ahogy egyre inkább beépítjük mindennapjainkba a műholdas rendszerek használatát, katonai szempontból fontossá válik az ellenséges műholdas rendszerek megbénítása, rombolása. Így jelentek meg a műhold elleni fegyverek (Anti-satellite weapons – ASAT). Céljuk az ellenséges műholdak tevékenységének megakadályozása, vagy elpusztítása. Manapság csak az Egyesült Államokról és Kínai Népköztársaságról ismeretes, hogy rendelkezik ilyen képességekkel, vagy folytat fejlesztéseket. Természetesen régebben, az 1960-as évektől kezdve, a szovjeteknek is megvoltak az ilyen irányú kísérleteik. A hidegháború vége, a rendszerváltás, a kétpólusú világrend megszűnése miatt egy időre a háttérbe szorultak. Napjainkra egyes nagyhatalmak már rendelkeznek ASAT képességekkel és a rohamosan fejlődő országok is egyre inkább kacsingatnak ezen képességek rendszeresítése felé.

As we incorporate satellite systems into our daily lives, it becomes more and more important to be able to jam or destroy hostile satellite system, from the perspective of the military. That is reason for developing anti-satellite weapons (ASAT). Their main purpose is to prohibit our adversaries' satellites from operating. Nowadays only the U.S. and China are known of possessing such capabilities or pursuing researches. Of course in the past, from the '60s, soviets' also had similar researches. Due to the end of the Cold War, the change of the regime, end of the bipolar world order threw them into the shade. By today, specific great powers possess ASAT capabilities and some quickly developing countries wish to put these capabilities into their inventory as well.

Kulcsszavak: *ASAT, légi indítású, űrtelepítésű, ballisztikus rakéta, hidegháború ~ ASAT, airborne missile, space-based, ballistic rocket, cold war*

A világűr kutatásakor használatos rakéták, melyek felhasználhatóak lehetnek magaslégkör-kutatás, hordozórakéták, vagy űreszközök mozgatására szolgáló fedélzeti rakétákként. Egy másik szféra, mely ilyen rakétákat használ, a hadsereg, ámbár más követelményeket állít ezen eszközök elé. Az űrtevékenységi célokra alkalmas rakéták nem jók katonai célokra és fordítva. Kezdetben, mikor még csak tanultuk a rakéták építését, a rakétákat mindkét célra egyaránt alkalmazták. Hamarosan azonban a két terület teljesen szétvált. A katonai követelmények alapvető része az azonalli bevethetőség, indíthatóság. Az általános, kutatási célú alkalmazásnál ez nem követelmény. Fontos a hadi alkalmazásoknál, hogy valamely célt minél gyorsabban érjen el a rakéta. Az űrbéli alkalmazásnál a szempont inkább az adott pálya végigrepülése, igaz kötött idő alatt, de nagy hangsúlyt helyezve a szállított, nagy érzékenységű eszközök és emberek biztonságára. A nagy gyorsulástól mind az eszközök, mind a személyzet sérülhet. Katonai feladatoknál a robbanófej sokkal inkább elviseli a gyorsulásból adodó nehézségi terhelést. Így ma már mind normál katonai alkalmazásoknál, mind a légvédelmi és rakétaelhárítási feladatoknál speciálisan erre a célra kifejlesztett rakétákat használnak. Katonai alkalmazások közé tartozik még a különböző tartományú (látható fény, infra) felderítő-, katonai hírközlő-, nukleáris tevékenységet ellenőrző-, elektronikai eszközöket bemérő-, ballisztikus rakétavédelmi rendszer részét képező műholdak pályára állítása.

Mint minden katonai technológiát, ezt is követte az azt megzavarni, elpusztítani képes technológiák igénye. Így jelentek meg a műhold elleni fegyverek (Anti-satellite weapons – ASAT). Céljuk az ellenséges műholdak tevékenységének megakadályozása, vagy elpusztítása. Manapság csak az Egyesült Államokról és a Kínai Népköztársaságról ismeretes, hogy rendelkezik ilyen képességekkel, vagy folytat fejlesztéseket. Természetesen régebben, az 1960-as évektől kezdve, a szovjeteknek is megvoltak az ilyen irányú kísérleteik. Ők interkontinentális ballisztikus rakétákkal képzelték a leghatékonyabb kivitelezést. Fő célpontok a kommunikációs, helymeghatározó, időjárás kutató és képi felderítő műholdak lettek volna. A hidegháború korszakában ezeket a fegyvereket nukleáris robbanófejjel tervezték, de ahogy közeledtünk a rendszerváltáshoz, egyre inkább kezdtek áttérni a hagyományos robbanófejek alkalmazására. Mivel a hidegháború korszakában élték fejlesztésük fénykorát ezen fegyverek, nagyon valószínű volt, hogy egy esetleges ASAT fegyver alkalmazása, masszív nukleáris választámadást eredményezett volna. Legalábbis a korai elemzők ezen a véleményen voltak. [1]

A korai kísérletek közé tartozik a Bold Orion projekt. Ennek keretében egy B-47-esről kilőtt, légi indítású ballisztikus rakétákkal kísérleteztek. 12 kísérleti indítást hajtottak végre a program keretében. Az utolsó kísérlet az Explorer 6 nevű műhold elleni támadás-szimulálás volt. A rakéta 6,4 km-re megközelítette a 251 km magasan keringő műholdat. Történt mindez 1958-1959-ben.

Ezzel egy időben zajlott a High Virgo program. Ugyanúgy légi indítású ballisztikus rakétát használtak egy B-58-asról indítva. Indítás után minden kommunikáció és kamera kép megszakadt a rakétával, bizonytalanná téve annak sikerességét.

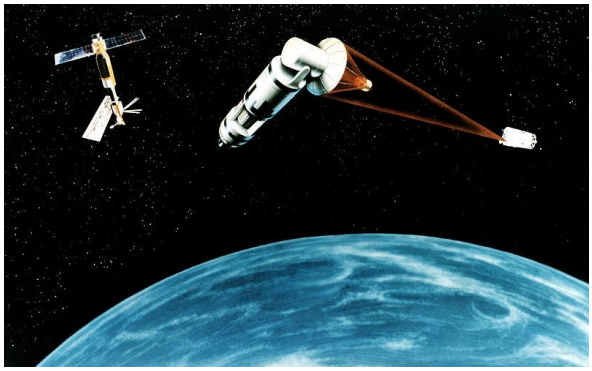
Egy másik kísérlet az Önvezérlésű Rakéta Kísérlet (Homing Overlay Experiment – HOE) volt 1984-ben. Infravörös szenzorok, irányító elektronika és megfelelő meghajtó rendszerek segítették a kinetikus romboló eszköz (Kinetic Kill Vehicle – KKV) célravezetést és pályán tartást. Űrbe érés után kinyitotta a 36 darab, 4 méter hosszú aluminium „karját”, mely egy esernyő vázához hasonlított, ezzel is növelve az ütközés valószínűségét.



1. ábra. Homing Overlay Experiment – HOE

A sikeres kísérleteket követően felmerült itt is a nukleáris robbanófejek használata, különösképpen az azt követő elektromágneses impulzusok (EMP) miatt. Az 1958-as Hardtack Teak és az 1962-es Starfish Prime nagymagasságú nukleáris tesztek során elektromos berendezések robbantak fel különböző műholdakon, energiaellátási zavarokat is okozva, valamint megzavartak minden kommunikációs műholdat a Csendes-óceán térségében. [2][3][4]

A fejlesztések egy másik területe az irányított energia fegyverek voltak, beleértve a nukleáris robbantással táplált röntgen lézer, mely része volt Reagen elnök Star Wars (eredeti nevén Strategic Defense Initiative - SDI) néven is ismert programjának.



2. ábra. Röntgen lézer – X-ray laser

Nemcsak űr-telepítésű lézerek ötleteivel álltak elő, hanem földi telepítésűekével is. Ezek nagy hátránya, hogy a lézer sugárnak át kellene hatolnia az atmoszférán, mely következtében a nyaláb jelentős csillapítást szenvedne. Összességében kétséges, hogy ekkora távolságban hatékony lenne-e. Napjainkban is inkább ballizstikus rakéták, sorozatvető rakéták és tüzérségi gránátok elleni alkalmazásukkal kísérleteznek, ld. Airborne Laser vagy Skyguard programok.

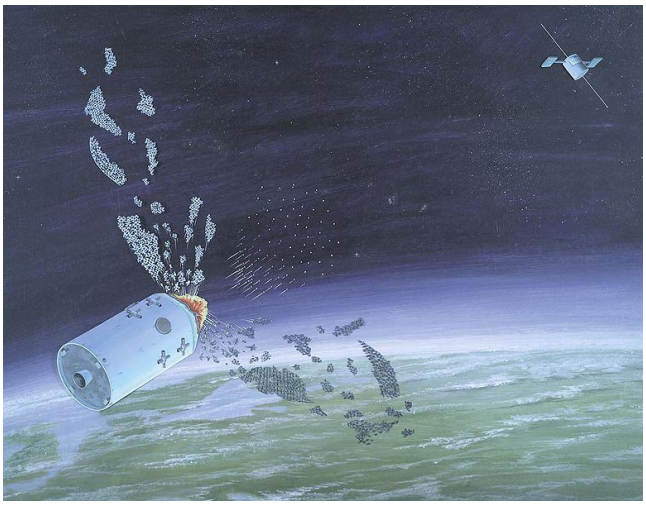
Az első sikeres kontakt találattal végződött amerikai kísérlet 1985. szeptember 13-én történt, mikor is lelőtték a P78-1 műholdat egy F-15-ös vadászgépről indított ASM-135 típusú ASAT rakétával. [5]



3. ábra. Az ASM-135 ASAT indítása, 1985. szeptember 13.

A rakétát egy földi radar irányította a bejövő cél környékére, azután a robbanófej már saját magát vezette a célpont pályájára. Ez a megoldás sokkal kifinomultabb, mint a szovjet rendszerek voltak. A támadási fázis nem tart tovább, mint 10-20 perc, tehát a célba vett műholdnak csak nagyon kevés ideje van manőverezésre, kitérésre. Hátránya, hogy csak alacsony pályán keringő műholdak támadására alkalmas. A déli félgömbön nemigen lett volna hatékony, ahol a Molnyija pályán keringő szovjet kommunikációs műholdak a legközelebb érnek a Földhöz. Ennek oka, hogy az F-15-ös vadászgépet nem repülőgép hordozón való szolgálatra tervezték és földi kiszolgálás abban a térségben nem volt elérhető. [6]

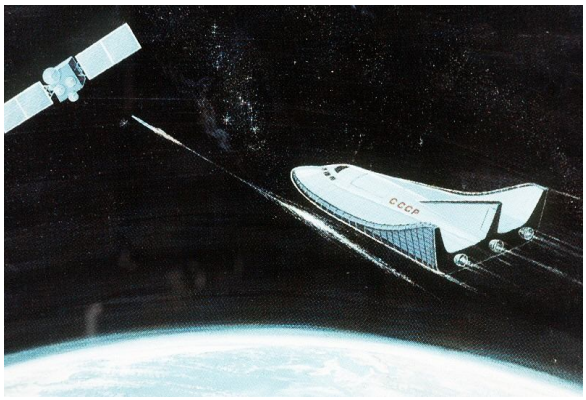
Mint minden amerikai fegyvernek, technológiának, ennek is megvolt az orosz/szovjet megfelelője. A szovjet műhold elleni fegyverek eredete bizonytalan. 1960-ban Hruscsov zöld utat adott az űrbe telepített védelmi rendszerek fejlesztésének, melynek első eredménye az UR-200-as hordozórakéta. 1961-ben indult el az Istrebitel Sputnik (Műholdak Rombolója) program. A rendszer lényege az volt, hogy a robbanófejet jóval a célműhold odaérkezése előtt pályára állítsák és miután kellő távolságba ér, repeszeket robbantsanak rá. Úgy kell elképzelni, mint egy orbitális sörétes puska. Körülbelül 90-200 percet vett volna igénybe az eljárás az indítástól az elfogásig. Fedélzeti radar irányította volna az elfogót. Később leállították az UR-200-as programot, késztetve ezzel a tervezőket a hordozó rakéta leváltására. 1973 februárjában nyilvánították hivatalosan is működőképesnek a rendszert.



4. ábra. A szovjet Istrebitel Sputnik Műhold Elleni Fegyver

Amerikai megfelelője a Brilliant Pebbles rendszer, melyben nagyszámú apró elfogó-rakéta keringett volna az űrben, melyek aktiválás után sokadmagukat rávezettékk volna a célra (apró irányitott „sörétek").

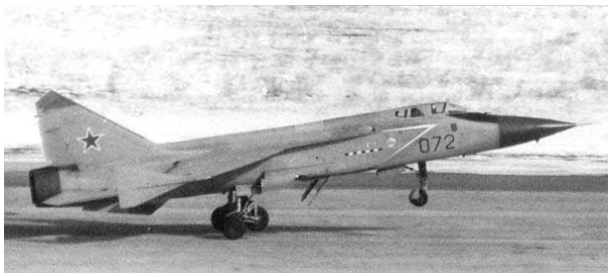
Voltak egyéb irányú, akkor még sci-fi-be illő elképzelések is, melyek egyike a következő képen látható:



5. ábra. A korai szovjet ASAT tervek egyike

Az 1970-es évektől a szovjetek is kísérleteztek földi telepítésű lézer fegyverekkel a Terra-3 nevű kísérleti központban. Az itt folytatott kísérletek a vörös rubint és szén-dioxid lézerekkel nem bizonyultak hatásosnak műholdak ellen, ámbár átmenetileg képesek voltak megvakítani a műholdak optikai szenzorait. Mintegy erőfitogtatás, a Terra-3-as lézert a Challenger űrsikló célkövetésére is használták, meghibásodásokat okozva ezzel a fedélzeti rendszerekben, megvakítva az űrsiklót. [7]

1987-ben megépült az F-15-ösről indítható ASAT rakéta szovjet megfelelője. A repülőgép a MiG-31D típusszámot kapta. Szolgálati magassága 17000 méter, szolgálati sebessége 3000 km/h volt. [8]



6. ábra. MiG-31D

Az 1990-es évek elején törölték a MiG-31D változatot. A két megépült prototípus törzse alatt egyetlen rakétát hordozott volna, amely ellenséges műholdak megsemmisítésére szolgált. Az amerikai ASAT programra adott orosz válasz befejezetlen maradt.

Napjainkban a Kínai Népköztársaság is rendelkezik ASAT képességekkel. 2007. január 11-én sikeresen lelőtték az egyik meteorológiai műholdjukat, a FY-1C-t. Erre a célra az amerikai ERIS rendszeren alapuló SC-19-es kinetikus romboló eszközt használták. [9] Habár Kína nem rendelkezik olyan fejlett űrképességekkel, mint az Egyesült Államok, hihetetlen mértékű fejlődést mutatnak. Állításuk szerint programjuk békés szándékú, de „csak erővel lehet a békét megőrizni", mondta Xu Quiliang vezérezredes. [10] 2010-ben újabb tesztekre került sor, melyben félő, hogy Kína az ASAT képességeit szerette volna kibővíteni. Pontosan 3 évvel az első kísérletük után, 2010. január 11-én lőtték fel a HQ-19-es, föld-levegő rakétájukat, fedélzetén egy kinetikus romboló eszközzel. [11]

2006-ban az USA fellőtte az USA-193 kódjelű kémműholdját, azonban a műhold meghibásodott. 2008. február 14-én lőtték le egy anti-ballisztikus rakétával, mert a fedélzetén lévő mérgező üzemanyag veszélyt jelentett volna az emberekre az esetleges lezuhanása után. Jelentések szerint az indítás után robbanás látszódott az égbolton. [12] Tudosók vitatják, hogy az üzemanyag tartály elégett volna-e az atmoszférában, illetve, hogy az ekkora mennyiségű mérgező üzemanyag mekkora hatást gyakorolt volna az emberi szervezetre. Egyes elemzők szerint a hivatalos állítás nem takarja a teljes igazságot, hanem a kínai ASAT kísérletekre volt ez inkább egy válaszlépés.

2010-ben India is bejelentette, hogy szándékában áll lézer és ballisztikus rakéta alapú műhold elleni fegyvereket kifejleszteni. V.K. Saraswat, a Védelmi Kutatási és Fejlesztési Szervezet igazgatója elmondta, hogy India rendelkezik a szükséges létesítményekkel, habár a kinetikus rombló eszközt még ki kell fejlesztenie. [13] A hordozó eszköz elvi alapjai már léteznek az AGNI ballisztikus rakétákban. A fejlesztések részét képezhetik az indiai ballisztikus rakétavédelmi programnak, mely kísérleti fázisa 2014-ben fejeződik be a tervek szerint. Az első kísérleti indításra 2010 novemberében került sor. [14]

Oroszországban is jelentős fejlesztéseket kívánnak véghezvinni. 2020-ra a fegyveres erők egy új fegyvernemét kívánják létrehozni, mely a magját alkothatja a lég- és űrvédelmi alakulatoknak. 2020-ra állandó készültségi szintet kívánnak elérni, az alakulatok teljes feltöltöttsége, jobb kiképzettsége, valamint új generációs fegyverek kifejlesztése és rendszeresítése mellett. Az új lég-űr védelmi elgondolás szerint a meglévő légvédelmi rendszereket lecserélnék S-400 és S-500 típusú légvédelmi rendszerekre. Az S-400 hatótávolsága kürölbelül a kétszerese az amerikai Patriot rakétáknak. [15] Alexander Zelin tábornok állítása

szerint képes lopakodó repülőgépek, cirkáló rakéták és ballisztikus rakéták elfogására. Az 5. generációs S-500-as még a tervező asztalon van, tervek szerint 2012-re lesz kész és jóval felülmúlja majd az S-400 és a Patrior-3 rendszereket. Mindezek mellett megint elővették a MiG-31 Foxhound fejlesztését, melyet a lég- és űrvédelmi hálózat egyik alap elemévé terveznek tenni. [16]

ÖSSZEGZÉS

Láthatjuk, hogy a műhold elleni fegyverek, illetve azok tervei a hidegháborúban élték fénykorukat és abban az időben rohamosan fejlődtek. A hidegháború vége, a rendszerváltás, a kétpólusú világrend megszűnése miatt egy időre a háttérbe szorultak. Azonban ahogy egyre inkább beépítjük mindennapjainkba a műholdas rendszerek használatát, katonai szempontból fontossá válik az ellenséges műholdas rendszerek megbénítása, rombolása. Egyes nagyhatalmak már rendelkeznek ASAT képességekkel és a rohamosan fejlődő országok is egyre inkább kacsingatnak ezen képességek rendszeresítése felé. A hidegháborúban alkalmazásuk nem volt elképzelhető a támadás első lépcsőjében, hiszen egy nukleáris válaszreakció lett volna a legvalószínűbb megtorlás. Egy műhold lelövése nem ért volna ennyit. Mára egyre inkább elterjedtek a műholdakat használó adattovábbító, kommunikációs, saját csapat követő, felderítő stb rendszerek. Műholdak kiütése, rombolása meggátolhatja az ellenséget mind a saját, mind az ellenséges erők hollétének ismeretétől, a velük való kommunikáció (utasításadás, jelentések fogadása) képességétől. Ez egy adott harci érintkezésben döntő előny lehet, nem beszélve a hosszú távú, hatásalapú megközelítésről. Egy megsemmisített, vagy fizikailag megrongált műholdat csak hosszú idő elteltével, hatalmas anyagi ráfordításokat követve tudnak csak pótolni, helyrehozni. Konfliktusban, illetve háborúban ez anyagi nehézségekhez és hadiipari leterheltségekhez vezethet.

Felhasznált irodalom

[1] Nigel Flynn - War in Space, Winward Kiadó, ISBN 0 7112 0444 6, 1986., 20. Old

[2] Museum of Learning, Hardtack Teak, (2010. december 6.)
http://www.museumstuff.com/learn/topics/Hardtack_Teak

[3] WiseGEEK, What is Starfish Prime?, (2010. december 6.)
http://www.wisegeek.com/what-is-starfish-prime.htm

[4] Nigel Flynn - War in Space, Winward kiadó, ISBN 0 7112 0444 6, 1986. 25. old

[5] Astronautix.com, ASAT, (2010. december 6.)
http://www.astronautix.com/lvs/asat.htm

[6] Anti-Satellite Weapons and U.S. Military Space Policy, Lanham : University Press of America, ISBN 0819154768, 1986, 12. old.

[7] Astronautix.com, Terra-3, (2010. december 6.)
http://www.astronautix.com/craft/terra3.htm

[8] GlobalSecurity.org, USSR/CIS Miniature ASAT, (2010. december 6.)
http://www.globalsecurity.org/space/world/russia/mini.htm

[9] GlobalSecurity.org, ERIS Exoatmospheric Reentry-vehicle Interceptor System, (2010. december 6.)
http://www.globalsecurity.org/space/systems/eris.htm

[10] CNN, Adam Levine – In today's space race, watch our for China, (2010. december 6.)
http://edition.cnn.com/2009/TECH/space/11/18/china.space/index.html?iref=allsearch

[11] DefenceNews, Wendell Minnick – China missile test has omnious implications, (2010. december 6.)
http://www.defensenews.com/story.php?i=4460204

[12] Zarya, Satellite Tracking - USA-193 Interceptor, (2010. december 6.)
http://www.zarya.info/Tracking/USA193/USA193.php

[13] Space News, Peter B. de Selding – India developing means to destroy satellites, (2010. december 6.)
http://www.spacenews.com/military/india-developing-anti-satellite-technology.html

[14] Nuclear Threat Initiative, India test-launches nuke-capable missile, 2010. november 29., (2010. december 6.)
http://gsn.nti.org/gsn/nw_20101129_6016.php

[15] Warfare.ru, SA-21 GROWLER / S400 Triumph Long Range TABM/SAM, (2010. december 6.)
http://warfare.ru/?linkid=1699&catid=264

[16] RIA Novosti, Anton Denisov – Russia to revamp air-space defenses by 2020 – Air Force chief, 2009. november 8., (2010. december 6.)
http://en.rian.ru/mlitary_news/20090811/155782307.html

Képek jegyzéke

1. ábra. Homing Overlay Experiment – HOE, http://einestages.spiegel.de/hund-images/2008/03/18/21/a3a2792d9f08354ee9b068ed2213e1fd_image_document_large_featured_borderless.jpg, (2010. december 6.)
2. ábra. Röntgen lézer – X-ray laser, http://www.martinfrost.ws/htmlfiles/aug2006/sdiolaser2.jpg, (2010. december 6.)
3. ábra. Az ASM-135 ASAT indítása, 1985. szeptember 13., http://upload.wikimedia.org/wikipedia/commons/thumb/2/24/ASAT_missile_launch.jpg/250px-ASAT_missile_launch.jpg, (2010. december 6.)

4. ábra. A szovjet Istrebitel Sputnik Műhold Elleni Fegyver, http://upload.wikimedia.org/wikipedia/commons/thumb/7/77/IS_anti_satellite_weapon.jpg/773px-IS_anti_satellite_weapon.jpg, (2010. december 6.)
5. ábra. A korai szovjet ASAT tervek egyike, http://www.stardestroyer.net/Armour/ShepDoDPix/Spaceplane.JPEG, (2010. december 6.)
6. ábra. MiG-31D, http://www.airwar.ru/image/idop/other/mig31d/mig31d-2.jpg, (2010. december 6.)

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Gábri Máté
gabri.mate@modernbiztonsag.org

BIZTONSÁGI KOMPLEXUMOK AZ INFORMÁCIÓS KORBAN

Absztrakt

Jelen cikkemben a biztonságelméletek rövid történeti fejlődésének bemutatására alapozva szeretnék rávilágítani bizonyos hiányosságokra, változásokra, melyek szükségessé teszik a további kutatásokat. Az informatika érezteti hatását az élet minden területén, ezért elengedhetetlen, hogy a biztonság, mint elmélet oldaláról is megvizsgáljuk a következményeket.

In my article through a brief historical presentation I would like to explore the shortcomings of the most widely accepted security theories which ask for more research in this topic. Computing affects every aspect of our life so it is vital to research its effects regarding security as a theory.

Kulcsszavak: *biztonságelmélet, információs társadalom, információ biztonság ~ security theories, information society, information security*

Bevezetés

A tanulmány célja a buzani többdimenziós biztonsági modellen keresztül felvázolni egy aktualizált, napjaink viszonyaihoz igazított biztonsági modell elméletét. Terjedelmi okok miatt az elmélet rövid bemutatását, illetve indoklását kívánom megtenni. A mélyreható, részletesebb elemzés további publikációk tárgyát képezi majd. A második világháború végéig a biztonságfelfogás egyértelműen katonai síkon alapult, ennek következtében két vonulat alakult ki. Az egyik azt vallotta, hogy a nagyobb katonai erő nagyobb biztonságot jelent, ezzel szemben a másik a földrajzi tér nagyságához kötötte a biztonságot, vagyis hogy a nagyobb terület magasabb biztonsági szintet eredményez.

Az emberiség történelme, de legfőképpen az első és második világháború megmutatta ezen elméletek hibáit. Igaz, a hidegháború első éveiben, a két nagyhatalom fegyverkezési versenyének korai szakaszában még alkalmazták mindkét teóriát egészen addig, amíg az előbbi gazdasági eszközzé nem vált az Amerikai Egyesült Államok kezében. A történelmi tapasztalatok, a második világháború utáni európai államok belső helyzete, valamint ezen államok társadalmi és a gazdasági állapota jelentős mértékben hozzájárultak a biztonságfelfogás átalakulásához.

A nyugati államok, élükön az USA-val, egyre inkább felismerték, hogy egy állam biztonságát nem lehet pusztán katonai erejéhez, vagy területének nagyságához kötni. Az Egyesült Államok hiába garantálta Nyugat-Európa katonai biztonságát haderejének jelenlétével, mert az államok jelentős része gazdasági, politikai és társadalmi válságoktól szenvedett a háborús veszteségek miatt. A Szovjetunió lépést tartott a fegyverkezési verseny tekintetében az USA-val, azonban a gazdasága, és közvetve a társadalma nem bírta elviselni ezeket a terheket, amely szintén hozzájárult a felbomlásához. A biztonságelméletek kutatói között a '90-es évek elejére két csoport alakult ki.

Az egyik csoport a tradicionális elméleteket képviselte, míg a másik a széles látókörűek, avagy a „nyitók" csoportja volt. A tradicionalisták, vagy klasszikusok, nevükből is adódóan az eddig jól bevált, már megszokott módszert követték. Szerintük a biztonságot katonai oldalról kell megközelíteni, ahol a fegyveres erők jelentik az eszközt, az aktív szereplő pedig az állam. A másik elméleti vonulat megtartotta a katonai szempontokat, azonban beemeltek más tényezőket is a vizsgálati körbe.

Ezen a ponton az elmélet képviselői között nincs egyértelmű összhang. Egyesek tartanak a biztonság túlzott „nyitásától", mert szerintük ezzel értelmét veszti a kifejezés és a hozzá kapcsolódó folyamatok ellehetetlenülnek, míg mások a biztonságot minden kapcsolat alapjaként látják, közjóként tekintenek rá és univerzális jelentéssel ruházzák fel. Waever szerint ez egy veszélyesen szűk látókör. Szerinte a biztonságnak konfliktusok, fenyegetések stabilizált állapotát kell jelentenie, vagyis a biztonság hiánya az az állapot, amikor a fenyegetésekkel szemben nincs hatásos eszköz.

A liberális gondolkodók is ellenzik a biztonság univerzális jellegét. Gazdasági szempontokkal érvelnek, miszerint a túlbiztosított, stabil piaci helyzet a verseny ellen dolgozik, így háttérbe szorul a gazdasági, technológiai fejlődés.[1]

Mielőtt folytatnám a biztonságelméletek bemutatását meg kell határozni azokat a kereteket, melyek között a vizsgálatokat elvégzem. A legmeghatározóbb kapcsolat a két elméleti vonal között a biztonság, hiszen ez van a kérdések középpontjában és a biztonság fogalmához, illetve tulajdonságaihoz való viszonyuk határozzák meg a tradicionalisták és nyitók közötti különbségeket.

Biztonsági kérdések vizsgálata

Mit tekinthetünk biztonsági kérdésnek? A tradicionalisták egyszerűen megválaszolják: a katonai kérdések megegyeznek a biztonsági kérdésekkel. Szélesebb körben sajnos már nem lehet egyértelműen, objektíven meghatározni azt, hogy mit takar a biztonság kérdésköre.

Mi a biztonság?

Elkerülhetetlen és a legfontosabb kérdés az, hogy mit is értünk biztonság alatt? A kifejezés önmagában mindenki számára egyértelmű, hiszen egy nyugodt, fenyegetettségtől mentes állapotot jelent. Mélyebbre ásva azonban számos elmélet és szemléletmód kapcsolódik a biztonság fogalmához, ami hatást gyakorol a biztonsági kérdések vizsgálatára is. Az alábbiakban idéznék néhány definíciót meghatározó forrásokból.

Az Új Magyar Lexikon meghatározása: „Külpolitikai":~ állapot, melyben az állam függetlenségét más állam részéről nem fenyegeti támadás, és nincs kitéve annak a veszélynek, hogy a belső ügyeikbe külső hatalom beavatkozzék.[1]

Az UNESCO meghatározása: A fizikai veszély hiányát, vagy az e veszéllyel szembeni védekezést jelenti.

[1] Új Magyar Lexikon (Akadémiai Kiadó, Bp. 1959.)

Az Amerikai Nemzetbiztonsági Stratégia: A nemzetbiztonság nem csak lakosságunk és területeink védelme a közvetlen támadástól, hanem létfontosságú gazdasági és politikai érdekeink védelme különféle eszközökkel.

A Hadtudományi Lexikonban a következő olvasható: A biztonság: egyének, csoportok, országok, régiók (szövetségi rendszerek) a maguk reális képességein és más hatalmak, nemzetközi szervezetek hatékony garanciáin nyugvó olyan állapota, helyzete (és annak tudati tükröződése), amelyben kizárható vagy megbízhatóan kezelhető az esetleges bekövetkező veszély ill. adottak az ellene való eredményes védekezés feltételei.[2]

Összességében elmondható, hogy a biztonság fogalma valamiféle fenyegetés köré épül, mely fenyegetésnek van egy forrása és egy alanya. A fenyegetés meghatározása lehet objektív és szubjektív. Előbbi a tradicionális vonulatra, míg az utóbbi az újszerű gondolkodásra jellemző. A fenyegetéshez kapcsolódóan a biztonság jelentheti a fenyegetés hiányát, vagy a fenyegetés korlátozására, visszaszorítására alkalmazható eszközök meglétét. A tradicionális gondolkodók közül például Stephen Walt szerint a biztonsági tanulmányok tárgya a fenyegetés, illetve a fegyveres erők felhasználása és irányítása. Ezzel szemben az újszerű gondolkodók közül Daniel Deudney a biztonságot közjóként tekinti, míg Ole Waever egy olyan állapotot lát mögötte, ahol a fenyegetések léteznek, de képesek vagyunk ellenlépések megtételére. A biztonságelmélet kutatói között elfogadott megfogalmazás úgy hangzik, hogy a biztonság jogalap erőszakos, a hétköznapitól eltérő eszközök használatára a fenyegetés visszaszorítása érdekében.[1]

Vizsgálati szintek

A vizsgálat szintekre osztása segíti a szereplők, az érintettek rendszerezett meghatározását, segít leírni egy adott rendszer (komplexum) belső kapcsolatrendszerét, létrejöttének okát és körülményeit, valamint a nemzetközi színtéren elfoglalt pozícióját. A biztonsági tanulmányok a nemzetközi kapcsolatok rendszerének szintjeit alkalmazzák saját vizsgálataik során. Ezek a szintek a következők:

1. Nemzetközi rendszerek:
Jelenleg egy nemzetközi rendszert tudunk meghatározni, ez pedig nem más, mint a bolygó összes szereplője által alkotott legnagyobb egyesülés.

2. Nemzetközi alrendszerek:
Olyan egységek csoportja a nemzetközi rendszeren belül, amelyek egyértelműen elkülöníthetők természetük, illetve interakcióik és kölcsönös egymásrautaltságuk által. Területi alapon szerveződött alrendszer esetén regionális szerveződésről beszélünk.[3]

3. Egységek: Szervezetek, közösségek egysége, akik önálló szereplőként képesek megjelenni. Például államok, nemzetek, nemzetközi vállalatok.

4. Alegységek: Egyének szervezett csoportja, akik képesek a náluk eggyel magasabb egységre befolyást gyakorolni.

5. Egyének: A társadalomtudományok vizsgálati szintjeinek legalsó eleme.

[2] Hadtudományi lexikon (MHTT, Bp., 1995)
[3] A klasszikus biztonságelméletben a területi alapon szerveződött alrendszert, egységet tekintjük biztonsági komplexumnak.

Szektorok

Míg a szintekkel a biztonsági kérdések alanyait osztottuk fel hierarchikus, kölcsönhatásokat és viszonyokat tükröző rendszerben, vagyis egyfajta vertikális struktúrát határoztunk meg, addig a szektorok a biztonsági kérdések tárgyát, a fenyegetés forrását illetve célját kategorizálja. Mondhatjuk, hogy ez egy horizontális struktúrát eredményez, azonban a szektorok nem egymás mellett, hanem egymással összefonódva helyezkednek el. A szektorok, csakúgy, mint a szintek, kölcsönhatásokat azonosítanak: • katonai értelemben a fegyveres összeütközést:

- politikai értelemben a hatalmat gyakorlók kapcsolatait, elismertségét;
- gazdasági értelemben a kereskedelmi, termelési, pénzügyi kapcsolatokat;
- társadalmi értelemben a kollektív tudatot jelenti;
- míg környezeti vonatkozásban az ember és a természet kapcsolatát tükrözi.

Az iménti szektorok adják a nyitó elméleti vonalat képviselők számára az alapot a biztonság dimenzióinak meghatározásához.

Barry Buzan az alábbi módon definiálja a dimenziókat:

- katonai: államok támadó és védelmi képessége, illetve a szereplők egymás iránti szándéka;
- politikai: államok szervezeti stabilitása, kormányzati rendszerének és ideológiájának legitimitása;
- gazdasági: nyersanyagok hozzáférhetősége, pénzügyi és piaci lehetőségek a jólét és stabilitás fenntartására;
- társadalmi: fejlődés, fenntarthatóság, örökség[4] megőrzése;
- környezeti: helyi és bolygó szintű bioszféra épségben tartása az emberiség jövője szempontjából.

Buzan szerint az állam minden szektorban központi tényezőként van jelen, viszont más szereplőket is beenged, hogy valódi többszektoros elméletről beszélhessünk.[1] A szektorok, dimenziók sajátos jellemzőket azonosítanak, ezért elméleti szinten jól elkülöníthetők egymástól, azonban a biztonsági kérdések vizsgálata során ez nem célszerű és gyakorlatilag nem is lehetséges. Egyes kérdések eredeztetése során elképzelhető a kizárólagosság, azonban mélyrehatóbb elemzés során közös metszéspontok alakulnak ki más szektorokkal is. Pontosan ez a jelenség hívta elő a többdimenziós szemléletmódot, illetve ez teszi komplexszé és szubjektívvé a biztonsági kérdések tárgyalását. Egy megnevezett fenyegetés - legyen akár külső, vagy belső - forrása és célja nem feltétlenül ugyanaz a szektor. A fenyegetés visszaszorítására, kezelésére alkalmazott eszközök is származhatnak különféle szektorokból. Remek példa erre a vezető gazdasági hatalmak által alkalmazott embargó, mint gazdasági eszköz. Egy adott régióban potenciális katonai fenyegetést jelentő állam ellen gazdasági eszközöket alkalmaznak, hogy elkerüljék a fegyveres összeütközést és csökkentsék a fenyegetés mértékét. A fenyegetés forrása több, mint valószínű, hogy politikai eredetű[5] az alkalmazott eszköz a katonai szektorban materializálódik, a válasz a fenyegetésre azonban első körben a politikai szektorból, majd az esetek jelentős többségében a gazdasági szektorból érkezik és csak legvégül jut el a fegyveres harcig a konfliktus.

[4] Hagyományok, nyelv, vallás, kultúra, nemzeti tudat.
[5] Nacionalizmus, gazdasági érdekérvényesítés szomszédos országokkal szemben, történelmi okok, stb.

Biztonsági komplexumok

A nemzetközi biztonság a szereplők közötti interakciókon, kapcsolatokon alapszik. A szereplők, egységek érdekeik és az érdekeikre hatást gyakorló külső tényezők[6] alapján regionális szerveződéseket, alrendszereket alkotnak. Ezeket az alrendszereket a klasszikus biztonságelmélet biztonsági komplexumnak nevezi. A komplexumok működését az alábbi szempontok alapján vizsgálja:

- az emberi közösségek hogyan viszonyulnak egymáshoz a fenyegetések és sebezhetőség tekintetében;
- miként függnek ezek a közösségek a természetes környezetből eredeztetett fenyegetésektől.

A szempontok vizsgálata során az alábbi kapcsolati tényezőket vehetjük figyelembe:

- biztonsági dilemmák;
- erőegyensúly;
- fegyverkezési verseny;
- biztonsági komplexumok, rezsimek.[1]

Klasszikus biztonsági komplexum elmélet

A klasszikus biztonsági komplexum elmélet regionális alrendszerekben gondolkodik, amelyen belül az állam a legfontosabb szereplő és a katonai, illetve politikai szektorok képezik a biztonság értelmezésének kulcsát. A komplexum létrejöttét, vagyis a tagok, szereplők összeszerveződését a földrajzi elhelyezkedés befolyásolja, mely meghatározza az állam szomszédjait, alapvető gazdasági helyzetét, melyekből következik reális érdekérvényesítő képessége.

Ezen tényezők összessége útmutató egy állam számára, hogy miként formálja kül- és biztonságpolitikáját, vagyis milyen gazdasági, politikai, katonai szövetségi rendszert alakítson ki. Ezek a rendszerek az említett tényezőkből fakadó biztonsági egymásrautaltság miatt a történelem során alakultak ki és földrajzilag jól elkülöníthető területeken mutatkoznak. Röviden a biztonsági komplexum olyan államok csoportja, melyek fő biztonsági érdekei annyira összefonódtak, hogy nemzeti szinten nem lehet a szereplőkről külön-külön érdemben beszélni.[1]

A klasszikus biztonsági komplexum az alábbi négy tulajdonsággal jellemezhető:

1. kettő vagy több állam alkotja;
2. ezen államok összefüggő területi egységet alkotnak;
3. ezen államok közötti kapcsolatot a kölcsönös biztonsági egymásrautaltság jellemzi;
4. a biztonsági egymásrautaltság nem állandó, de elég mély és stabil ahhoz, hogy közös érdekek fűződjenek köré a történelem egy bizonyos szakaszában.

Már többször előkerült, de ismételten szeretném kihangsúlyozni azt, hogy a klasszikus elméletben a komplexumokat területileg szomszédos államok alkotják. Az elmélet követői ezt azzal magyarázzák, hogy a klasszikus elmélet által tárgyalt fenyegetések annál jobban érezhetőek és realizálódnak, minél kisebb a földrajzi távolság. Ez a megállapítás kulcsfontosságú az új komplexumelmélet meghatározásakor. Biztonsági komplexumok hiányáról beszélhetünk akkor, hogyha egy adott területen lévő államok érdekérvényesítési képességei annyira csekélyek, hogy képtelenek a határaikon túli nyomásgyakorlásra, politikai és gazdasági érdekképviseletre. Ilyen esetben jellemző, hogy egy erős külső állam még jobban

[6] Földrajzi elhelyezkedés, szomszédok, nyersanyagok, nemzeti kisebbségek, stb.

elfojtja a helyi erők természetes viselkedését. A beavatkozásnak két módját határozzák meg a nemzetközi kapcsolatok kutatói:

1. Overlay: a külső fél helyi erőfölényt alkalmazva elfojtja az adott közösség belső dinamikáját. Jellemzően katonai erő alkalmazásával jár.
2. Beavatkozás: megerősíti a helyi dinamikát. Jellemzően katonai erő nélkül történik.

A klasszikus elmélet a komplexum viselkedésének belső dinamikáját a barátság - ellenség görbéjén vizsgálja. A negatív oldalt a konfliktuson, félelmen, versengésen alapuló egymásra utaltság jellemzi. Középen az egyensúlyi állapotot írja le, ahol érezhető ugyan a fenyegetés, de már tettek megelőző lépéseket a felek. A pozitív oldalon szerepel a biztonsági közösség, ahol a partnerek nem tervezik erőszak alkalmazását a másik féllel szemben. A biztonsági komplexumok alrendszerek, miniatűr anarchiák, tehát saját belső struktúrával rendelkeznek. A belső felépítésük vizsgálatával leírható, nyomon követhető az érintett régió biztonsági folyamatai, aktuális biztonsági kérdései. A három összetevő, mely alapján a komplexum felépítését vizsgálni lehet, a következő:

1. az alkotó egységek térbeli elhelyezkedése és a köztük fennálló különbségek;
2. a barátság és ellenségeskedés jelenléte, vagyis az egységek közötti interakciók hangulata;
3. az alrendszert meghatározó egységek közötti erőmegoszlás.

A három tényező bármelyikében bekövetkező változás a komplexum újraértelmezését vonhatja magával. A kérdés az, hogy a változás a struktúra megtartását vagy átalakítását célozza? A biztonsági komplexum elmélet kutatói négy lehetséges változási célt határoztak meg:

1. status quo megtartása:
   A komplexum erőmegosztása és viselkedési mintája nem változik. A változás a meglévő rendszer megerősítése céljából történt.
2. belső átalakulás:
   A változás a komplexumot belső kontextusában érinti. Belső regionális politikai integráció, vagy belső hatalom újrafelosztás következtében a belső struktúra változik, de a kifelé irányuló kapcsolatok érintetlenek maradnak.
3. külső átalakulás:
   A komplexum külső határai változnak és ennek következtében a struktúra is változik, alkalmazkodik. A külső átalakulás általában belső átszerveződéssel is járhat.
4. overlay:
   Külső erő megjelenése és aktív beavatkozása teljesen felborítja az eddigi rendet. A struktúra általában gyökeresen átalakul.

A biztonsági komplexum elméletének nyitása

A nyitás legnagyobb kérdése az, hogy a bevezetett új szektorok, dimenziók hogyan befolyásolják a komplexumok szerveződését?

A kutatók két lehetséges válasszal álltak elő:

1. Homogén komplexum: Ez az elmélet megtartja a klasszikusok azon gondolatát, hogy a biztonsági komplexum egy adott szektorra épül és jól meghatározható kapcsolatok alakulnak ki a közel azonos egységek között. Ezáltal különböző komplexumok alakulnak ki a különböző szektorokban, dimenziókban.

2. Heterogén komplexum: Felhagy az elszigetelt és különálló szektorok elméletével. Az elmélet szerint a különféle szereplők (egységek, alegységek) kapcsolatai átnyúlnak kettő vagy több szektoron és az így realizálódott háló jelenti a biztonsági komplexumot. A két

elméletnek megvan a maga előnye és hátránya, melyek a kutató szubjektív megítélése alapján befolyásolják, hogy mit választ.

A homogén elmélet lehetőséget ad a szektorok elszigetelt vizsgálatára, ami kizárja a külső, „zavaró" tényezőket, azonban minden egyes szektor számára fel kell építeni a saját környezetét, ennek következtében azonban a szektorok közötti kapcsolatokat nem lehet megfelelő módon vizsgálni. A heterogén rendszer esetében minden érintett szektort egyszerre kell vizsgálni, ami lehetőséget ad a szektorok közötti folyamatok feltárására és figyelembe vételére, azonban ez bonyolultabbá teszi az elemzést. A gyakorlatban a két elméleti út nehezen választható szét, sőt szinte a heterogén nézőpont dominál, hiszen ez írja le a lehető legpontosabban a valóságban zajló folyamatokat.[1]

Barry Buzan a többdimenziós komplexum elmélet kapcsán a következő módon írja le a szektorokat:

1. Katonai szektor: Állam vagy valamilyen politikai szereplő a középpontban. Hagyományos értelemben minden katonai esemény „biztonsági" eseménynek tekinthető.[7] A modern demokráciák esetében azonban ez nem mindig igaz. Szövetségi kötelezettségből például misszióban való részvétel katonai esemény, azonban a szövetség tagjai közül nem érint mindenkit közvetlen fenyegetésként az adott misszió tárgya.

2. Politikai szektor: Állami önállóság, függetlenség és legitimitás van a középpontban. Minden esemény ami megkérdőjelezi a legitimitást, a hatalmat, fenyegetésnek számít. Államok közötti politikai entitások is ide sorolhatók.

3. Gazdasági szektor: Nehéz a vizsgálat középpontját alkotó szereplők meghatározása. A vállalatok létét fenyegeti az anyagi csőd, a változó törvényi keretek, stb. Ellenben ezek a szereplők nem jelentenek állandó tényezőt, mellyel saját maguk is tisztában vannak, ezért elméleti szinten nem foglalkoznak saját biztonságuk vizsgálatával. A nemzetgazdaságokat már érintik biztonsági kérdések, azonban ezek a fenyegetések más kontextusban jelennek meg. A fenyegetést kezelő szereplő az állam, a fenyegetés pedig leggyakrabban a háború.

4. Társadalmi szektor: Kollektív azonosság, amely képes államoktól függetlenül létezni. Nehéz meghatározni a veszélyforrásokat. A fejlődési folyamat átalakulással jár, ami kizár és beolvaszt bizonyos dolgokat. A kizárt dolgok megjelenhetnek fenyegetésként, de ez nem mindig egyértelmű.

5. Környezeti szektor: Rendkívül széles az érintettek listája. Ember és természet harmonikus kapcsolata a cél. Az ezt megváltoztató, hátráltató események veszélyként, fenyegetésként kezelhetők.

Buzan által definiált szektorok és a belőlük eredeztetett új komplexum elmélet nagy ugrás volt a - visszatekintve - egysíkú és korlátozott nézőpontokat feldolgozó klasszikus elmélethez képest. Lehetőséget adott arra, hogy a hidegháború utáni konfliktusok, kapcsolatok rendszerét árnyaltabban definiálhassák és a fenyegetések lehető legszélesebb skáláját meghatározhassák.

Az elmúlt húsz év infokommunikációs fejlődésének köszönhetően olyan változások következtek be a buzan-i szektorok belső szerkezetében, ami - véleményem szerint - szükségessé teszi a dimenziók felülvizsgálatát. A változási folyamatot itt és most - a korlátozott terjedelem és a témától való eltávolodás miatt - nem kívánom bemutatni és részletezni, azonban annyit szükségesnek tartok megjegyezni, hogy a folyamat eredményeként az emberiség által felhalmozott, illetve a folyamatosan keletkező információ, valamint az ezt kiszolgáló infrastruktúra értéke eddig még soha nem tapasztalt szinteket ért el.

Mielőtt bemutatnám ennek hatását a biztonsági komplexum elméletre úgy gondolom elkerülhetetlen, hogy a biztonsági kérdést, mint folyamatot megvizsgáljam és bemutassam.

[7] Klasszikus elmélet.

Biztonsági kérdéssé válás folyamata[8]

A biztonság, mint folyamat, átlépteti a politikát az elfogadott szabályokon túlra és speciális politikaként, vagy politikán túliként definiálja. A securitization angolszász kifejezés azt a folyamatot jelenti, amikor a fenyegetésben érintett szereplők[9] megfelelő lépésekkel biztonsági kérdéssé emelik az adott eseményt.

Állami szemszögből nézve ez a folyamat az „ átpolitizálásnak" egy extrém változata és az alábbi szintek állapíthatók meg:

1. nem átpolitizált: az állam nem foglalkozik a kérdéssel;
2. politizált: a nyilvános politika része, állami döntéseket és erőforrásokat igényel;
3. biztonsági kérdéssé emelt: az esemény fenyegeti a létbiztonságot, rendkívüli lépéseket kell tenni a mérséklése érdekében és feljogosít elfogadott kereteken kívüli cselekvésre is.[1]

A folyamat érdekes abból a szempontból, hogy egy önmagára hivatkozó cselekményről beszélünk, hiszen valami attól válik biztonsági kérdéssé, hogy azzá teszik. Kézzel foghatóbb módon megfogalmazva: a fenyegetés létezik, azonban a fenyegetés fenyegetésként történő bemutatása teszi azt valóban fenyegetéssé.

Egy esemény, probléma biztonsági kérdéssé emelésével, vagy „megbélyegzésével", lehetőséged ad arra, hogy a témát felhozó egyén különleges eszközöket alkalmazzon. A folyamat megértéséhez nem a fenyegetés objektív mivoltát, létezését kell felderíteni, hanem azt, hogy a szereplő, aki biztonsági kérdésként hozta fel a kérdést, milyen módon teszi közössé a problémát a hallgatósággal és hogyan válik közös fenyegetéssé a probléma.

A folyamat három állomását lehet meghatározni:

1. egy létező fenyegetés;
2. a fenyegetés által kiváltott cselekvés, amely a fenyegetés visszaszorítására vagy megszüntetésére irányul;
3. a kiváltott cselekvés következménye az érintett egységen belüli kapcsolatokra.

A folyamat szempontjából a biztonsági szektorokat olyan határoknak lehet tekinteni, amelyeken belül pontosan leírható, az adott szektorra jellemző interakciók zajlanak. Az interakciókban résztvevő szereplők számára a biztonság ugyanazt jelenti, azonban a megjelenési formája más és más.

A folyamat egészét megvizsgálva eljutunk az újító gondolkodók azon megállapításához, miszerint a „több biztonság nem egyenlő a nagyobb biztonsággal". Ezzel azt kívánják kifejezni, hogy optimális esetben a minél kevesebb biztonsági kérdéssel foglalkozó egység, alrendszer elérte azt, hogy a hagyományos politikai eszközökkel sikerült normalizálni az egység, alrendszer hosszú távú működését ezért csak minimális rendhagyó lépésekre van szükség.

Láthatjuk, hogy ez a kijelentés valóban csak elméleti szinten, optimális esetben létezhet, hiszen az imént volt szó arról, hogy valami biztonsági kérdésként kezelése valójában egy szubjektív mozzanat, amihez külső jóváhagyásként a kérdésben érintettek közreműködésére is szükség van. A közreműködés, támogatás meghatározása azonban rendkívül nehéz és legtöbbször a biztonsági kérdést felvető egyén képességein múlik a siker.

Állami szintre vetítve ezt a problémát megállapítható, hogy a nemzetbiztonsági kérdéskör lehetőséget ad a veszélyek, fenyegetések hatalomszerzés és megtartás céljából történő kihasználására.[1]

A folyamat során két nagyon fontos kérdés merül fel:

[8] Securitization
[9] Nem az alanyok.

1. Mi fog történni, ha nem teszünk „biztonsági lépéseket”?

2. Mi fog történni, ha teszünk? (Hogyan kellene működnie az elfogadott biztonsági lépéseknek?)

Mindkét kérdés egy jövőben potenciálisan bekövetkező állapotot vizsgál ezért nehéz tudományos választ találni rájuk. Az első kérdés mindenképpen kritikus a folyamat kezdetén, hiszen ezzel lehet alátámasztani a kérdés szempontjából már fenyegetésnek számító probléma következményeit az érintettekre.

A második kérdésre nehezebb megadni a választ, mert a korábban megfogalmazott fenyegetésre adandó válasz és az ezt lehetővé tevő, végrehajtó biztonsági cselekvés módja, kivitelezése[10] függ az érintettektől, vagyis az eredeti biztonsági kérdés megfogalmazójától és a fenyegetés alanyaitól.

A folyamatban három szintre oszthatjuk a résztvevőket:

1. hivatkozási alany;
2. a biztonsági kérdést megfogalmazó szereplő;
3. funkcionális, működő szereplő.

A hivatkozási alany az, akinek joga van a túléléshez a fenyegetésekkel szemben, vagyis ő az, akit közvetlenül fenyeget valamilyen esemény, veszély. A kérdést megfogalmazó szereplő az, aki az adott eseményt biztonsági kérdéssé emeli azzal, hogy valakit - a hivatkozási alanyt - fenyegetve tünteti fel az adott eseménnyel szemben. A funkcionális szereplő létezésével hatást gyakorol az adott szektor dinamikájára, azonban nem jelenik meg hivatkozási alanyként vagy biztonsági kérdést megfogalmazó szereplőként.

Buzan remekül hozza fel példaként a környezeti szektorban a nehézipari szereplőket, akik létezésükkel szennyezik a környezetet, azonban ez a folyamat nem veszélyezteti a létezésüket, ezért ők maguk ebből nem csinálnak biztonsági kérdést és mások sem hivatkoznak rájuk ebben a tekintetben.[1]

Biztonsági komplexum és az információ

Szükségesnek tartottam a klasszikus és újszerű biztonságelméleti modellek alapjait bemutatni, mert azok alapszintű ismerete nélkül nehéz rávilágítani az információ, de leginkább az információt feldolgozó infrastruktúra okozta változások hatásaira.[5]

Az infrastruktúra bemutatására nem szeretnék kitérni, azonban annyit kívánok szűkíteni a fogalmon, hogy az informatikai infrastruktúrát és globális szinten a világhálót értem a kifejezés alatt. A jelen tanulmány további gondolataihoz ennél részletesebben nem szükséges tárgyalni ezt a kérdést. Az információról, mint változást előidéző tényezőről azonban ejtenék néhány szót. A tudás mindig is meghatározó tényezője az emberi társadalomnak.[3]

A nem nyilvános, vagy csak kevesek által ismert információ előnyt jelenthet azok számára, akik birtokolják, éppen ezért az információ-szerzés fontos szerepet kap az emberek közötti kommunikációban. Ez a jelenség végigkíséri történelmünket az őskortól egészen napjainkig. Uralkodói, illetve állami szinten a XX. század közepéig a katonai jellegű, valamint az ország háborús képességeit befolyásoló, a gazdasági szektor és a politikai vezetés alrendszereiben fellelhető információk kaptak prioritást, míg a civil szférában egyértelműen a gazdasági információ rendelkezik releváns értékkel.[4]

Dorothy Denning szerint az információ értékének két összetevője van: átváltható, illetve műveleti érték. Az átváltható érték mérhető, a piac határozza meg, és azt mutatja, hogy valaki

[10] Ezek összessége adja meg a kérdésre a választ.

mennyit hajlandó megadni az adott információért. A műveleti érték megmutatja, hogy milyen nyereség várható az adott információ felhasználásával.[2]

Az információ alapú hadviselés és biztonság szempontjából az utóbbinak van jelentősebb szerepe. A védekezés oldaláról megközelítve azt a kérdést, hogy mekkora egy adott információ értéke, az alábbi problémák merülnek fel:

• nem tudjuk felmérni, hogy adott információ milyen értéket képvisel más számára, ezért nehéz a kiemelten védelmezni kívánt információk körét szűkíteni;

• nehéz meghatározni, hogy egy általunk birtokolt információ megszerzése milyen előnyökhöz juttatja az adott személyt, szervezetet, esetleg államot, mely függ:

- képes-e egyáltalán felhasználni a megszerzett információt;
- milyen célra és hogyan kívánja felhasználni, a megszerzéstől számítva milyen gyorsan képes ezt megtenni;
- milyen egyéb információk vannak a birtokában, melyek esetlegesen megnövelik az újonnan szerzett információ felhasználhatóságát (műveleti értékét);
- milyen konkurens szereplők jelennek meg az információ megszerzéséért folytatott harcban.

Ezzel a néhány gondolattal azt kívántam bemutatni, hogy az információ értéke az informatikai rendszerek hatására olyan szinten megnőtt, hogy közvetlenül befolyást gyakorol az őt körülvevő szektor belső működésére, amely kihat az egység, alrendszer és rajtuk keresztül közvetve az adott biztonsági komplexum belső dinamikájára.

Dolgozatom témája szempontjából a legfontosabb változás a tér és idő fogalmának újraértelmezése. A világháló és hozzá kapcsolódó szolgáltatások gyakorlatilag megszűntették a kapcsolattartás távolság és idő okozta korlátait. Az elmúlt évtizedek során az információtechnológia beépült a különböző vizsgálati szintek működési mechanizmusába, ezért az egyéntől egészen a nemzetközi rendszerig valamilyen formában megtalálható az informatika és az általa tárolt, feldolgozott információ, mint a rendszer egy kritikus pontja. Ez az integráció alapjaiban véve azonos változásokat idézett elő, melyek közül a tér és idő problémáját már említettem, azonban ezeken kívül még említésre méltó az információ hozzáférhetőségének tulajdonsága, mely egy érme két oldalához hasonlítható. Nagy általánosságban azt lehet mondani, hogy a világhálón tárolt információ egyrészről előnyös a legitim felhasználó számára, mert nincs helyhez kötve, másrészről ezt egy vetélytárs is kihasználhatja a megfelelő képességek birtokában. Ez a megfogalmazás természetesen nagyon egyszerű, de az alapvető gondolat helytálló és jelen cikkben nincs lehetőség ezen problémakör mélyebb kifejtésére.

A klasszikus biztonságelméletből kiindulva látható, hogy az elmélet alapjait dönti meg az informatika. A résztvevők interakcióiban már nem játszik szerepet a távolság, hiszen ez a fogalom gyakorlatilag nem létezik ebben a viszonylatban. A globális valós idejű kapcsolatok miatt a szektorokon belüli interakciók átalakulás alatt vannak melyek hatására átértékelődnek a szektorokon belüli és szektorok közötti kapcsolatok. Nem szükséges közvetlen fizikai szomszédságban lennie két szereplőnek ahhoz, hogy hatást, ellenhatást gyakoroljanak egymásra.

A korábban felvázolt vizsgálati szintek között is észrevehető változás. A klasszikus és a nyitó elméletek az államot, vagyis az egységeket, és az államon belüli, esetleg azzal nagyjából egy szinten lévő alegységeket[11] veszi a középpontba és rájuk építkezik, hiszen ezen szereplőknek van meg az a fizikai és elméleti hátterük, hogy hatást gyakoroljanak az őket érintő szektorokra. A korábban felvázolt tér és idő problémával együtt figyelembe kell venni

[11] Például gazdasági, politikai, katonai szervezetek.

azt is, hogy az információs hálóba való becsatlakozáshoz szükséges tudás és eszköz megszerzésére már az egyén szintjén lehetőség van.

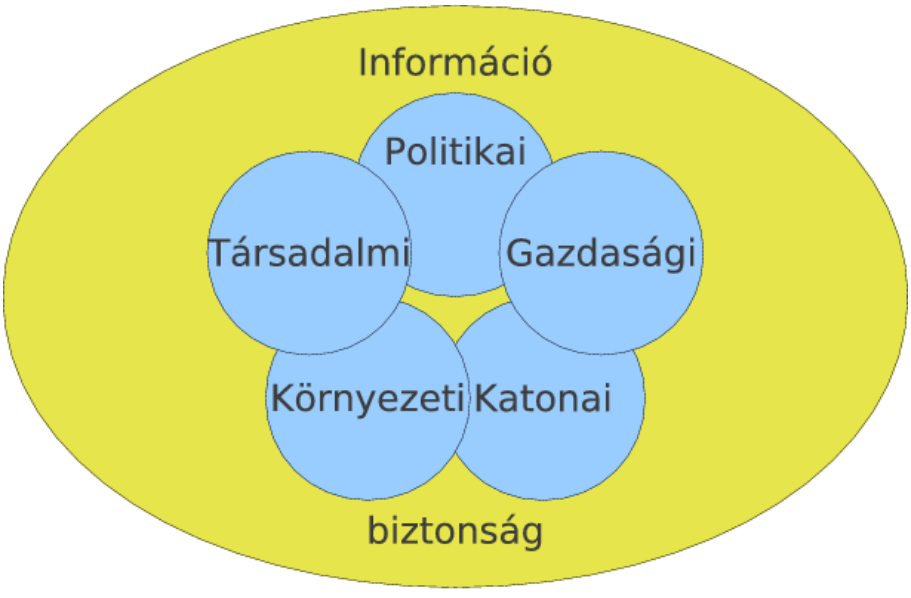
Ezt követően az egyén számára feltárul egy olyan világ, ahol akár képes lehet a nála magasabb szinteken lévő működési mechanizmusokra hatást gyakorolni. Ez természetesen megint egy elméleti állapot, de a lehetőség adott. Kicsit reálisabb példa lehet azonban az, hogy egy adott alegység, például gazdasági szervezet vagy terrorista csoport, olcsóbb, könnyebben és anonim módon beszerezhető eszközökkel tud befolyást gyakorolni. A fontos gondolat az, hogy az egyén és az alegység szerepe megnő a megváltozott érdekérvényesítő képesség miatt. Ezek a változások hatással vannak a biztonsági kérdések életciklusaira is. Említettük, hogy a biztonsági kérdésnek van egy hivatkozási alanya.

Ez az alany egy adott kérdést tekintve változatlan, hiszen nem a fenyegetés változott, hanem a fenyegetés realizálásának a módja. A biztonsági kérdést felvető szereplőnek lesz nehezebb dolga, mert míg a fenyegetést meg tudja határozni, addig a fenyegetés lehetséges forrásai gyarapodtak.

Korábban egy fenyegetés realizálása szinte csak a hivatkozási alany működéséhez köthető területen következhetett be, mint például egy gazdasági-technikai áttörés, piaci pozíciót befolyásoló lépések, politikai vetélytárs elleni győzelem, stb. Az információ-technológia hatására lehetőség van egy alany működésének befolyásolására, veszélyeztetésére egy olyan dimenzióban, amely ezidáig nem volt szerves része, illetve nem tartozik szigorúan hozzá.

Az iménti gondolatok alapján felvázolnám egy kezdeti, úgynevezett „információ szektor” vázát a buzan-i meghatározások alapján. Hangsúlyozom, hogy ez csak egy váz, amire további kutatásomat kívánom építeni.

- Információ szektor:
  - Multiszektorális, vagyis a megjelenése nem szűkíthető le egy szektorra
  - Bármelyik szektorból kerülhet ki hivatkozási alany és biztonsági kérdést megformáló szereplő
  - A fenyegetést könnyű meghatározni
  - A következményeket nagyon nehéz
  - Megváltozik az eddigi vertikális vizsgálati szint
  - Fenyegetések új dimenziója



1. ábra. A hatodik dimenzió

Összességében elmondható, hogy a vizsgálati szinteken megjelenő szereplők működésére és az őket érő fenyegetések jellegére hatást gyakorol az információ. Ennek következményeként az információnak, mint tényezőnek, meg kell jelennie a biztonsági komplexumok vizsgálata során.

A buzan-i ötdimenziós modellt alapul véve megállapítható, hogy az információ és az információt feldolgozó infrastruktúra jelen van és befolyásolja, körülöleli mind az öt szektort. (lásd: 1. ábra.)

Irodalom

[1] Barry Buzan - Ole Waever - Jaap de Wilde. Security: A New Framework for Analysis. Lynne Rienner Publishers, 1998.

[2] Dorothy E. Denning: Information Warfare and Security. Addison-Wesley, 1999.

[3] Glatz Ferenc (szerk.): Az információs társadalom. Magyar Tudományos Akadémia, 2000.

[4] Matus János (szerk.): Biztonságpolitikai szöveggyűjtemény. Zrínyi Miklós Nemzetvédelmi Egyetem, 1999.

[5] W. Schwartau: Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age. Thunder's Mouth Press, 1996.

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Illési Zsolt
illesi.zsolt@proteus.hu

AZ IGAZSÁGÜGYI INFORMATIKAI SZAKÉRTÉS MODELLEZÉSE

Absztrakt

A büntetőeljárás során végzett informatikai igazságügyi szakértői feladatok rendkívül sokrétűek és összetettek. A szakértés eredménye gyakran elbillentheti Justitia mérlegét a felek számára kedvező vagy épp kedvezőtlen irányba ezért mindenki számára fontos, hogy a szakértés jó minőségű legyen. A hazai informatikai szakértői munka minőségére azonban jelentős szórás jellemző; attól függ, hogy a szakértő milyen felkészült, milyen eszközparkja van, és milyen módon gondoskodik a továbbképzéséről. A jelenlegi jogszabályok előírják ugyan a szakértői módszertani levelek elkészítésének és publikálásának a követelményét, azonban ezt a kötelezettek nem hajtották eddig végre. A cikk a módszertani levelek kialakításának elkezdésére tesz kísérletet, bemutatva, hogy az UML modellezés milyen jó szolgálatot tehet ebben.

Computer forensic tasks made during the criminal procedure are very diverse and complex. The forensic expert's report may turn the balance of Justitia's scale favourably or unfavourably to the parties, so the good quality of the forensic expert is important to everyone. The quality of the work of domestic computer experts, however, varies considerably. The quality depends on the expert preparation, the available technical tools and his/her arrangements for training. The current legislation requires the preparation and publication of letter of expert's methodologies; however, the obligation has not been implemented. This article attempts to start developing such methodology letters, demonstrating the good services that that UML modelling can do.

Kulcsszavak: *büntetőeljárás, informatikai igazságügyi szakértés, modellezés, UML ~ criminal procedure, computer forensics, modelling, UML*

BEVEZETÉS

A bűnüldöző szervek, a hatóságok és a bíróság a büntetőeljárás során többször kerülnek olyan helyzetbe, hogy a tényállás egyes elemeinek értelmezéséhez nem elegendő az általános műveltség, hanem sajátos felkészültség és ismeret szükséges. Ezt a speciális szakmai ismeretet biztosítják a Magyar Igazságügyi Szakértői Kamara (a továbbiakban: MISZK) tagjai az eljáró hatóságok számára.

Az eljárók szakértőkkel és a feladataikkal kapcsolatban a jogszabályok (a szakértői tevékenységről szóló 2005. évi XLVII törvény, az igazságügyi szakértői kamaráról szóló 1995. évi CXIV. törvény, az igazságügyi szakértői működésről szóló 31/2008. (XII. 31.) IRM rendelet stb.) részletesen meghatározzák, hogy kik, milyen módon végezhetik a tevékenységüket.

Informatikai igazságügyi szakértőként azt tapasztalom, hogy a büntetőeljárások mindennapi gyakorlatában informatikai és igazságügyi jellegű szakértői feladatokat nem igazságügyi szakértők (pl. a hatóságok munkatársai, eseti szakértők) is ellátnak, illetve az informatikai igazságügyi szakértők munkája a végzettségük, szakmai tapasztalatuk és eszközparkjuk függvényében jelentős szakmai és minőségi eltérést mutat. A szakvélemények heterogenitása, minőségi különbségei azért jelentenek problémát, mert azok esetleges fogyatékosságai miatt az ügydöntő hatóság a tényállást nem tudja helytállóan megállapítani, utólagosan rekonstruálni így előfordulhat, hogy a sértettek nem nyernek megfelelő elégtételt és kártérítést, a bűnösök nem kapnak megfelelő büntetést. A szakvélemények hibája miatt előfordulhat pont az ellenkezője is: sértettként leshetnek azonosítva és kártérítést kaphatnak arra jogosulatlanok és bűnösként lesznek elítélve akár ártatlanok is. Véleményem szerint az informatikai szakvélemények szakmai színvonalának emeléséért rengeteget kellene és lehetne tenni, ennek megvannak mind a szakmai, mind a módszertani alapjai.

A szakvélemények általános hibái

- kompetencia megsértése (azaz a jogkérdésben nyilvánított vélemény, a kirendelő határozatban fel nem tett kérdésre adott válasz[1] és a leleten kívül található forrásból származó bizonyítékokra tekintettel adott szakvélemény),
- tartalmi megalapozatlanság (azaz, az iratellenesség, téves következtetés, hiányzó ténymegállapítás és felderítetlenség),
- módszertani megalapozatlanság (azaz a szakértő a szakvéleményben nem, vagy értékelhetetlen sekélyességgel jelöli meg a vizsgálat módszerét és annak validitását).

{[1] p136}

Meg kell említeni, hogy a módszertanok bizonytalanságai nem általánosak a MISZK szakértői körében. Vannak olyan igazságügyi szakmai részterületek (igazságügyi orvostan, közúti közlekedésbiztonsági műszaki, igazságügyi könyvszakértő), amelyekre az a jellemző, hogy képviselői egységes módszertani elvek alapján végezik a tevékenységüket. Ez az egységesség és módszertani megalapozottság azonban egyáltalán nem a MISZK érdeme, hanem a fenti szakterületeket delegáló kamarák (Magyar Orvosi Kamara, Magyar Mérnöki Kamara és a Magyar Könyvvizsgálói Kamara) színvonalát és több évtizedes szakmai munkáját dicsérik.

A minőségi eltérések mellett jellemző az is, hogy informatikai kérdésekben a kirendelő/ megbízó hatóság az informatikai szakmai kompetencián túlmutató kérdésekre is választ vár (pl. szerzői jogsértések esetén az okozott kár, a károsult azonosítása vagy a

[1] Ilyennek kell tekinteni a kirendelő határozatokban gyakran előforduló „*a szakértő egyéb észrevételei*" jellegű formulákra adott, az érdemi kérdések keretén túlmutató válaszokat is.

jogsértés meglétének megállapítása).

A módszertani levelek lehetőséget biztosítanának a büntetőeljárásban a kirendelő hatóságok laikus tagjainak arra is, hogy egy szakmai katalógusra épülve szakszerű kérdéseket tegyenek fel, illetve a módszertani levelek segítenek abban is, hogy a laikusok értelmezni is tudják a kérdéseikre adott szakmai válaszokat.

Jelen cikkemben áttekintem a büntetőeljárásban az igazságügyi szakértői vélemények sztenderdizálásának – a szakértői módszertani leveleknek – a jogszabályi hátterét, a módszertani levelekkel szemben támasztott minimális követelményeket. A követelmények ismertetése után szeretnék ismertetni néhány UML modellt, amellyel demonstrálni szeretném, hogy a megfelelő modellek kiindulópontjai lehetnek az informatikai igazságügyi szakértői leveleknek, így reményeim szerint az informatikai szakág felzárkózhat a nagy múltú szakágak mellé az igazságügyi szakvélemények minősége tekintetében is, sőt meg is előzheti azokat.

IGAZSÁGÜGYI SZAKÉRTŐI MÓDSZERTANOK JOGSZABÁLYI KÖRNYEZETE

Szakértői módszertani levél

A szakértői módszertani levelekkel kapcsolatban három jogszabály határozza meg a tennivalókat:

1) Az igazságügyi szakértői kamaráról szóló 1995. évi CXIV. törvény (a továbbiakban: Iszktv.) [2] a módszertani levelekkel kapcsolatban kimondja, hogy
   A Magyar Igazságügyi Szakértői Kamara
   16. § (2) A küldöttgyűlés
   g) megalkotja a szakértői tevékenység etikai kódexét és az etikai eljárási szabályzatot, a szakértőjelölti igazolvány kiadásáról és külalakjáról szóló szabályzatot, valamint a szakértői módszertani levél kiadásának részletes szabályairól szóló szabályzatot.

2) Az igazságügyi szakértői tevékenységről szóló 2005. évi XLVII. törvény (a továbbiakban: Szaktv.) [3] a szakértői módszertani levelekkel kapcsolatban a következőket állapítja meg:
   Szakértői módszertani levél
   30/A. § (1) A MISZK elnöksége (a továbbiakban: elnökség) a szakértői tevékenység egységes és magas színvonalú ellátása érdekében szakértői módszertani levelet ad ki. A módszertani levél kiadását a MISZK és a szakértői kamara szakbizottságai, valamint a miniszter indítványozhatja.
   (5) Az elnökség nem adhat ki szakértői módszertani levelet olyan szakterületen, amelyen az egészségügyért felelős miniszter vagy annak irányítása, felügyelete alatt működő szervezet külön jogszabály alapján módszertani levél kiadására jogosult.
   30/C. § (1) A miniszter gondoskodik a szakértői módszertani levél Hivatalos Értesítőben történő közzétételéről, és az általa vezetett minisztérium honlapján való megjelentetéséről. A szakértői módszertani levél – annak visszavonásáig – a honlapról nem távolítható el.
   (3) Az elnökség figyelemmel kíséri a közzétett szakértői módszertani leveleket, és szükség esetén intézkedik – a szakértői módszertani levél kiadására vonatkozó rendelkezések szerint – azok visszavonásáról, illetve új módszertani levél kiadásáról.
   30/D. § A szakértői módszertani levél a Hivatalos Értesítőben történő közzétételétől a kirendelő szerv számára tájékoztatásul, a szakértőnek pedig a szakértő tevékenység ellátása során iránymutatásul szolgál. Ha a szakértő a szakértői módszertani levélben

foglaltaktól eltér, azt a szakvéleményben meg kell indokolnia.

3) A büntetőeljárásról szóló 1998. évi XIX. törvény (a továbbiakban: Be.) [4] közvetlenül ugyan nem hivatkozik a módszertani levelekre, de több helyen is megköveteli a résztvevőktől, hogy definiálják az általuk használt módszereket, illetve a módszerekkel eszközökkel kapcsolatban sajátos követelményeket tesz:

Szakértői vizsgálat

105. § (1) A szakértő szakértői vizsgálat alapján ad véleményt. A szakértő a vizsgálatot a tudomány állásának és a korszerű szakmai ismereteknek megfelelő eszközök, eljárások és módszerek felhasználásával köteles elvégezni.

A szakvélemény előterjesztése

108. § (2) A szakvélemény magában foglalja

b) a vizsgálat módszerének rövid ismertetését,

Bírói engedély

203. § (1) A titkos adatszerzés engedélyezéséről a bíróság az ügyész indítványára e Fejezet VI. Címe szerinti eljárásban határoz.

(2) Az indítványnak tartalmaznia kell

c) a titkos adatszerzés tervezett alkalmazásával érintett nevét, illetőleg az azonosításra alkalmas adatot, valamint a titkos adatszerzés vele szemben alkalmazni kívánt eszközének, illetőleg módszerének megnevezését,

e) az alkalmazás 201. §-ban és 202. §-ban meghatározott feltételeinek a meglétére vonatkozó részletes leírást, így különösen az alapul szolgáló bűncselekmény megnevezését és a bűncselekmény gyanújára okot adó adatokat, a titkos adatszerzés elkerülhetetlen alkalmazását indokoló körülményeket, az alkalmazás célját és annak valószínűsítését, hogy a bizonyíték a titkos adatszerzés során alkalmazott eszközzel, illetőleg módszerrel beszerezhető,

(4) A bíróság az indítvány előterjesztésétől számított hetvenkét órán belül határoz. Ha a bíróság az indítványnak helyt ad vagy részben ad helyt, meghatározza, hogy kivel szemben, a titkos adatszerzés mely eszköze, illetőleg módszere mettől meddig alkalmazható.

A titkos adatszerzés végrehajtása

204. § (5) A titkos adatszerzés végrehajtásáról jelentést (168. §) kell készíteni, amely részletesen tartalmazza a titkos adatszerzés lefolyását, így különösen azt, hogy annak során milyen eszközt, illetőleg módszert, meddig és hol alkalmaztak…

A szakértői módszertani levelek elkészítését a jogszabály csak a MISZK feladatává teszi, azonban a Be. rendelkezéseiből kiderül, hogy például a titkos adatszerzés során az azt végrehajtónak előre meghatározott módszerek és technikák alapján kell a feladatát elvégeznie.

A minisztériumok honlapján is csak itt-ott lehet szakértői módszertani leveleket találni; ezeknek a központilag egységes kezelése és publikálása nem megoldott, csak eseti módon történik.

Szakértői feladatokat (vagyis, ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges Be. 99.§ (1) bek.) azonban nem csak az igazságügyi szakértők, hanem esetenként az eljáró hatóságok tagjai is végeznek. Nevesített szakértői jellegű feladatkör a szaktanácsadói, akinek az igénybevételét a Be. 182.§ (1) bekezdése megengedi, ha a bizonyítási eszközök felkutatásához, megszerzéséhez, összegyűjtéséhez vagy rögzítéséhez különleges szakismeret szükséges.

Érdekesség, hogy amíg az igazságügyi szakértéssel és szakértővé válással kapcsolatban a jogszabályok szakmai szűrőket építettek be (képesítés, legalább ötéves szakmai gyakorlat, kötelező kamarai tagság ld. Szaktv. 3.§), addig az eljáró hatóságok szakértői jellegű

tevékenységet végző tagjaival és a szaktanácsadókkal szemben ilyen követelményt a jogszabályok nem tartalmaznak. (A szaktevékenységeknek szakértői módszertani levelekhez való kötése ezen a területen is jelentős javulást hozna, mivel az eljáró hatóság „laikus szakértőivel" és a szaktanácsadókkal szemben is meghatározna legalább egy szaktevékenységgel összefüggő módszertani és eszköz minimumot.)

Szakértők szakmai továbbképzése

A szakértői tevékenység minőségének javítását szolgálná a Szaktv. képzésekkel kapcsolatos fejezete is, amely kimondja:

> ***Az igazságügyi szakértők képzése***
> *18. § (1) Az igazságügyi szakértő részére szükséges* ***jogi ismeretek oktatásának*** *és a jogi vizsgának a megszervezéséről a miniszter gondoskodik. A rendszeres jogi oktatáson való részvétel és – a miniszter rendeletében meghatározott mentesülés esetét kivéve – az igazságügyi szakértő névjegyzékbe való felvételét követő jogi vizsga letétele kötelező.*
> *(2) Az igazságügyi szakértő a névjegyzékbe való felvételéről szóló határozat kézhezvételétől számított 15 napon belül köteles a jogi oktatásra és a jogi vizsgára jelentkezni vagy a vizsga alóli mentesülési feltétel meglétét igazolni.*
> *18/A. § Az igazságügyi szakértő számára kötelező a névjegyzékbe való felvételről szóló határozat kézhezvételétől számított egy éven belül a szakértés alapismereteivel összefüggő képzésben való részvétel és – a miniszter rendeletében meghatározott mentesülés esetét kivéve – az ehhez kapcsolódó vizsga letétele. Az alapismereti oktatásról és vizsgáról a MISZK gondoskodik, a vizsgát a mellette működő vizsgabizottság előtt kell letenni.*
> *18/B. § Az igazságügyi szakértő köteles a szakértői tevékenysége gyakorlásához szükséges rendszeres szakmai továbbképzésen részt venni, és a miniszter rendeletében előírt képzési kötelezettség teljesítését igazolni.*

A jogszabály alapján tehát jogi és szakmai képzéseket és vizsgákat is kéne szerveznie a MISZK-nek a minisztériumokkal karöltve. A jogi képzés valóban működik. A szakaértők a szakértéssel kapcsolatos jogi ismeretket megismerik, ebből vizsgáznak és jobbára megoldott a továbbképzés, az ismeretek felfrissítése is. A szakmai vizsga azonban szintén nem megoltott. Nincs olyan képzés, ami pl. az informatikai igazságügyi szakértés alapismereteivel függ össze. A probléma az, hogy olyan ismereteket egyetlen magyar felsőoktatási intézmény nem ad, amelyek az igazságügyi szakértés speciális követelményeivel foglalkoznának, nem ismertetik a rendelkezésre álló technológiákat, hardver és szoftver eszközöket, módszereket és technikákat. A hazai informatikai jogi felsőoktatás egyik fellegvárának számító Pécsi Tudományegyetemen az infokommunikáció kriminológiai ismeretei között csak a mátrix nyomtatók lenyomatának elemzésével foglalkoznak…

A jogszabályok elemzése alapján megállapítható tehát, hogy kötelező és szükséges lenne szakértői módszertani leveleket készíteni, de ezzel kapcsolatban informatikai téren nem történt semmi, a minisztériumok és a MISZK mulasztásos törvénysértést követnek el a módszertani levelek el nem készítésével és nem publikálásával.

AZ IGAZSÁGÜGYI INFORMATIKAI SZAKÉRTÉS MODELLEZÉSE

A jogszabályi elemzés és a józan paraszti és tehát azt sugallja, hogy az igazságügyi szakértés módszertani keretei legyenek rögzítve, ezzel is biztosítva a büntető eljárásban résztvevők számára az optimális szakmai munkavégzés.

Jelen munkámban a Unified Modeling Language[1] (a továbbiakban: UML) technikáival modelleztem a büntetőeljárást és az informatikai (igazságügyi) szakértést. A cikknek nem célja az UML ismertetése, és mivel ez egy az informatikában általánosan elterjedt műszaki ábrázolás és nem célom az UML ismertetése ezért a továbbiakban az egyes modelleknél csak speciális esetben magyarázom a modell elemeket.

A modellezési bemutatóm során a következő főbb kérdések megválaszolását és modellezését terveztem:

- Hol értelmezett az informatikai igazságügyi szakértői tevékenység?
- Mik a bizonyítás eszközei és a bizonyítékok állapotai?
- Kik a Büntetőeljárás szereplői, ezek közül ki vézet informatikai szakértés jellegű feladatokat?
- Mik a digitális nyomfelkutatás, -rögzítés, -biztosítás főbb állomásai és tevékenységei?

A modellezési példák során az UML osztálydiagram, állapotdiagram és használói esetdiagramokat alkalmaztam.

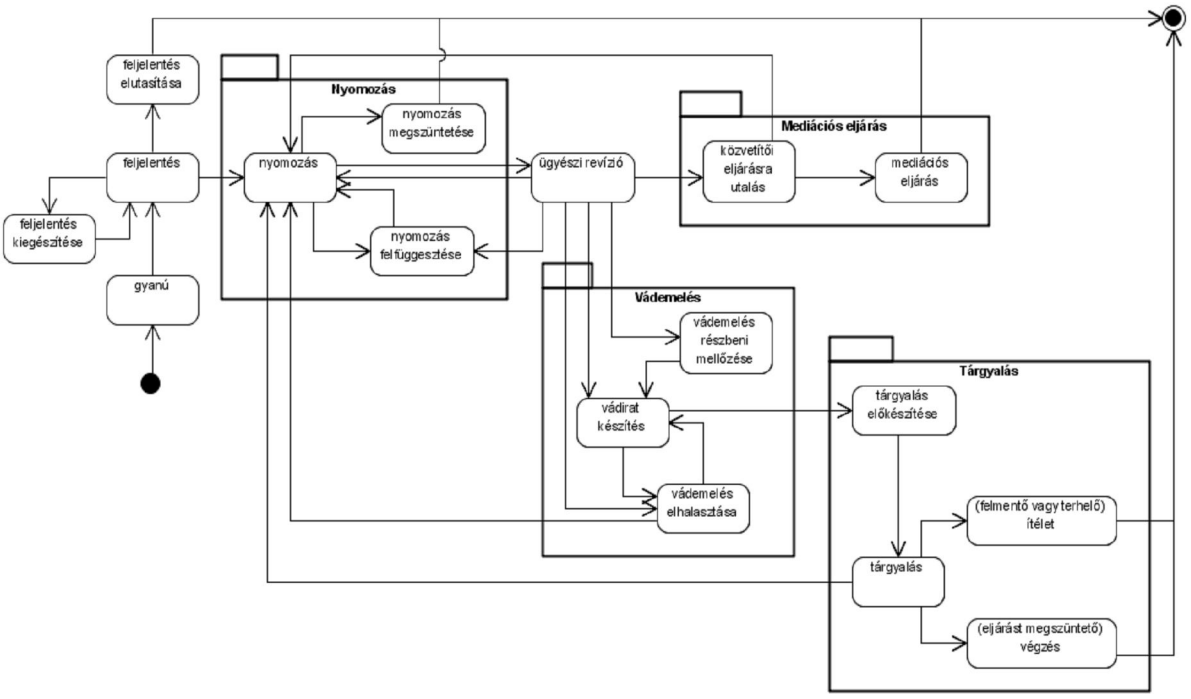
A büntetőeljárás

A büntetőeljárást a Be. szabályozza, ez alapján a főbb eljárási feladatok a

- nyomozás;
- vádemelés;
- mediációs eljárás;
- tárgyalás.

Ezek mellett természetesen a törvény több eljárási cselekményt is tartalmaz, amelyek összefoglalását a következő ábra tartalmazza:

[1] http://www.uml.org/



1. ábra. A büntetőeljárás főbb állomásai
(szerk.: Illési Zsolt)

A modellben nem szerepeltettem az egyes állomások részleteit, ezek belső kapcsolatait. Az ilyen al-modelleket természetesen létre lehet hozni, azonban az összkép felvázolásához és az egész eljárás felvázolásához ezek a részletek feleslegesek, sőt zavaróak lennének.

Informatikai szakértői feladatokat jellemzően a büntetőeljárás 3 fő mozzanatában (nyomozás, mediációs eljárás és tárgyalás) végeznek, azonban a feljelentés, illetve a feljelentés kiegészítés során szintén előfordulhatnak szakértői feladatok főleg magánvádas ügyekben (pl. interneten történő becsületsértés esetén).[1]

A bizonyítás eszközei

A bizonyítási eszközök azok a büntetőeljárási cselekmények vagy dolgok, amelyekből a hatóság, bíróság illetve az eljárás résztvevői a bűncselekményre vagy az elkövetőre vonatkozó ismereteket szereznek. A jogi szakirodalomban a bizonyítási eszköz kifejezés szinonimájaként a bizonyítékforrást is használják (mint olyan eszköz, amelyből a bizonyíték ered).

A Be. tartalmazza a törvényes bizonyítékforrásokat:

Be. 76. § (1) A bizonyítás eszközei a tanúvallomás, a szakvélemény, a tárgyi bizonyítási eszköz, az okirat és a terhelt vallomása.

(2) A büntetőeljárásban fel lehet használni azokat az okiratokat és tárgyi bizonyítási eszközöket, amelyeket valamely hatóság - jogszabályban meghatározott feladatainak teljesítése során a hatáskörében eljárva - a büntetőeljárás megindítása előtt készített, illetőleg beszerzett.

A fentiek alapján az informatikai igazságügyi szakértés tárgya elsősorban tárgyi bizonyítási eszközök (számítógépek, számítógépes hálózatok stb.), az eredménye pedig szakvélemény. Az infokommunikációs eszközökkel és rendszerekkel kapcsolatban a

bizonyíték az azokkal kapcsolatos tárgyi bizonyítási eszközökben tárolt, feldolgozott vagy az azokon keresztül továbbított adatokból nyerhető. A nyomokkal a kriminalisztika egyik részterülete a krimináltechnika foglalkozik. A klasszikus krimináltechnika szerint a nyom keletkezésében három tényező együttesen vesz részt:

- a nyomképző, vagyis az a dolog (tárgy vagy testrész), amely a nyomképződési folyamat során a nyom hordozón nyomot hagy;
- a nyom hordozó, vagyis az a dolog (tárgy, testrész, talajrész), amelyen a nyomképző a nyomképződési folyamat során nyomot hagy;
- a nyomképződési folyamat, vagyis a kölcsönhatás módját meghatározó folyamat, amely meghatározza a nyom egyedi jellemzőit, fajtáját.

A krimináltechnikában a nyom és az anyagmaradvány szorosan összefüggő fogalmak, és sok esetben csak a módszer alapján lehet eldönteni, hogy nyom vagy anyagmaradvány vizsgálata történt-e meg, azonban a két fogalom mégsem azonos, az alábbiak szerint különülnek el:

- nyom, a nyomhordozón a nyomképző érintkező felületének formája (alakbeli sajátosság) a vizsgálat tárgya (pl. harapás);
- anyagmaradvány, a nyomhordozón a nyomképző anyaga rakódik le és ennek elemzése a vizsgálat tárgya (pl. nyál). [5]

Véleményem szerint ezt a szűk értelmezést célszerű lenne kiegészíteni az adatmaradvány fogalmával, mivel a digitális nyom nem felel meg az anyagmaradvány vagy a lenyomat definíciójának, és olyan egyedi sajátosságokkal rendelkezik (pl. egy időben több helyen is hiteles „eredeti” formában állhat rendelkezésre) [6]

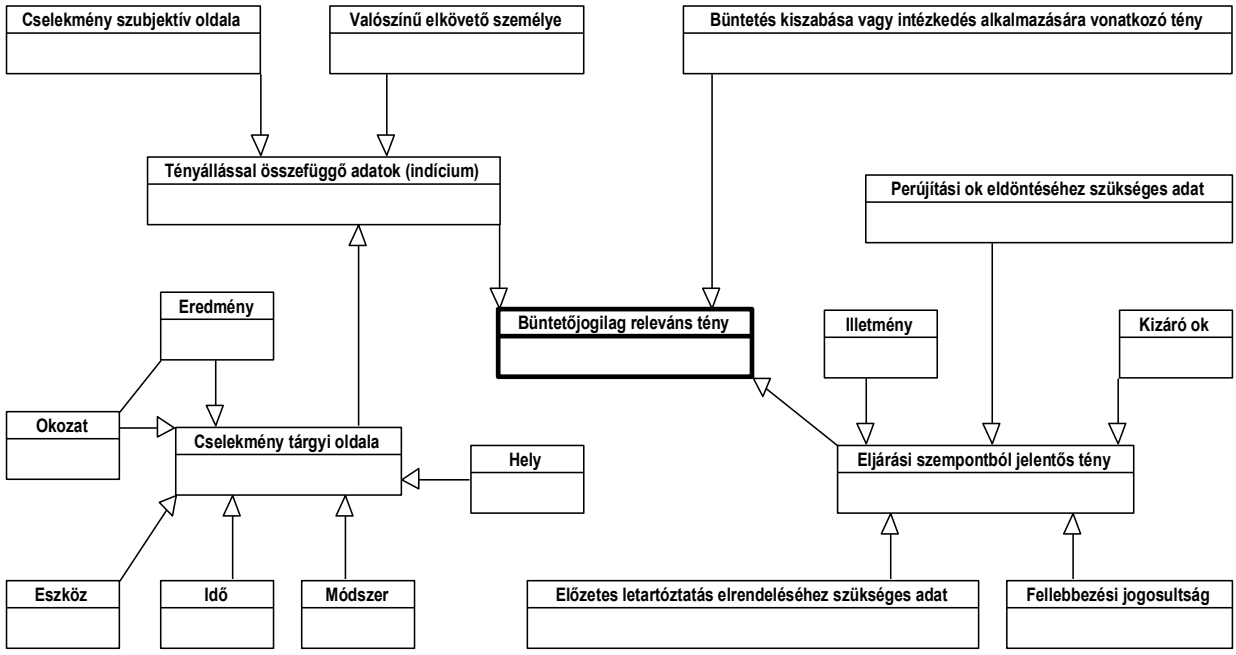
A büntetőeljárásban a bizonyítékok „*olyan adatok,*

a) amelyek büntetőjogilag releváns tényekre vonatkoznak;

b) amelyeket a törvény által megengedett forrásokból szereznek be,

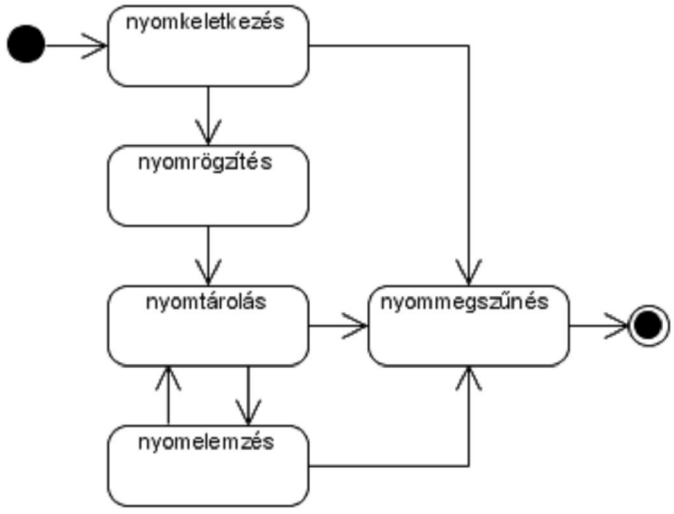
s éppen ezért összességükben és összefüggésükben felhasználhatók (alkalmasak) a büntetőjogilag releváns tényállásnak az ügydöntő hatóság általi megállapítására, utólagos rekonstrukciójára (eljárásjogi bizonyíték)” {[1] p79.}

A bizonyíték, tehát büntetőjogilag releváns tény, amelynek a „csontváz” osztálydiagramját a következő ábra tartalmazza:



2. ábra. Büntetőjogilag releváns tények
([7] alapján szerk.: Illési Zsolt)

A bizonyítékok nem statikusak, hanem sajátos életciklusuk van: megszületnek-vannak-eltűnnek. A bizonyítékok lehetséges állapotváltozásait az alábbi ábra mutatja be:



3. ábra. A nyom állapotváltozásai: a nyomok „életciklusa”
(szerk.: Illési Zsolt)

Az ábrából kitűnik, hogy a nyomok a keletkezésüket követően, ha nem fedezik fel őket az eljáró hatóságok vagy nem tárják fel az érintettek – a kriminalisztikus szemszögéből nézve – anélkül is megszűnhetnek, hogy értékelésére sor került volna, illetve az általa a tényállással kapcsolatban hordozott információtartalmat értékelték volna.

Az ábra alapján látható egy másik sajátos állapotváltozás is, ha a nyomelemzés során

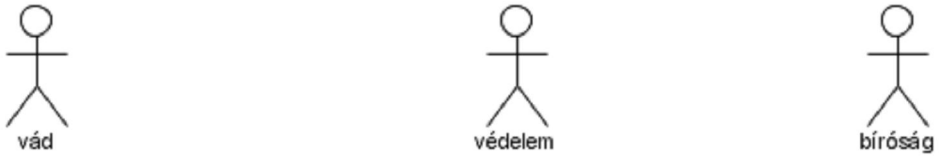
szűnik meg a nyom. Erre általában roncsolásos vizsgálatok során kerül sor, illetve informatikai eszközök esetén például a merevlemezen található hibák javításával elvész a hibajavítás előtti „bizonytalan”, hibás állapot.

A nyomok kezelésének természetesen a „normál” menete az, ha a nyomot az eljáró hatóságok felfedezik, rögzítik, elemzik és az elemzést követően, ha a szükséges törvényi feltételek fennállnak (pl. a pert jogerősen elbírálta a bíróság) majd megsemmisítik, illetve adat-bizonyíték esetén az adathordozót megfelelő módon – visszaállíthatatlanul – törlik.

A büntetőeljárás szereplői

Miután sikerült modellezni, hogy milyen eljárás során mivel kell foglalkozni, felmerül annak a kérdése, hogy ki is végez informatikai szakértői feladatokat.

A modellezés kiindulópontjául először a klasszikus vád-védelem-bíróság triászból próbáltam kiindulni, de hamar be kellett látnom, hogy ebbe a hármas-alapú modellbe a szakértő nem helyezhető el (ha másért nem a Be-ben meghatározott kizárások miatt).



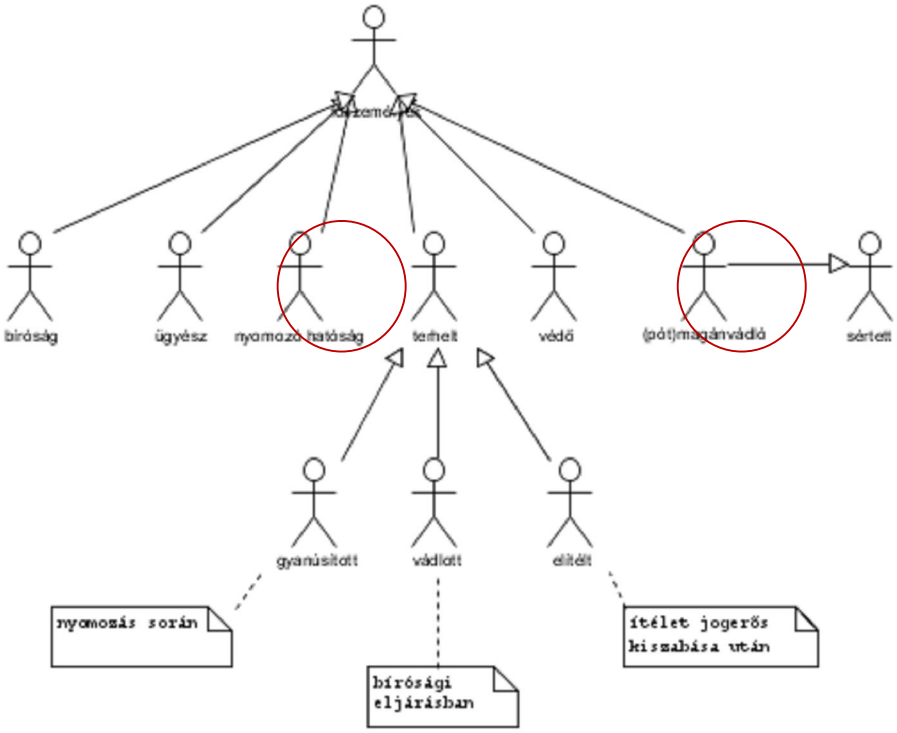
4. ábra. A Be. szereplői (1): Általános modell
([7] alapján szerk.: Illési Zsolt)

A következő megközelítés alapja a Be-ben betöltött szerep elsődlegessége, ez alapján a következő modell rajzolható fel:



5. ábra. A Be. szereplői (2): Szakértőket is tartalmazó modell
([7] alapján szerk.: Illési Zsolt)

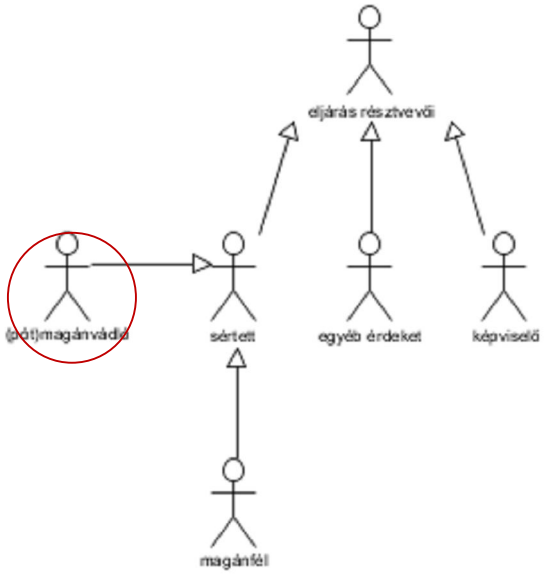
Az egyes személyek kibontásával a fő személyekre a következő modell adódik:



6. ábra. A Be. szereplői (3): Főszemélyek
([7] alapján szerk.: Illési Zsolt)

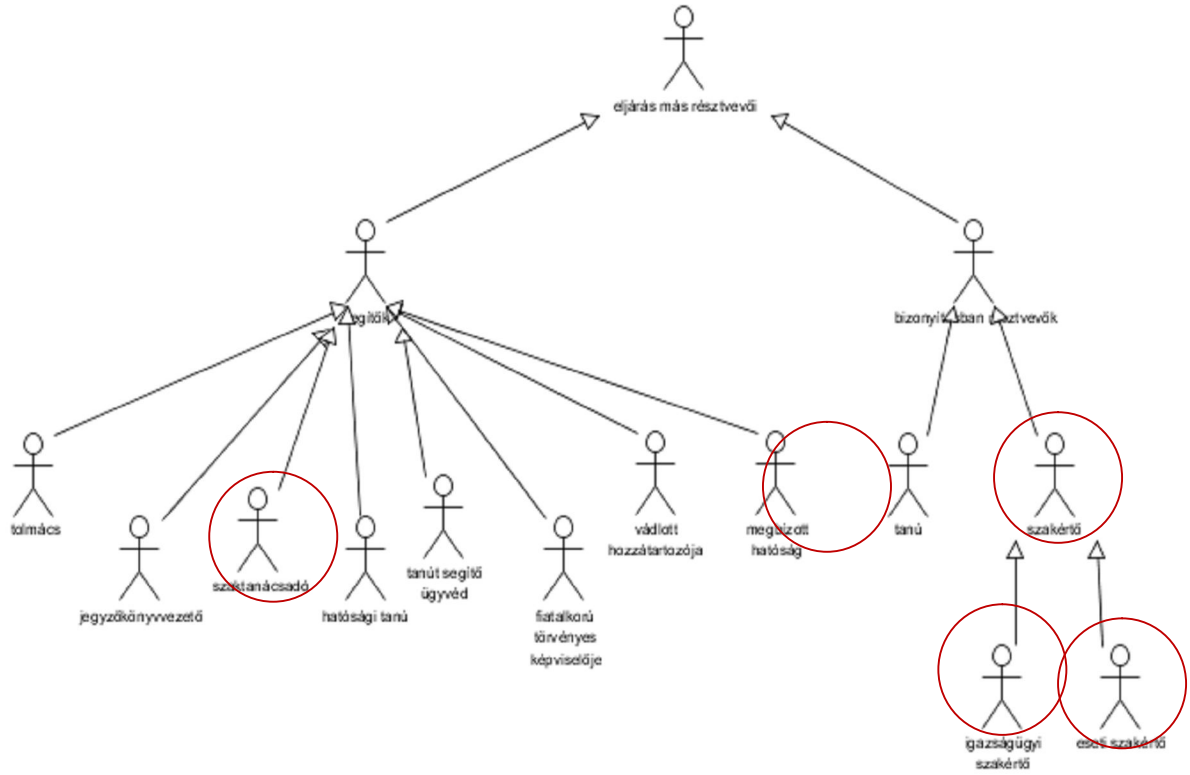
A főszemélyek funkcióinak vizsgálatával megállapítható, hogy informatikai szakértői feladatokat a nyomozóhatóság és a pótmagánvádló szerepkört betöltő személyek játszhatnak.

Az eljárás személyeinek elemzésével a következő modellt állítottam elő:



7. ábra. A Be. szereplői (4): Az eljárás résztvevői
([7] alapján szerk.: Illési Zsolt)

Ezek közül a szereplők közül csak a sértett speciális esetben (pótmagánvádlóként) végez informatikai szakértés jellegű feladatokat.



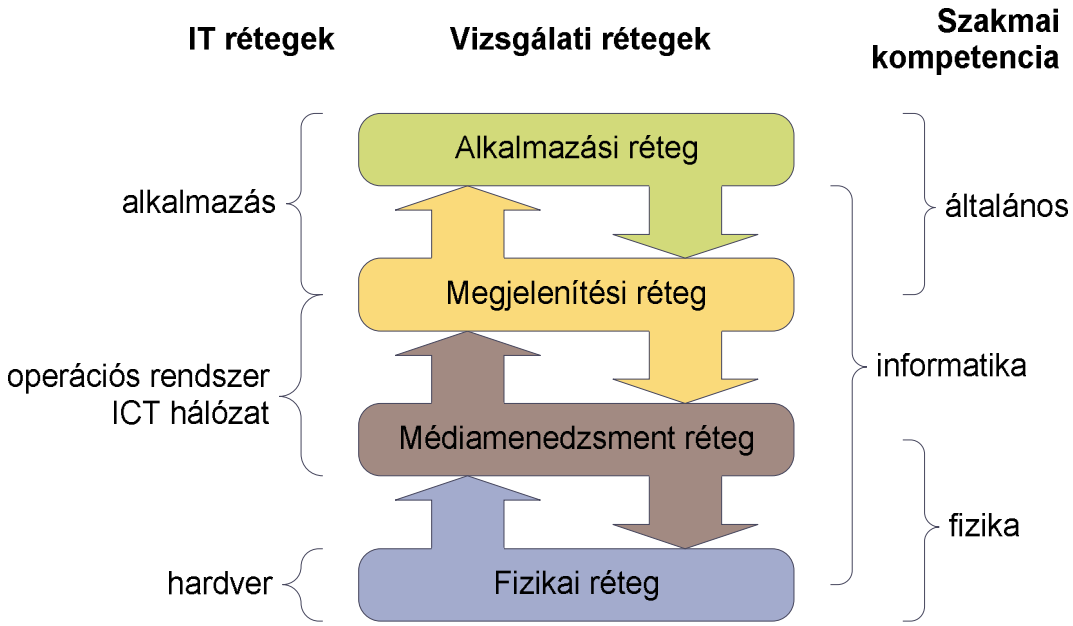
8. ábra. A Be. szereplői (5): Az eljárás más résztvevői
([7] alapján szerk.: Illési Zsolt)

Az eljárás más résztvevőinek funkcióelemzése során már több olyan szakértői tevékenységet betöltő személyt találunk, akiket szakértőként nevesít a Be. Ezek a szakértők az igazságügyi szakértő, az eseti szakértő és a szaktanácsadó. Ezek mellett informatikai szakértői tevékenységet láthat el a megbízott hatóság is, amennyiben informatikai, hírközlési kérdésekben áll a bíróságok vagy a nyomozóhatóság számára.

A fenti modellek jól érzékeltetik, hogy nem csak egy szakértői (vagy a szakértéssel összefüggő, szakértői jellegű) tevékenységet végző szerepkörű résztvevője van a büntetőeljárásnak, hanem több egymástól elkülönült személy vagy hatóság is végez ilyen feladatokat. (Viszont csak az igazságügyi szakértőkkel szemben támaszt szakmai és egyéb szakmai-jellegű garanciális feltételeket a hatályos jog; így nem követeli meg a többi szereplőtől a szakirányú végzettséget, szakmai gyakorlatot, nincs kötelező kamarai tagságuk sem és nem vagy csak részben köti őket szakmai munkavégzés „kényszere”.)

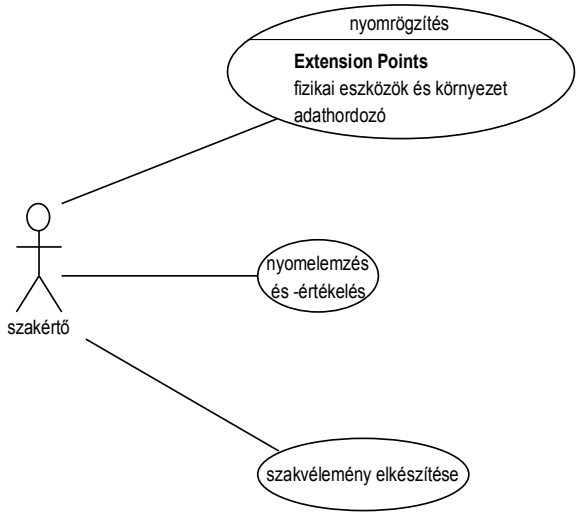
Az informatikai vizsgálatok rétegei

Az informatikai szakértői vizsgálatok összefoglalását Brian Carrier modellje az általam tett kiegészítésekkel mutatja be:



9. ábra. Informatikai rendszerek vizsgálati rétegei
([8] alapján szerk.: Illési Zsolt)[9]

A modell alapján felrajzolható az informatikai szakértés általános használati esetdiagramja a következők szerint:

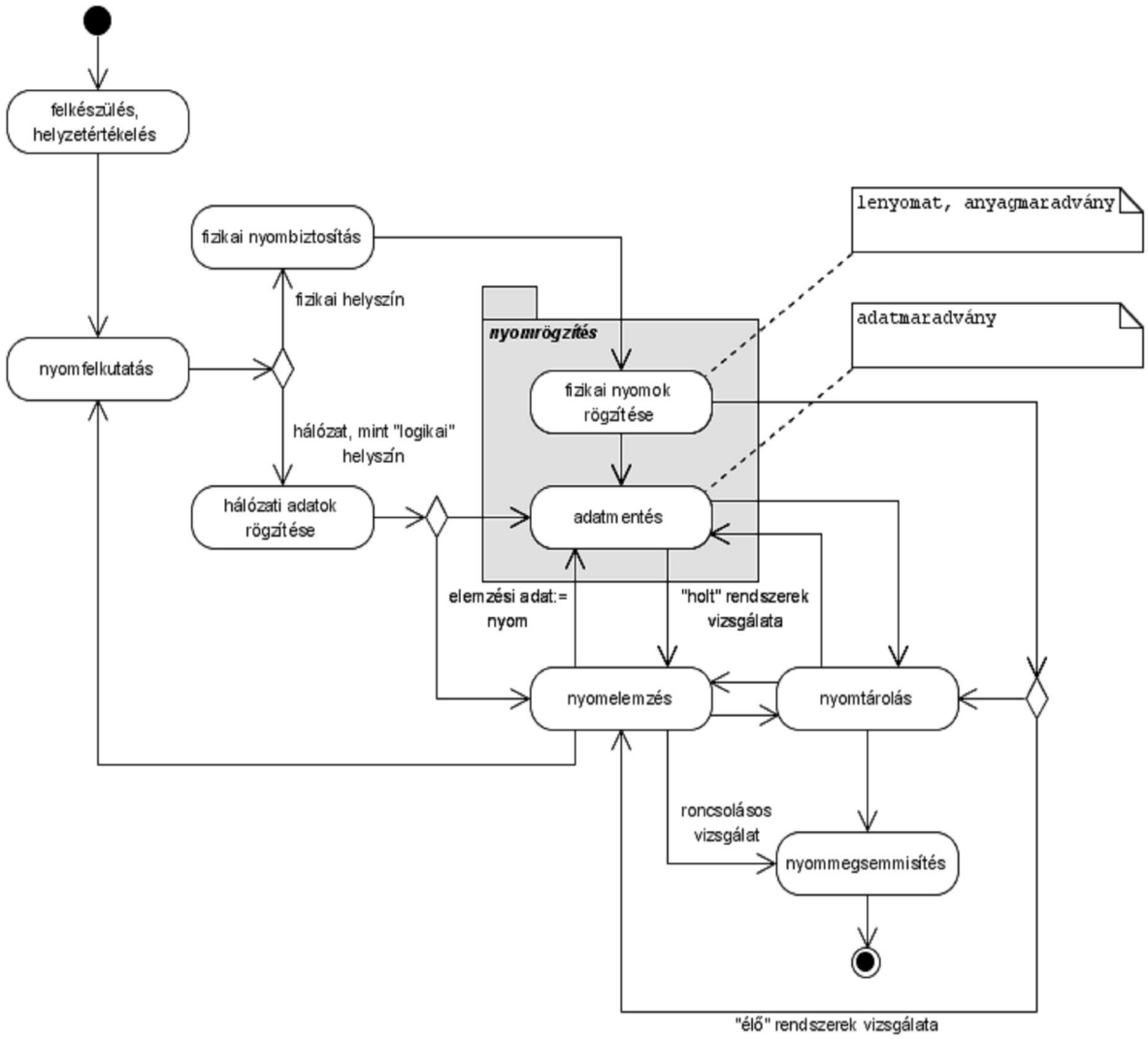


10. ábra. Informatikai szakértés általános feladatai
(szerk.: Illési Zsolt)

A használati eset modell kiegészítéseként meg kell jegyeznem, hogy a nyomrögzítés kapcsolódik a fizikai réteghez, a nyomelemzés és értékelés pedig együttesen a médiamenedzsment, a megjelenítési és az alkalmazási réteghez. A nyomelemzés és- értékelés sajnos olyan szerteágazó feladat, hogy ennek az elemzésére ebben a cikkben nem

vállalkozom.

A nyomrögzítés egy olyan összetett tevékenység (talán helyszíni tevékenységnek is nevezhetném), amely során az eljáró hatóság és szaktanácsadó (esetleg szakértő) felkészülnek a fizikai és digitális nyomok rögzítésére, biztosítására, rögzítésére és elemzésére az alábbiak szerint:



11. ábra. Digitális nyomfelkutatás, -rögzítés, -biztosítás
(szerk.: Illési Zsolt)

A nyomelemzés feladat ebben a modellrészletben – bár valamennyi elemzési és -értékelési feladat elképzelhető a tevékenység során – azokra az elemzési tevékenységekre szűkítve értelmezendő, amelyek további nyomok kereséséhez szükségesek.

ÖSSZEFOGLALÁS

Jelen írásban példákon keresztül bemutattam, hogy hogyan lehetséges az informatikai (igazságügyi) szakértés, illetve valamennyi szakértői feladat modellezése, a modellezés egyre részletesebb és alaposabb kifejtésével pedig lehetséges a szakértői tevékenység modellezése.

A modelleken keresztül felépíthető a szakértői résztevékenységeket leíró módszertani levél.

Az általam elkészített modellek nagy része nem csak a saját szűk szakmai területemre az informatikai igazságügyi szakértésre, hanem valamennyi igazságügyi szakértésre, sőt a büntetőeljárásban szakértői tevékenységet ellátó egyéb szereplők tevékenységeinek a modellezésére is alkalmas. Úgy vélem, hogy például a nyom állapotdiagramja kellő kiindulópontja lehet valamennyi kriminál technikai vizsgálatnak, módszertannak.

Az elemzéseimből kiderült, hogy szükséges lenne szakértői módszertani levél elkészítése, kiadása és használata, mivel így jelentősen növelni lehetne az igazságügyi szakértés és a kapcsolódó szakértői és szakértő jellegű feladatok minőségét, a kirendelő hatóságok számára olyan sillabuszt jelenthetne, amelyre alapozva „jó" kérdéseket tennének fel, hogy „jó" válaszokat kaphassanak. Sajnos az elemzésem alapján az is megállapítható, hogy a MISZ és a minisztériumok mulasztásos törvénysértésben vannak azzal, hogy nem születtek meg és nem lettek publikálva a módszertani levelek.

A fentiek mellett el kell ismerni azt is, hogy a jogszabály csak terheket ró a MISZK-re, de nem biztosítja a feladat végrehajtásához szükséges erőforrásokat. Nincs anyagi forrás, nincs tudományos kutatási pályázat, nincs eszközbeszerzési pályázat, amit a MISZK igénybe tudna venni módszertani fejlesztésekhez. Márpedig a minőségi munka pénzbe kerül, a fejlesztésekhez szükséges megfelelő kutatói-módszertani bázis létrehozása a hazai felsőoktatási intézményekben. Sajnos az igazságügyi szakértői intézetek jelenleg nem alkalmasak az informatikai szakértés módszertani bázisa szerepének betöltésére, mivel jelenleg csak egy, a Igazságügyi Szakértői és Kutató Intézetek Veszprémi Intézete, foglalkozik informatikai jellegű szakkérdésekkel, de ott is csak egy munkatárs kompetenciájára alapozva.

(Egyébként az egyéni szakértők többségének számára[1] sem megoldott az életvitel szerű munkavégzés; egyedül vagy kis cégekbe tagoltan végzik a munkájukat, nem áll rendelkezésükre pályázati pénz a szakértői eszközök beszerzéséhez, a hatóságok nem fizetik ki őket a törvényes határidőn belül[2].)

Véleményem szerint a szakértés modellezése utat nyitna az összehasonlító elemzéseknek, összehasonlíthatóvá tenné az egyes (EU tag)országok (igazságügyi) szakértői rendszereit és feladatait, rávilágítana a hazai rendszer sajátosságaira (pl. sem a MISZK sem pedig a tagjai nem részei a „law enforcement"-nek, a törvények végrehajtásának, így nem kapcsolódhatnak közvetlenül a hasonló feladatokat ellátó nemzetközi szervezetekhez, nem vehetnek igénybe kapcsolódó kedvezményeket, nem jogosultak hardver és szoftver kedvezményekre sem).

A modellek véglegesítése, kifejtése lehetővé tenné igazságügyi szakértői szoftverek (pl. szakértői keretrendszerek, folyamatmenedzsment/workflow rendszerek) kifejlesztését, hiszen az UML modellek mögött, azokkal egy időben elkészül egy pszeudo-kód, mi gyor fejlesztést tesz lehetővé.

[1] Speciális kivétel például az orvos szakértőké, ahol a szakértő munkahelye biztosítja – ingyen (?) – a szakértői díjon felüli „havi rendszeres fizetést", a vizsgálati eszközparkot; a továbbképzések a szakmai továbbképzés része; ezen a szakterületen rendelkezésre állnak egészségügyi kutatási-fejlesztési pályázatok, van egyetemi képzés és továbbképzés.

[2] Ld. http://www.mr1-kossuth.hu/hirek/itthon/meg-iden-kifizeti-adossagait-a-rendorseg.html

Irodalomjegyzék

[1] Tremmel Flórián: Bizonyítékok a büntetőeljárásban, Dialóg Campus, Budapest-Pécs, 2006.

[2] Az igazságügyi szakértői kamaráról szóló 1995. évi CXIV. törvény (Iszktv.)

[3] Az igazságügyi szakértői tevékenységről szóló 2005. évi XLVII. törvény (Szaktv.)

[4] 1998. évi XIX. törvény a büntetőeljárásról (Be.)

[5] Tremmel Flórián – Fenyvesi Csaba: Kriminalisztika tankönyv és atlasz, Dialóg Campus Kiadó, Budapest-Pécs, 2002.

[6] Illési Zsolt: Krimináltechnika szerepe az informatikai védelem területén, Hadmérnök, IV. Évfolyam 1. szám – 2009. március 170 183.p. ISSN 1788-1919

[7] Király Tibor: Büntetőeljárási jog, Osiris Kiadó, Budapest, 2008.

[8] Brian Carrier: Defining Forensic Examination and Analysis Tools Using Abstraction Layers, International Journal of Digital Evidence, 2003. Volume 1 Issue 4., Economic Crime Institute (ECI) at Utica College, USA, 2003.

[9] Illési Zsolt: Számítógép hálózatok krimináltechnikai vizsgálata, Hadmérnök, IV. Évfolyam 4. szám – 2009. december 163 175.p.

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Kassai Károly
kassai.karoly@hm.gov.hu

AZ ELEKTRONIKUS ADATKEZELŐ KÉPESSÉGEK MŰKÖDÉSFOLYTONOSSÁGÁVAL KAPCSOLATOS ÁLTALÁNOS FELADATOK

Absztrakt

A honvédelmi szervezetek működése napjainkban nem képzelhető el elektronikus adatkezelő képességek nélkül. Az ezt megvalósító eszközök, rendszerek, szolgáltatások egyre fontosabb szerepet játszanak, így kiemelt figyelmet érdemel rendelkezésre állásuk kérdése. Nem elégséges csak egy eszköz, rendszer beszerzésére koncentrálni, mert a hardver és szoftvertámogatás vagy a karbantartás hiánya a teljes életciklusra vetítve hiányosságokat és problémákat okozhat az üzemeltetés során. A meghatározott szinten történő üzemeltetés támogatás kihívásokat jelent a katonai üzemeltetési környezet, valamint az ezzel kapcsolatos információs fenyegetések és sebezhetőségek miatt.
A cikk az elektronikus adatkezelő szolgáltatások folytonos működésre vonatkozó feladatrendszerét vizsgálja. Támpontokat ajánl a híradó és informatikai rendszerek tervező, üzemeltető szerveinek, biztonsági menedzsmenteknek az elektronikus adatkezelés előre meghatározott szolgáltatási szinten történő biztosítása érdekében.

Nowadays the activity of military organisations unimaginable without electronic information handling capabilities. The communication equipments, systems have more and more importance so the availability aspect of these supporting capabilities requires focus point of view. The focus is not only on acquisition of equipments or systems because lack of hardware and software upgrading and maintenance during all life cycle can cause deficiencies and problems in service.
The agreed level service support has some challenges because of specific military environment, information threats and vulnerabilities. This article observes the business continuity framework of CIS and offers milestones to the planning, operating authorities and security managements for the agreed level electronic information handling capabilities.

Kulcsszavak: *biztonságpolitika, információbiztonság, információvédelem, rendelkezésre állás, működésfolytonosság ~ security policy, information security, information protection, availability, business continuity*

BEVEZETÉS

Az elektronikus adatkezelő képességek biztonságára vonatkozóan hazánkban átfogó jellegű, a közigazgatásra érvényes – így a Magyar Honvédségnél is kötelező jellegű – követelmény nem azonosítható. Az elektronikus információbiztonság hármas célkitűzésén belül (bizalmasság, sértetlenség, rendelkezésre állás) az adatokra és adatkezelő képességekre egyaránt értelmezhető sértetlenség és rendelkezésre állás követelményei jogszabályokban még pontosan nem azonosítottak.

A minősített adatkezelésre vonatkozó jogszabályok közvetlenül nem határoznak meg a szolgáltatások fenntartására irányuló biztonsági követelményeket, csak azt rögzítik, hogy *a hagyományos (papír alapú), vagy elektronikus adatkezelést helyi, illetve rendszer-specifikusan kell szabályozni*, melynek részleteit az adatkezelésért felelős vezetőnek kell meghatároznia [1.][2.].

Az iratkezelésre vonatkozó jogszabály az elektronikus iratkezelésre vonatkozóan rendelkezésre álláshoz köthető feladatokat nem tartalmaz, csak azt rögzíti, hogy az üzemeltetésre vonatkozó követelményeket az iratkezelő szerv vezetőjének kell meghatároznia [3.].

Az elektronikus közszolgáltatás biztonságát szabályozó jogszabályban a központi szolgáltató rendszerrel kapcsolatban a folytonos üzemeltetést célzó követelmények gyakorlatilag a katasztrófa elhárításra vonatkozó eljárásrendben nyilvánulnak meg, így ez a szabályozó sem tartalmaz alkalmazható eljárásrendet [4.].

A fentiek alapján megállapítható, hogy *jogszabály nem tartalmaz olyan követelményeket vagy módszertani segítséget, ami támpontot nyújtana az elektronikus adatkezelő képességek folytonos üzemeltetésének biztosítását célzó eljárások kialakításához.*

A Magyar Köztársaság Katonai Stratégiája szerint a Magyar Köztársaság biztonsági környezetében *biztonsági kockázatot jelenthetnek a kritikus infrastruktúra elleni támadások.*
A védelempolitika alapja, hogy a honvédelem – benne a katonai erő – legyen képes mind a Magyar Köztársaság védelmét, mind a külföldi műveletekben való részvételt a *hagyományos és az aszimmetrikus hadviselés viszonyai között egyaránt teljesíteni, melybe egyértelműen beleértendő az információs fenyegetések és a sebezhetőség kérdésének kezelése*.

A magyar haderővel szemben állított követelmények között szerepel az *erők védelme és megóvása*, a *hálózatközpontú környezetben való alkalmazás képessége*, a hatékony felderítés, *az információszerzés és –csere*, a telepíthetőség, mobilitás, a hosszú távú fenntarthatóság, mely kitűzések az elektronikus adatkezelő rendszerek (képességek) *szükséges mértékű rendelkezésre állásának biztosítása nélkül nem képzelhetők el* [5.].

A Stratégia általánosan megfogalmazott követelményeinek végrehajtását célzó miniszteri feladat meghatározásban az információbiztonsági követelmények mellett a rendelkezésre állás, az üzemeltetés folyamatos biztosítása is megjelenik, de a dokumentum jellegéből adódóan csak általános irányokat tűz ki, és nem határoz meg részterületi feladatokat [6.].

A honvédelmi tárcánál a fentiek mellett az *elektronikus adatkezelő képességek szolgáltatásainak folytonosságára specializált, általánosan alkalmazható, korszerű követelmény nincs kialakítva,* csak rendszerekhez kapcsolódó rendszabályok azonosíthatók.

A katonai szervezetek működéséhez nélkülözhetetlen elektronikus adatkezelő képességekre irányuló fenyegetések és a sebezhetőségek *nem csak a katasztrófa jellegű szolgáltatás megszűnés, hanem a szolgáltatás csökkenés vagy kiesés rendszer-specifikusan sokszínű formájában is jelentkezhetnek.* Emiatt a nemzetközi gyakorlattal összhangban *célszerűnek látszik szervezeti működés folytonosságához (nemzetközi szakirodalom és szabványok megfogalmazása szerint üzletmenet folytonossághoz) szükséges üzemeltetés támogatási kérdések vizsgálata,* az ezzel kapcsolatos alapvető eljárások megfogalmazása *a rendszer-specifikus védelmi rendszabályok kialakításának támogatása érdekében.*

A kialakítandó eljárásokhoz támpontot adhatnak a menedzsment szemléletű általános ajánlások [7.][8.][9.][10.]. Ezen túlmenően kiegészítésként célszerű a nemzetközi szabványok figyelembe vétele a katonai működési sajátosságok szerinti specializálás, valamint a NATO, EU minősített elektronikus adatkezelésre vonatkozó követelmények teljesítése érdekében [11.][12.][13.][14.][15.].

A cikk a honvédelmi szervezetek működésének folytonosságához szükséges IT szolgáltatások szervezet és rendszer-specifikus sajátosságok nélküli, keretrendszerű, általános követelményeinek kialakítását célozza (így nem feladat a tervezés és üzemeltetés körébe tartozóan a rendszerek hibatűrésére, redundanciájára vonatkozó követelmények, irányelvek meghatározása). *Az adott szervezet működéséhez szükséges képességek folytonosságát biztosító rendszabályok ezen általános követelmények alapján pontosíthatók.*

1. CÉLKITŰZÉSEK

A honvédelmi szervezetek működés-megszakadásának elhárítására irányuló tevékenységébe integrálva a kritikus folyamatokat védeni kell az információs rendszerek nagy hibáinak, vagy üzemzavarainak hatásaitól. A bekövetkezett negatív események hatásait mielőbb ki kell küszöbölni, és biztosítani kell a szolgáltatások kellő időben történő újrakezdését.

A szervezeti működésfolytonosság irányítási folyamatába olyan megelőző és helyreállító intézkedéseket kell bedolgozni, melyek az információs szolgáltatások szándékos vagy véletlen okból bekövetkezett kiesése esetén biztosítják a szervezetre gyakorolt hatás csökkentését.

Az üzemzavarok, meghibásodások, szolgáltatás elvesztés, biztonsági incidensek, illetve az információs szolgáltatások rendelkezésre állásra vonatkozó követelményeit működési hatáselemzéssel (business impact analysis; BIA) kell vizsgálni. A hatáselemzés alapján működésfolytonossági terveket kell kialakítani és bevezetni.

2. AZ INFORMÁCIÓBIZTONSÁG MŰKÖDÉSFOLYTONOSSÁGBA TÖRTÉNŐ INTEGRÁLÁSA

A honvédelmi szervezetek működésének folytonosságára irányuló vezetői, szervezési és szervezeti feladatok közé be kell sorolni azokat a felelősségeket, folyamatokat és feladatokat, amelyek biztosítják az adatkezelő képességek működésfolytonosságának támogatását. Az ehhez szükséges feladatok a következők:

1) a kritikus működési folyamatok azonosítása, az elsőbbségi sorrend megállapítása, valamint az ezekkel kapcsolatos szervezeti kockázatok azonosítása;
2) a kritikus működési folyamatokhoz szükséges információs szolgáltatások, az ehhez szükséges képességek azonosítása;

3) az információbiztonsági incidensek hatásainak azonosítása;
4) az esetleges biztosítási lehetőségek azonosítása;
5) a megelőző, illetve a negatív hatásokat mérséklő rendszabályok azonosítása;
6) a szükséges pénzügyi, szervezeti, technikai erőforrások azonosítása;
7) működésfolytonossági terv kidolgozása;
8) a működésfolytonossági terv felülvizsgálatának és naprakészségének biztosítása.

A fentiek alapján látható, hogy a hadműveleti (alkalmazói) követelmények hiányában, illetve csak úgy általánosságban nem hozható döntés annak meghatározására, hogy egy-egy esetben szükség van-e a működésfolytonossági kérdések vizsgálatára, vagy elégséges a napi üzemeltetés körébe tartozó fenntartási és javítási kapacitások alkalmazása. Amennyiben ezzel a kérdéssel foglalkozni kell, *a működésfolytonossági tervet be kell építeni a szervezeti folyamatokba és a működésfolytonossági folyamatokért való felelősséget megfelelő szervezeti elemekhez kell hozzárendelni*.

A szervezeti folyamatokba történő integrálás kulcskérdése annak felismerése és helyes kezelése, hogy *az IT képességekre vonatkozó működésfolytonosság követelményeinek meghatározása nem az informatikai vagy híradó szakterület feladata*. A szervezetek alapító okiratában, működési szabályzatában meghatározott feladatok tűrésen belüli kiesésének biztosításához szükséges *minimum adatkezelő igények felmérése, meghatározása és a tartalék megoldásokra vonatkozó lehetőségek feltárása összetett szervezeti feladat.*

3. A MŰKÖDÉSFOLYTONOSSÁG KOCKÁZATELEMZÉSSEL TÖRTÉNŐ TÁMOGATÁSA

A szervezeti szintű vizsgálat eredményeképpen az elektronikus adatkezelő rendszerekre irányuló kockázatelemzés és menedzselés a következő lépcső, ami segít a feladatok azonosításában és kidolgozásában. A kockázatok azonosításnak és felmérésének legjobb támogatása a meglévő szolgáltatások ismerete (service catalogue) és felügyelete a tipikus megfogalmazású „írjátok össze, hogy mink van, és mire lenne szükség” megközelítés helyett.

A feladat megoldását segíti a meglévő folyamatok monitorozása és a szolgáltatások rendelkezésre állásának naplózása. Az üzemeltetés során meg kell őrizni az üzemeltetésre vonatkozó adatokat, összehasonlításokat kell végeznie az IT szolgáltatásokra vonatkozó követelményekkel, és ki kell mutatni a hiányosságokat. Dokumentálni kell és ki kell vizsgálni a nem megfelelőséget (részleges vagy teljes kiesések, hibás működés), valamint lehetőség szerint előre kell jelezni a jövőben várható, a rendelkezésre állásra vonatkozó egyedi csúcsterheléseket (adatkezelési vagy feldolgozási határidők, gyakorlatok, rendezvények), vagy fejlesztési igényeket (létszámnövekedés vagy új alkalmazások által történő kapacitásbővítési szükséglet). Ahol lehetséges, előre kell jelezni a várható trendeket, kapacitás igényeket és megelőző jellegű tevékenységet kell végezni a sokkoló hatások elkerülése érdekében.

A kockázatelemzés során megtörténik az elektronikus adatkezelő képességek működéséhez szükséges elemek, üzemeltetési környezet, valamint az üzemeltetéshez szükséges humán és szervezeti feltételek azonosítása. Ennek során meg kell határozni a megszakadások valószínűségét és időbeli hatását, az okozott kár mértékét és a helyreállításhoz szükséges időt, valamint:
1) a megszakítástól kezdve a maximális időkiesést, mely még megengedhető;
2) a kiesés alatti minimális szolgáltatási szintet;
3) azt a határidőt, melyre a normál szolgáltatást helyre kell állítani.

Fel kell tárni a kulcsfontosságú tevékenységek szempontjából lényeges függőségeket, beleértve a beszállítókat, szolgáltatókat és külső partnereket, és azonosítani kell azon beszállító és együttműködő szervezeteket, akiktől a kritikus tevékenységek függenek, illetve azon szolgáltatásokat, melyeket ezen szervezetek biztosítanak.

A működésfolytonosság kockázatának felmérése során a működési források és folyamatok tulajdonosait teljes körűen be kell vonni. A különböző kockázati szempontokat össze kell kapcsolni, hogy a szervezet működésfolytonossági követelményeiről teljes kép alakuljon ki (a gyakorlatban is figyelembe kell venni az ok-okozati összefüggéseket, mert az áramszünet, csőtörés, épületgépészeti meghibásodás, vagy vegyi katasztrófa nem mindig tiszta esetként jelentkezik).

A felmérés azonosítsa, számszerűsítse és sorolja be a kockázatokat a szervezetre vonatkozó kritériumok és célok szerint, beleértve a kritikus erőforrásokat, a megszakadás hatásait, a megengedhető kiesési időket és a helyreállítási elsőbbségeket.

A kockázatfelmérés eredményére alapozva ki kell dolgozni a folyamatos működés biztosítását célzó feladatokat, és a tervet jóvá kell hagyatni.

Összetett elektronikus adatkezelő képességek, bonyolult szervezeti folyamatok esetén a terv készítése is erőforrás igényes, hosszú feladat. Ebben az esetben először működésfolytonossági stratégiát kell kialakítani az átfogó közelítés meghatározása érdekében. A stratégiát jóvá kell hagyatni és meg kell benne határozni a folyamatos működés biztosítását célzó terv (tervek) kialakítására, jóváhagyására, felülvizsgálatára vonatkozó követelményeket.

4. A MŰKÖDÉSFOLYTONOSSÁGI TERVEK KIDOLGOZÁSA ÉS MEGVALÓSÍTÁSA

A működésfolytonossági tervezés célja a meghatározott szintű működés biztosítása (a minimális szintű munkavégzéséhez szükséges szolgáltatások helyreállítása), így az egyéb feladatokat (a fenntartási feladatokhoz tartozó általános javítási feladatokat) külön kell tervezni és végrehajtani.

A honvédelmi szervezetnél rögzíteni kell, hogy az incidensek megoldását milyen tevékenységekkel kell megoldani, és hogyan lehet egy előre meghatározott szintre helyreállítani (és fenntartani) a megszakítás által okozott szolgáltatásokat. A tervnek:

1) meghatározott cél és hatáskört kell szolgálnia;
2) elérhetőnek kell lenni minden olyan személy számára, akinek használnia kell azt;
3) azonosítania kell a felülvizsgálatért, naprakészségért és jóváhagyásért felelős személyeket;
4) szabályoznia kell az incidens ideje alatt a külső szervezetekkel kapcsolatos eljárásokat.

A tervezés során:

1) azonosítani kell minden felelősséget és működésfolytonossági eljárást és azokat egyeztetni kell a szükséges együttműködő partnerekkel;
2) azonosítani kell az elfogadható információ- és szolgáltatásvesztést;
3) azonosítani kell a szükséges szolgáltatásokat és erőforrásokat, beleértve a személyzettel való ellátást, az egyéb szükséges szolgáltatásokat (pl. szállítás, helyigény, valamint a tartalék adatfeldolgozó eszközökre vonatkozó intézkedések);
4) eljárásokat kell bevezetni az üzemeltetés határidőre történő helyreállása, visszaállítása, érdekében;

5) eljárásokat kell kialakítani a helyreállítás függőben lévő befejezésének követésére;
6) meg kell határozni az egyeztetett eljárások és folyamatok dokumentálási feladatait;
7) meg kell határozni a helyreállítással kapcsolatos képzési feladatokat, beleértve a menetközben előforduló, előre nem várt események kezelésének fogásait is;
8) meg kell határozni a tervek felülvizsgálatának és pontosításának rendjét.

A működésfolytonossági tervek, dokumentumok, és a feladatok végrehajtásához szükséges anyagok tárolásakor fő szempont, hogy azok *mentesüljenek a fő helyszínen (telephelyen) bekövetkező üzemzavar miatti károsodás alól*.

A tartalék, és egyéb másodlagos üzemeltetési helyszíneken a védelmi rendszabályoknak az elsődleges üzemeltetési környezet szintjén kell lennie. A működésfolytonossági terveknek tartalmaznia kell:

1) a riasztáshoz és a helyzet megoldáshoz szükséges kommunikációs kapcsolatokat;
2) a feladatokat, és a végrehajtásukhoz szükséges támogató információkat;
3) a meghatározott személyek, szervezeti elemek felelősségét, feladatait a helyzet megoldása során, és azt követően;
4) a tervek aktivizálására vonatkozó felhatalmazást, valamint az eseteket, amikor azokat hatályba kell léptetni;
5) a tervek aktivizálásának módszerét;
6) a találkozási helyeket (és tartalékaikat), a naprakész elérhetőségi adatokat és a más szervezetek mozgósításhoz szükséges információkat;
7) azokat a folyamatokat, melyek az incidensek megoldását szolgálják;
8) a kapcsolatokat minden fontos személyhez, akiknek felelőssége, feladata lehet a helyzet megoldásában;
9) a kieséssel kapcsolatos azonnali teendőket:
   a) stratégiai és üzemeltetési változatokat a kiesés megoldására;
   b) a további szolgáltatás kiesések, vagy a rendelkezésre állás megszűnésének megakadályozására irányuló feladatokat;
10) az incidens megoldására vonatkozó tevékenységeket:
   a) a kritikus időszak alatti szolgáltatások;
   b) a helyreállításra irányuló tevékenységek;
11) a végrehajtás végző személyek magánkommunikációjára és az együttműködő szervezetekkel való kapcsolattartásra vonatkozó megoldásokat;
12) a média kommunikációval kapcsolatos feladatokat;
13) az incidensre, a végzett feladatokra és döntésekre vonatkozó fontos adatok rögzítésére vonatkozó eljárásokat;
14) az elvégzendő részletes feladatokat;
15) a működésfolytonossághoz és a helyreállításhoz szükséges erőforrásokat;
16) a kritikus tevékenységekhez rendelt helyreállítási sorrendet, szolgáltatási szinteket és határidőket.

A működésfolytonosságot biztosító tervnek, illetve a végrehajtását támogató dokumentumoknak, segédanyagoknak *gyakorlatban használható, pontosan kidolgozott üzemeltetési dokumentumoknak kell lenniük*. A bennük megfogalmazott műveletekre vonatkozó *biztonsági követelményeket és védelmi rendszabályokat az elektronikus adatkezelő képességek biztonsági dokumentumaiban kell megfogalmazni és jóváhagyatni*. Ez mutatja *az üzemeltetési és a biztonsági dokumentumok szoros kapcsolatát és összehangolásuk szükségességét*.

Önmagában a helyreállítási tevékenység tervezése és gyakorlása nem elégséges a helyzetek kezelésére. *A fenntartáshoz szükséges javító és karbantartó anyagok tervezése, beszerzése, készletezése, szétosztása és pótlása nélkül a folyamatos üzemeltetés nem képzelhető el.*

Ugyanígy szükség van a kritikus infrastruktúra körbe tartozó kritikus információs infrastruktúra elemek azonosítására és erre vonatkoztatva fontossági sorrend szerint helyreállítási és készletezési eljárások kialakítására és fenntartására. Abban az esetben, amikor nem lehetséges megfelelő mennyiségű tartalék képzése, *egyéb helyettesítő megoldások kialakítására van szükség (más rendszerek alkalmazása, külső szolgáltató igénybe vétele)*.

A költségvetési tartalékok kialakításakor figyelembe kell venni, hogy a katonai, speciális üzemeltetési sajátosságok miatt *kialakulhatnak olyan helyzetek, amikor a meghibásodások, kiesések előre nem látható kombinációja következik be*. Ezek leküzdése csak akkor lehetséges, ha az eszköz beszerzések, szolgáltatás szerződések területén *általános, azonnal aktivizálható tartalékok állnak rendelkezésre*.

5. A MŰKÖDÉSFOLYTONOSSÁGI TERVEK FELÜLVIZSGÁLATA, PONTOSÍTÁSA ÉS GYAKORLÁSA

Általános követelmény, hogy a működésfolytonossági tervek *folyamatosan pontosítva, minden szükséges helyen rendelkezésre álljanak*.

A helyreállítási csoportoknak és más, illetékes személyeknek ismerniük kell a működésfolytonossági tervet és felelősségét a működésfolytonosságért – ezen belül az információbiztonságért –, és ismerniük kell a tervek aktivizálásának kritériumait is.

A működésfolytonossági tervek felülvizsgálatának tartalmi követelményeit és gyakoriságát, valamint a felelős személyeket (szervezeti elemeket) az üzemeltetésért felelős vezetőnek kell meghatároznia. A felülvizsgálat ütemezésekor minden végrehajtandó feladat ellenőrzését ütemezni kell. A felülvizsgálathoz a következő módszereket (és azok kombinációit) kell alkalmazni:

1) a különböző forgatókönyvek asztali vizsgálata (a működés helyreállítási intézkedések tárgyalása, teszt megszakításokat alkalmazva);
2) szimulációk (különösen a személyek oktatásában, az incidensek utáni kríziskezelési feladatokban);
3) műszaki helyreállítási vizsgálat (annak biztosítása, hogy az információs rendszerek eredményesen visszaállíthatók);
4) a visszaállítás vizsgálata egy alternatív helyszínen (amikor a működési folyamatok a visszaállítási üzemeltetésekkel párhuzamosan futnak a főhelyszíntől távol);
5) a szállítók eszközeinek és szolgáltatásainak vizsgálata (biztosítva, hogy a külső felek által nyújtott szolgáltatások és termékek kielégítsék a szerződéses kötelezettségeket);
6) teljes próbák (annak vizsgálata, hogy a szervezet, a személyzet, a berendezés, az eszközök és a folyamatok képesek-e a meghibásodások vagy kiesések elhárítására).

A felülvizsgálatok végrehajtását dokumentálni kell. Minden esetben rögzíteni kell a megfelelőséget, a feltárt hiányosságokat és a változtatási javaslatokat. A változtatási javaslatokat a változáskezelési eljárások figyelembe vételével kell kezdeményezni, tesztelni, jóváhagyni, oktatni és hatályba léptetni.

A működésfolytonossági tervek változtatását mérlegelni kell a következő esetekben:

a) új berendezés beszerzése, a rendszerek bővítése, vagy
b) változások a következőkben:
   i) a személyzetben;
   ii) a címekben és telefonszámokban;
   iii) a szervezeti stratégiában, fontosabb feladatokban vagy folyamatokban;
   iv) a helyekben, eszközökben és erőforrásokban;
   v) a jogszabályokban;
   vi) a szerződő felekben, szállítókban és kulcsfontosságú vevőkben;
   vii) a kockázatban (üzemeltetési és pénzügyi).

A szervezetnél *a működésfolytonosságra vonatkozó tevékenységet gyakoroltatni kell* a szervezeti követelményeknek való megfelelőség biztosítása érdekében.

Az időszakosan tervezett és a meghatározott szintű változásokhoz kötött gyakorlásokat a gyakorlásból, képzésből adódó kockázatok csökkentése érdekében dokumentáltan kell tervezni; *a gyakorlás célját és hatókörét pontosan meg kell határozni*, a tervet jóvá kell hagyatni.

A működésfolytonossági tevékenységek teljes körének ellenőrzése, hatékonyságának igazolása érdekében különböző típusú és szintű gyakorlásokat kell tartani.

A gyakorlások után értékelni kell, hogy a cél megvalósult-e és a gyakorlatok lefedték-e a tervezett területeket. A gyakorlás eredményét dokumentálni kell, és *a felelős vezetőt tájékoztatni kell az eredményről*; javaslatokat kell tenni az esetleges változtatásokra.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Az egyik legfontosabb levonható következtetés, hogy a működésfolytonossági tevékenységet egyrészt *integrálni kell a katonai szervezetek tevékenységébe*, másrészt azokat *előre meghatározott célok megvalósítása érdekében kell kialakítani*.

Fontos annak leszögezése is, hogy a kívánt célt – a szükséges mértékű rendelkezésre állást – csak tervezett, dokumentált, tesztelt, jóváhagyott, begyakorolt, felülvizsgált és pontosított eljárások szolgálhatják, a rögtönzés, összehangolatlan döntések (vagy döntések hiánya) a helyzetet csak ronthatják. Az előre jósolható, fontosabb eseteket modellezni kell, és *típus eljárásokat kell kidolgozni, ami elősegíti azt, hogy a különböző szintű vezetőknek csak a valóban egyedi esetekben kell döntést hoznia*.

A fentiek alapján megállapítható az is, hogy *a honvédelmi tárca információ biztonságpolitikája a működésfolytonosságra vonatkozóan kiegészítésre szorul [15.]*. A nyilvánvaló szoros összefüggések alapján a kiegészítés során *célszerű a Kritikus Infrastruktúra Védelem feladatainak támogatását is figyelembe venni*.

A keretrendszerű, általános feladatok megfogalmazása alapján az egyes elektronikus adatkezelő képességekre vonatkozó védelmi rendszabályok egyszerűen *pontosíthatók a képességekért felelős vezetők, üzemeltetők, biztonságért felelős személyek által, illetve könnyebben megfogalmazhatók azok a fenntartási feladatok melyek a logisztikai szakterületről nélkülözhetetlenek a szükséges mértékű rendelkezésre állás megvalósítása*.

HIVATKOZÁSOK

[1.] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről, 58. §. 1-2. bekezdés

[2.] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 1. §. 22. p. és 58-59.§.

[3.] 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről, 7.§. d. és 8. §. (1)

[4.] 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról, 2. sz. melléklet, a központi elektronikus szolgáltató rendszer informatikai katasztrófaelhárítási tervének alapkövetelményei

[5.] Magyar Köztársaság Katonai Stratégia, I, II, és IV. fejezetek

[6.] 103/2009. (XII. 31.) HM utasítás a honvédelmi tárca 2010. évi fő feladatainak és a 2011-12. évi tevékenysége fő irányainak meghatározására, 6. §. és 11. §.

[7.] COBIT 4. 1. DS 4.1 – 4. 10. p, DS 11. 1. és 11. 5. p. DS 13. 1 – 13. 4. p.

[8.] ITIL v.3. Service Operation, 4.1. Event Management, 4.4. Availability management, 4.5. IT Service Continuity Management

[9.] The Standard of Good Practice for Information Security; Information Security Forum (ISF), 2007, UE 4. 4.2. p, SM 5.2. 5.2.2. p. SM 5.3. 5. 3. 6. p.

[10.] A Chief Information Officer kézikönyve, 2003, Management Kiadó Kft. ISBN 963 86190 9 0; 7. 4. 6. p, 7. 5. 3. p, és 7. 7. 1. p.

[11.] MSZ ISO/IEC 27001:2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények, „A” melléklet, A 14. 1 – 14. 1. 5. p.

[12.] ISO/IEC 17799: 2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002:2006), 14. 1 .1 – 14. 1. 5. p.

[13.] Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszer (MIBIK), Informatikai Biztonsági Követelmények v 1.1. 2008, 14. fejezet

[14.] Business Continuity Management – Part 2. Specification (BS 25999-2:2007); 4. 4. 1. p, 4. 4. 3. p, és 4. 4. 2. p.

[15.] Informatika. Szolgáltatásirányítás 1. rész: Előírás (MSZ ISO/IEC 20000-1: 2007), 6. 3. fejezet

[16.] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Koleszár Béla
koleszar@tele2.at

A ROBOTHADVISELÉS ETIKAI KÉRDÉSEI III[1]
ROBOTOK HELYETT EMBEREK?

Absztrakt

A szerző felsorolja azokat a kritériumokat, amelyek fékezik, illetve kizárják a robotok alkalmazását. Vannak olyan szituációk, amikor szeretnénk, de nem tudunk robotokat bevetni, automatikus vezérlést igénybe venni. Hol nem lehetséges, hol nem gazdaságos, hol nem szabad, hol nem etikus emberek helyett robotok, önműködő eszközök alkalmazása?

The author lists the criteria that hinder or preclude the application of robots. There are situations when we want to, but we can not deploy robots, use automatic control. Where is it impossible, where is it uneconomical, where is it forbidden, where is it unethical to use robots, automated tools instead of people?

Kulcsszavak: *robot, robothadviselés, robotetika ~ robot, robot warfare, robot ethic*

BEVEZETÉS

Két cikkemben [1, 2] már foglalkoztam a robothadviselés etikai kérdéseivel: Az elsőben elemeztem a robotokat, azon belül a felfegyverzett robotokat, taglaltam az emberek és a gépek közötti alapvető különbségeket. A másodikban a katonai erkölcs speciális területeit vizsgáltam. Akkor még sokkal elfogultabb voltam a robotokkal szemben. Talán kicsit tudatosan is, hiszen a kidolgozás alatt álló doktori értekezésem témája[2] a robotokkal kapcsolatos. Jelen írásomban részletesebben megvizsgálom a másik oldalt is, tehát felcsapok az „ember ügyvédjének”! Félreértés ne essék, nem a robotok ellen ágálok, hanem tisztázni szeretném az őket megillető helyüket a világunkban.

A kutatómunkám során újból és újból szembe kerültem a **robotfelhasználások, illetve a fel nem használásuk** erkölcsi problémáival. Most ez utóbbi témakörre, tehát a robotok bevetésének elvetése, késleltetése, elodázása, gátlása, korlátozása, szabotálása miatt felvetődő kérdésekre keresek választ. Sok esetben, még ha szeretnénk, sem lehet robotokat alkalmazni.

A teljesség igénye nélkül, néhány szemléltető példa alapján rendszerezem az okokat.

[1] A téma rövidített változatban, a Robothadviselés 10 [3] konferencián került előadásra
[2] Földi robottechnikai eszközök konstrukciós és alkalmazási kérdései, különös tekintettel a békefenntartó missziók biztonságának növelésére.

1 ROBOTOK CSERNOBILBAN

A **biorobot** kifejezést általában az állatvilág, ill. bionika[3] ihlette robotkonstrukciókra, az élőlények és gépek kombinációjára használják. Ilyenek például az állatokat (rágcsálókat, rovarokat, stb.) beültetett elektródákkal irányítani / vezérelni képes „rendszerek".

Jelen írásom kiváltó szikrája volt, amikor – a világhálón robotok után kutatva – ráakadtam a csernobili katasztrófáról készült dokumentumfilmben[4] egy másik biorobot-értelmezésre. A 7. részben [4] mutatják be, amikor az etika szempontjából nagyon visszás helyzet alakult ki. A robbanás által szétszórt, nagyon erősen sugárzó törmelékeket **robotjármű**vek segítségével próbálták eltakarítani, ezek sajnos csak nagyon rövid ideig maradtak működőképesek. (1. kép)



1. kép. Robotjármű a reaktortető tisztításakor [5]

Az uránium rudak burkolatából származó grafit-tömbök, óránként 1000 Röntgent is meghaladó sugárzása valósággal megbénította a robotok elektronikus áramköreit. Egyre hibásabban működtek, míg használhatatlanok nem lettek. Volt olyan is, amelyik a tisztítandó tetőről a mélybe „vetette magát". Végül, az idő szorítása miatt **a robotokat emberekkel helyettesítették!** Ezeket, a részben önként, részben parancsra (behívott fiatal tartalékosok voltak) cselekvő embereket akkor – a helyzetből adódóan – „**bio- robotok**"-nak nevezték el… (2. kép)

[3] *„A bionika egy tudományág, mely a biológiát, a technikát és az elektronikát hivatott egyesíteni. Fő célja, hogy az élőlények felépítését és mechanizmusait gyakorlati szinten megvalósítsák mesterséges gépekben, mintegy lemásolva az evolúció által évmilliókig tökéletesített természetes szervezeteket."* [6]

[4] Thomas Johnson: A csernobili csata igaz története - Battle of Chernobyl (Discovery Network International)



2. kép. „Bio- robotok” [7]

3500 tartalékos katona, esetenként pár percig dolgozott a tetőn, voltak, akik 5-5 alkalommal is. Személyi védelmüket (sisak, védőmaszk, dupla kesztyű, árnyékolt csizma, ólomkötények – 25-30 kg) maguk rögtönözték a bevetésük előtti éjszakán. Rosszabbul jártak a nyílt, erősen sugárzó reaktortérbe különböző anyagokat ledobó helikopterek pilótái, mert további cserepilóták híján sokszor kényszerültek repülni (összesen 1800 átrepülés). Közülük nagyon sokan kaptak halálos dózisú sugárzást. A helyszínre elsőként kiérkező tűzoltók is gyakorlatilag védőfelszerelések nélkül próbálták oltani az olthatatlant…

A robotjárművek **fejletlensége** (nem ilyen bevetésre tervezték őket), illetve a távirányítható légi eszközök **teljes hiány**a volt az ok, hogy robotok helyett embereket kellett bevetni. A katasztrófa okait vizsgálva derült ki, hogy az atomerőművet kezelő személyzet tagjai egy rosszul megtervezett és még rosszabbul kivitelezett kísérlet folytán **az automata üzemmódú biztonsági rendszereket kikapcsolták!** Paradoxon, hogy egy üzemzavari esetet próbáltak szimulálni.

2 ETIKAI MEGFONTOLÁSOK

2.1 Pszichológiai problémák

*„Az viszont kétségtelen, hogy a robottechnikának már most is vannak olyan alkalmazási területei, ahol felmerülnek etikai kérdések. Nem csak a hadi és az ipari robotok lehetnek veszélyesek: egy brit kutató szerint komoly pszichológiai kockázattal járnak azok a gépek is, amelyeket egyes ázsiai országokban mind gyakrabban használnak gyerekmegőrzésre és idősekről való gondoskodásra. Dél-Koreában és Japánban legalább tizennégy cég foglalkozik ilyen robotok gyártásával, és Noel Sharkey, a Sheffieldi Egyetem számítástechnika-professzora szerint ez a gyakorlat **előre nem várt kockázatok**hoz és etikai problémákhoz vezet. Azokat a gyerekeket, akikre robotok vigyáznak, hosszú távon **káros pszichológiai hatások** érik **az emberi kapcsolatok hiánya** miatt. Majmokkal végzett kísérletek bizonyítják, hogy azok a fiatal egyedek, amelyeket robotok gondoznak, képtelenné válnak a fajtársaikkal való kapcsolattartásra és a szaporodásra, írta Sharkey a Science magazinban 2008 decemberében. Ugyanígy gondot jelenthetnek az időseknek szánt robotok, mint a japán My Spoon* (3. kép)*, amely megeteti a gazdáját, vagy az az elektronikus fürdőkád, amely*

megfürdeti és megszárítja a tolószékes pácienseket, nem beszélve a Matsushita beszélő játékmackójáról, amely időről időre feltesz egy kérdést az idősek otthonában élő ápoltaknak, és a reakcióidőből állapítja meg, hogy riassza-e a humán ápolószemélyzetet."[5] [8]



3. kép. My Spoon, az etetőrobot [8]

Miklósi Ádám, Érzelmet a gépekbe! c. írásából, a fenti problémákat taglaló gondolatmenete: *„A közhiedelemmel szemben **a kommunikáció nem pusztán "információcsere", hanem érzelmek "cseréje" is**. Ha két ember beszélget, sok esetben a mondanivalót kísérő érzelmek fontosabbak, mint a mondatok jelentése. A pszichológusok régóta tudják, hogy az érzelmek fokozzák a kommunikáció hatékonyságát. Ezt a felismerést igyekeznek a modern kor szakemberei átültetni az **ember-gép kommunikáció** gyakorlatába. Feltételezésük szerint az ember-gép kapcsolat is sokkal hatékonyabb lehet, ha lehetőség nyílna arra is, hogy a gép és az ember kölcsönösen felismerje a másik érzelmi állapotát."* [9]

Vannak ilyen irányú fejlesztések, ahol az arcfelismerés, az emberi mimika felismerése, ill. utánzása a cél.

2.2 „Lovagiasság"

Idézet a Vadászati Kulturális Egyesület Etikai Bizottsága által kidolgozott **vadászat etikai kódex**ből: *„A vadászat végső célja a vad elejtése és birtokbavétele, de nem minden eszközzel és minden áron! A vadászat humanizálódása annyit jelent, hogy esélyt adunk a vadnak és lehetőségeink tekintetében korlátozzuk egymást és magunkat. **Sorozatlövő fegyverekkel tilos** és etikátlan vadászni, de az egyébként engedélyezett többlövetű ismétlő fegyverek használatánál is joggal elvárható a töltényszám minimalizálása, azaz az önkorlátozás. A gépkocsiból, traktorról, kombájnról, helikopterről történő vadászatot nemcsak a törvény, de a jóérzés is tiltja. Infratávcsövet, csalihangokat hallató magnetofon-felvételeket, az üzekedő állatok ösztöneire ható szagkeltő anyagokat, azaz **a modern technika képességpótló eszközeit az igaz vadász nem alkalmazza**, mert a vad istenadta képességeivel csak a vadász saját képességeit, illetve az emberi kitartást, szívósságot és akaraterőt illik szembeállítani."* [10]

[5] Az idézetekben található vastagon szedett kiemelések a cikk szerzőjétől (KB)

Az emberek (ellenséges katonák) ellen, a „tiltott, de tanított” **meglepő csapda**ként [11] robotokat alkalmazni nem etikus. Sem fejlettebb robotokat, sem „primitíveket”. Nagyon leegyszerűsítve ide sorolhatjuk a **taposóaknák**at és a **kazettás bombák** szétszórt résztölteteit is. Az ezek alkalmazását tiltó nemzetközi egyezményt még nem minden nemzet írta alá.

2.3 Emberek alkalmazása ⇔ hatékonyság ⇔ minőség

Robotok helyett / mellett emberek alkalmazása etikus is lehet: beléptető rendszereknél a gépek helyett emberek alkalmazása humánusabb. Az automata (gépi) rendszerek mellett alkalmazva, egymást segítve és kölcsönösen kiegészítve a hatékonyság is növekedhet. A munkanélküliség csökkentése is egy fontos szempont.

Magyarországon is használnak nagy teljesítményű, távirányítható robot-fűkaszáló-, ill. vetőgépeket. [12] Ezeket a nagy, meredek felületek füvesítésénél (pl. gátak, autópályák rézsűi, domboldalak), karbantartásánál használják. (4. kép)



4. kép. Dvořak fűkaszáló gép [13]

A versenykiírásoknál ezzel a modern technikával szemben állnak a füvesítő brigádok, akik kézzel, jobb esetben kézi vetőgépekkel vetnek, manuálisan, illetve egyszerű gépekkel kaszálnak.

Kézi munkával a **robot-minőség** elérhetetlen, viszont több embernek ad munkát. A támogatások rendszerétől (pl. kedvezmények a munkanélküliek alkalmazása esetén) is függ, melyik technológia a „nyerő”. **Környezetvédelmi szempontok** is közrejátszhatnak, például egy fokozottan védett területen tiltott lehet bármilyen gép használata.

A minőséget másként értékelve, robotokkal csak „**tömegáru**” **minőség**ű termékeket lehet előállíttatni, hiszen emberi irányítás nélkül hiányzik belőlük a kreativitás. Automata üzemmódban a betáplált programjaik szerinti „**klónok**”-at tudnak csak előállítani. A kézművességen túllépve, a művészi munkák egyedisége a **művész személyiség**ének „beledolgozása” nélkül nem valósulhat meg. Tehát robot segítségével is elő lehet állítani művészi értékkel bíró alkotást, de csak a művész direkt irányításával.

3 TOVÁBBI SZEMPONTOK

3.1 Ha a számítógép segítségre szorul

„Számos olyan problémakör van ugyanis a számítástechnikában, mely egy gépnek szinte megoldhatatlan, viszont egy ember pillanatok alatt megadja a választ. Kinek okozna például gondot, ha azt kellene eldöntenie, hogy egy adott képen szerepel-e banán? Gondolom senkinek. Viszont ha ezt a feladatot számítógéppel szeretnénk elvégeztetni, akkor speciális programot kellene írnunk, mely rengeteg számítás elvégzése után sem tudná egészen bizonyosan megmondani az eredményt. ... Manapság az ember-számítógép interakció a következőképpen működik: az ember megfogalmaz kérdéseket, majd a számítógép a jól feltett kérdéseket hosszas számítások árán megválaszolja. Miért ne lehetne megfordítani ezt a dolgot? Miért ne tehetne fel a számítógép is kérdéseket hús vér embereknek? Az ***Amazon Mechanical Turk****-je pontosan ezt csinálja. Biztosít egy olyan programozói felületet melyen keresztül pillanatokon belül kérdéseket küldhetünk az Amazon szervereinek. Ott ezeket a kérdéseket emberek böngészhetik, akik egy kérdés megválaszolása után megkapják az általunk felajánlott díjat. A szolgáltatásnak mindössze 10% közvetítői díja van. ...*

```
read (photo);
photoContainsHuman = callMechanicalTurk(photo);
if (photoContainsHuman == TRUE){
   acceptPhoto;
}
else {
   rejectPhoto;
}
```

A fenti program arra keresi a választ, hogy vajon a képen szerepel-e ember. Meghívja tehát az Amazon Mechanical Turk-jét, melynek segítségével pillanatok alatt megkaphatja a kérdéses eredményt." [14]

3.2 Robotok emberek általi felülbírálása

A **szabad akarat** pozitív dolog, sokan az emberi lét egyik legfontosabb ismérvének tartják. Az **öntörvényesség** ezzel szemben negatív. Nehéz egyértelműen eldönteni, hol húzódik kettőjük között a határvonal.

A gyalogos átkelőhelyeknél sokan már piroson lelépnek a zebrára, mintegy „megelőlegezve" a zöldet, tehát akkor, amikor az autók már lassítanak. Így viszont csökken a **biztonsági puffer**, ami az automata rendszer fontos része. Problémát jelenthet egy forgalmi-rend változás is, amikor például a leforduló sáv is kap plusz egy külön „zöldet". Bizonytalanságot jelent, hogy mindenki másként értékeli (hangulattól, stressztől függően is) a sárga jelzést, valaki hirtelen fékez, mások még jóval a kereszteződés előtt is „rágázolnak". Több országban, például a szomszédos Ausztriában is, a sárga előtt villogó zöld jelzést vezettek be, a sárga előkészítéseként. Saját tapasztalatból is mondom, hogy ez a megoldás nem jó, mert így jóval meghosszabbodik a fokozottan veszélyes „**hezitálási időszak**".

Vannak esetek, amikor az automatikusan vezérelt, közlekedési lámpák által szabályozott kereszteződésben a **rendőrök veszik át a forgalom irányítását**. Ez lehet a jelzőlámpák helyettesítése (pl. meghibásodás esetén), de lehet azok felülbírálása is (pl. kormánydelegációk áthaladása esetén). A **pillanatnyi forgalomtól független rendszer**ek egy bizonyos közlekedési frekvencia alatt csak fékezik a forgalmat, ezért is kapcsolják ki őket éjjel – kevés input – **alulszabályozott rendszer**. Kamerák, szenzorok beépítésével lehet ezen javítani, de ez nem olcsó. A jelzőlámpás kereszteződéseket egyre gyakrabban váltják le **körforgalom**mal. Ez a hagyományos kereszteződéssel összevetve, az emberek számára **egyszerűbb döntési**

feladatot jelent. Rossz döntés esetén sem olyan súlyosak a következmények, a tudatosan kikényszerített alacsonyabb sebességek miatt.

Az automaták ember általi felülbírálása megjelenik ajtóknál, felvonóknál, biztonsági beléptető rendszereknél, stb. is. Néha alig tud elindulni a közlekedési eszköz, mert mindig valaki blokkolja a fotocellás rendszert (hogy még mások be tudjanak szállni), ezzel akár csökkentve is az össz- szállítási kapacitást (frekvenciacsökkenés).

Az első **holdraszállás**kor *„a leszállást végig nehézségek kísérték, ismeretlen komputerhiba támadt kétszer is, majd a felszín fölött igen alacsonyan kiderült, hogy a simának hitt térség hatalmas sziklákkal és egy nagy kráterrel tarkított, ami közvetlen életveszélyt jelentett az űrhajósokra nézve. Armstrong végül az egyébként is szűkös üzemanyag intenzív felhasználásával,* ***kézi vezérléssel*** *bravúrosan egy biztonságos helyre navigálta a holdkompot…”* [15]

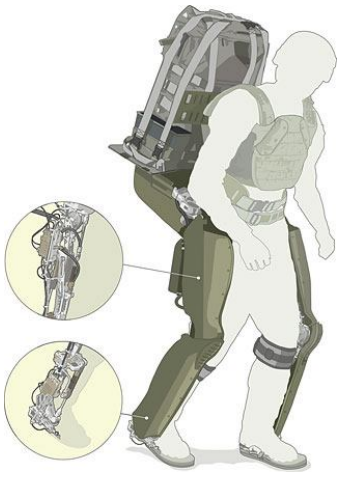
Hasonló esetekben a **túlszabályozás** is problémát jelent, mert a döntésképtelenség miatti kivárás időzavart eredményezhet.

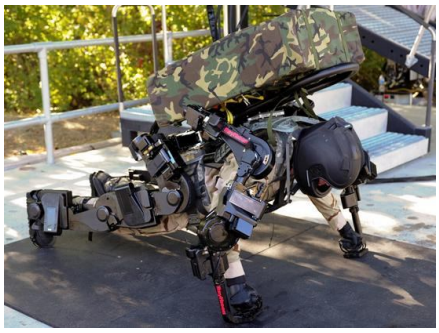
3.3 Emberek „ódzkodása” a robotoktól

Európában az automata sebességváltók elterjedése lassú, pedig sok előnnyel bírnak. Sokáig a magasabb fogyasztást nevezte meg a legtöbb ember legfőbb negatívumként. Az új fejlesztésű kapcsolószekrényeknél már ez nem állja meg a helyét. Sőt! Még a gyakorlatlan vezető is gazdaságosabban, és főleg biztonságosabban közlekedhet önműködő hajtással. Az automata fényképezőgépek megjelenésekor a manuális beállítások lehetősége általános elvárás volt, ma erre csak egy kisebb (szakértő, profi) csoport tart igényt.

A hús-vér emberre első pillantásra megtévesztésig hasonlító (humanoid) „lények” (androidok) taszítanak minket. Hasonló ellenérzés Japánban valószínűleg nem tapasztalható, ezt mutatja a számos robot-fejlesztés, s azok széleskörű támogatottsága.

Mi inkább elfogadhatónak tartjuk az **ember formájú robotok helyett a „robot formájú” emberek**et, tehát az emberek képességeit fokozni tudó segédeszközök, kiegészítők pl. exoskeletonok – külső vázak alkalmazását. (5. - 7. kép)







5., 6., 7. kép. „Citius, Altius, Fortius”[6] [16, 17, 18]

[6] **citius, altius, fortius** *lat, sport* az olimpia hármas jelszava: gyorsabban, magasabbra, erősebben [19]

3.4 Biztonság

Az aránylag jól automatizálható / robotizálható vonatközlekedésben komoly gondot jelentenek a **kábellopások**. Körültekintően tervezett rendszernél persze ez nem okozhat biztonsági problémát, viszont egy létfontosságú rendszer kiesése esetén a közlekedés azonnali leállítását eredményezheti. Humán mozdonyvezető ilyen esetben – ugyan korlátozott sebességgel, de tovább viheti a szerelvényt.

Az emberek egy része hajlamos arra, hogy az automata (akár biztonsági) rendszereket öntörvényűen felülbírálják, „velem nem történhet baj" alapon. Régebben például gyakori volt a szabványos olvadóbiztosítékok huzallal való áthidalása. Megoldást az automata (visszakapcsolható) biztosítékok hoztak.

Az **analóg tachográfok**[7] manipulálása is aránylag gyakori volt. Ezt megelőzendő, *„Az Európai Unió rendeletben (a Tanács 1998. szeptember 24-i 2135/98/EK rendelete) határozta meg a **digitális tachográfok** bevezetését a vezetési- és pihenőidők fokozottabb betartatásának érdekében. A digitális tachográfok kötelező alkalmazása a 3,5 tonna feletti megengedett legnagyobb össztömegű tehergépjárművekre, valamint a 9 főnél több személy szállítására alkalmas és erre a célra szolgáló személyszállító járművekre terjed ki."* [22]

Azok a jó automatikus biztonsági rendszerek, amelyekkel az emberek meg vannak elégedve, ideális esetben nem is tudnak a létezésükről. Tökéletes biztonsági rendszerek azok, amelyeket az emberek, még ha akarják, sem tudják kiiktatni. A csernobili atomerőmű biztonsági rendszere sajnos nem ilyen volt…

4 ROBOTHADVISELÉS

4.1 „Olcsó ragadozó"

Az MQ-1 Predator érzékelő és csapásmérő egységeit az ATK Integrated Systems rászereli egy személyszállító Cessnára (208B ISR Armed Caravan) [23] (5. és 6. kép) – a kiszolgáltatott (döntéshozásból kiiktatott) pilóta így gyakorlatilag azt sem tudja, miben vesz részt. A civil gépnek látszó repülőgép zavartalanabbul, feltűnés nélkül járőrözhet. Nem mellékes a rendszer üzemeltetésének gazdaságossága sem. Mindezek ellenére az eljárás erkölcsössége megkérdőjelezhető…



5. kép. Felfegyverzett Cessna [24]

[7] tachográf = menetíró



6. kép. Predatortól „kölcsönzött” érzékelő-dóm [25]

4.2 Helyzetismeret

Hans-Joachim Ruff-Stahl szerint: *„a **Situation Awareness**[8] (SA) fogalmat Dr. Mica Endsley-nek köszönhetjük. Az SA-nak három szintjét különbözteti meg:*

- *az információ észlelése és gyűjtése*
- *az információ jelentőségének megértése*
- *a további fejlődés ebből következtethető előrejelzése (prognózisa)*

...

Ezzel szemben áll az emberi agy behatárolt befogadó-, ill. feldolgozó képessége. Mindenekelőtt az agy soros, tehát lépésről lépésre működő (~töltődő-KB) *logikus-racionális kapacitásai lesznek a sokrétű-dinamikus helyzetekben gyorsan túlterheltek. Mindemellett **az emberi agy** főleg a nem racionális, a logikával párhuzamosan futó folyamatoknál nem csak a Situation Awareness egy magas szintjét képes biztosítani, hanem **képes gyorsan és helyesen dönteni anélkül, hogy az indokait meg tudná fogalmazni, vagy ésszerűen le tudná vezetni**.”*[9] [26]

Az érzékszerveink (ízlés, szaglás, tapintás, látás, hallás) által szolgáltatott – sokszor tudat alatti – információk mellett az általános tapasztalatnak, háttértudásnak, intuíció[10]-knak van szerepe az ilyen (jó) döntések „sugallatában”. Ezeket nem szabad összekeverni a latens[11] kívánalmainkkal, illetve a túlzott aggályainkkal, félelmünkkel. Az emóciók, stressz, „vad” ösztönök általában rossz tanácsadók!

Az automata rendszerek tökéletesen megfelelnek a helyzetismerethez szükséges (ill. nem szükséges) adatok gyűjtésére, tárolására. Sőt, ezeknek a rutinszerű osztályozásukra, előzetes kiértékelésükre is, nagyon hatékonyan támogatva a személyzet munkáját. **A következtetések alapján történő döntések meghozatala viszont az ember feladata marad!** Az ember viszont nem dönthet „gépiesen”, nem hagyatkozhat 100 %-ban a robot-műszerek, robot-algoritmusok által szolgáltatott adatokra (meghibásodás veszélye, rosszindulatú külső beavatkozás, stb.). Az egészséges bizalmatlanság itt erény, természetesen a „józan paraszti ész” határain belül.

---

[8] situation awareness=helyzetismeret; Dr. Munk Sándor szerint a helyzetismeret *"egy katonai művelet végrehajtási környezetére vonatkozó konkrét tudás."* [27]

[9] az idézetet magyar nyelvre fordította: KB

[10] intuíció – *„1. ösztönös megérzés, felismerés 2. élményből táplálkozó megismerés”* [20]

[11] latens – *„lappangó, rejtett, nyíltan nem mutatkozó”* [21]

A **hagyományos térképolvasás képessége** is nagy segítséget jelent az általános **helyzetismeret tökéletesítésé**hez. Már csak ezért meg kell maradnia ennek a tudásnak, de a globális helymeghatározó rendszerekre különben sem szabad korlátlanul / kritikátlanul hagyatkozni. A civil életben egyre gyakrabban, de már a mentőszolgálatnál is előfordult, hogy rossz helyre navigálta őket a gép: *„A késés oka valószínűleg az volt, hogy egy ideig rossz irányban haladtak a GPS-készülékük hibás útvonaljavaslata miatt…”* [28]

4.3 Fegyverhasználat

Robot helyett ember! A robothadviselés etikai törvénye szerint a robotok ember elleni bevetésekor **mindig az embernek kell a végső döntést meghoznia**, lehetőleg a bevetés minél későbbi / legeslegutolsó fázisában! Ma még nem létezik olyan szintű mesterséges intelligencia, amelyik a robotok (emberek elleni, és más) fegyverhasználatáról felelősségteljesen dönteni tudna. Ezért **a fegyverhasználatról nem dönthet más, csak ember**! Az indokolatlan, nem megfelelő, nem arányos mértékű válaszcsapás miatt történt balesetek miatt a mai fejlettségű robotok nem hibáztathatók. Még azok gyártói, tervezői, programozói, tesztelői, stb. is csak másodlagosan, olyan esetekben vonhatók felelősségre, ha bizonyítottan, az ő emberi mulasztásuk miatti hibás üzemmód, meghibásodás, illetve üzemzavar okozott balesetet.

Az asimovi értelemben vett Robot (tudatosan írtam nagybetűvel) létrehozása még sokáig várat magára. A mai legfejlettebb robotok is csak gyermeki szinteken vannak. Büntetőjogi szempontból „értékelhetetlennek” számítanak. Egyes tulajdonságaik ugyan jóval meghaladják az emberét (pl. számolási képességek, gyorsaság, erő, stb.), de az összefüggések felismerésében, a döntéshozatalban, programjaikra (programozóik következetességére, tanító-tesztelésük mélységére) vannak utalva. Új, saját következtetésekre képtelenek. Egy példa: az új állatvédelmi törvény [41/2010. (II. 26.) Korm. Rendelet] szerint tilos az ebet tartósan 4 m-nél rövidebb eszközzel kikötve tartani. Logikus következtetés, hogy hosszabbal lehet. Nem tudom, milyen választ kapnánk, ha megkérdeznénk egy robotot (ill. vezérlő algoritmusát), hogy egy embert milyen hosszú eszközzel lehet kikötni? A normális körülmények között fejlődő kisgyerekek tudják, hogy embert nem lehet megkötni. Tanulással, megfigyeléssel, beleéléssel tesznek szert egyre nagyobb tapasztalatra, egyre inkább kinyílik az „Én”-jük. Egy gép programozója viszont megfeledkezhet az „ezt már egy csecsemő is tudja” alapinformációkról. Nem szabad megfeledkeznünk a magunkkal hozott **ösztöneink**ről sem! Ezeket még magunk sem ismerjük igazán, nem hogy egy gépbe tudnánk táplálni…

A robotrendszerek régebben csak jelezték a veszélyt, ma már önműködően teszik meg az ellenlépéseket. Ezek az ellenlépések a körülmények nem teljes körű kiértékelése mellett veszélyesek lehetnek pl. a civil lakosságra, saját bajtársakra, stb. A robot, ha (számunkra) egyértelműnek számító információt / tiltást nem kap meg, rosszul dönthet! A betáplált logikai kapcsolatai alapján ugyan egyértelműen, de a helyzet megítéléséhez nincs elégséges információ tudatában „embertelen” döntést hozhat…

A nagyon gyors, önműködő fegyvereknél (pl. védelmi elhárító rendszerek) arra kell törekedni, hogy az emberi beavatkozás (leállítás) szükség esetén a lehető legrövidebb időn belül megtörténhessen. Például ha ellenség-barát felismerő rendszer nélkül valaki / valami berepül a „piros” zónába, akkor az automata rendszert ki kell kapcsolni, ill. a zóna határait módosítani kell.

Ki kell küszöbölni a felügyelet nélküli üzemmód (gondatlanság, figyelmetlenség, stressz, túlterheltség, sebesülés, elesés miatti) **lehetőségét**.

Pogácsás Imre szerint az UAV-k jövőbeni elterjedése mellett a földön maradnak a humán erők: *„A kiemelkedő harci potenciállal bíró pilóta nélküli és robotrepülőkkel támogatott hagyományos gyalogság, használva az evolúció által megadatott természetes **humanoid intelligenciá**t, a kettő kombinációjával csodákra lehet képes.”* [29]

4.4 Célzott, rosszindulatú emberi beavatkozások

*„A közelmúltban történt Irán elleni **kibertámadás**t minden bizonnyal mérföldkőként fogja számon tartani a történelem. 2010. szeptember 25-én Irán bejelentette, hogy **Stuxnet** nevű vírussal fertőződtek ipari létesítményeinek irányítási rendszerei. Ezt a vírust kifejezetten a Siemens által tervezett ipari létesítmények ellen készítették… Abba jobb nem belegondolni, hogy ez milyen következményekkel járhat például egy működő atomerőműben. Egy ilyen vírus készítése komoly ismereteket igényel nemcsak a programozás, hanem az ipari irányításrendszerek területén is. A különösen fontos létesítmények informatikai rendszere általában zárt. Persze a rosszul tervezett vagy fegyelmezetlen felhasználókkal működtetett hálózatok rést nyithatnak a világháló felé. … Jelen esetben valószínűleg egy „**titkos szolga**” szándékosan telepítette a vírust, mely most már önálló életet él. … Az azonban biztosnak látszik, hogy **a kibertér védelmét nem lehet csak technikai informatikai alapon kezelni**.”* [30]

Láthatjuk, hogy ilyen „sebészi” pontosságú támadást csak (szak-) emberek képesek véghezvinni, a rosszindulatú céllal, tömegesen indított **robot-programok** ilyen erre nem alkalmasak. Általában, még mielőtt komolyabb problémákat okoznának, már megvan ellenük a hatékony védelem.

Illetve mégsem? A Robothadviselés 10 konferencián [3] Sipos Marianna és Kovács László a fent említett támadásról egy nagyon részletes előadás (*Stuxnet és ami mögötte van*) keretén belül számoltak be. A többszörös titkosítással és védelemmel rejtett vírus legalább egy fél évig úgy fertőzött, hogy a számítógépek biztonságával foglalkozó cégek nem is tudtak a létezéséről!

5 GYÁRTÁS, FEJLESZTÉS, TESZTELÉS

A sokszor nagyon „kegyetlen-kemény” gazdasági mérlegeléseknél számolni kell azzal, hogy a már létező drága robotrendszerek helyett / mellett / védelmére (!) embereket vetnek majd be.

5.1 Civilizációk összecsapása?

Huntigton[12] korszakmagyarázó, már-már látnoki gondolatai újból és újból visszaköszönnek az élet szinte minden területén.

Clément Ruffier a **Francia robot – kínai munkás** c. cikkében az egyes termelési módokat *„A civilizációk összecsapása?”* kérdéseként veti fel. Az automata *„hibajelzők”* kicselezése: *„feleslegesen mozgatták pl. a kezüket az adott érzékelő előtt, így szimulálva azt, hogy épp egy hiányzó alkatrészt ragadnak meg; feleslegesen betettek valamit egy ládába, hogy egy-egy súlyérzékelőt becsapjanak. Hasonló célból odáig jutottak, hogy különféle tárgyakat fabrikáltak – olykor például egy fémlapot, ha arról volt szó, hogy az egyes alkatrészek behelyezésének ellenőrzésével megbízott mágnes „eszén túljárjanak”. Ilyen trükkökkel e berendezések szakértőivé lettek – azok, akiknek feladata elsősorban teherautómotorok összeszerelése lett volna!”…* A kínaiak, a termelést átvéve: *„Először is, a gyártósort a francia eredetihez képest kevésbé automatizálták, a robotok számát minimálisra csökkentették – tekintettel arra, hogy méregdrágák – és szó szerint túlságosan „megkötik a munkások kezét”. Robotok beállítására csak a kézi műveletek kudarca után került sor.”…* Az egyik szerelősör vezetőjének érdekes megjegyzése, amivel egyelőre a robotok nem sokra jutnak: ***„A szabályok olyan útjelzők, melyeket az ember használ ugyan, de sosem lehet szó szerint követni őket.”*** –

[12] Samuel P. Huntigton (1927-2008), Legismertebb műve: A civilizációk összecsapása és a világrend átalakulása [31]

„Az ő gépsorának szerelői megtehetik, hogy a főnökség engedélyével eltérnek a szigorú eljárásrendtől – ezt lehetővé teszi az igen kemény ellenőrzési rendszer.”…
„…a Renault Trucks arra törekedett, hogy a gyártási eljárások beállításával és betartatásával megelőzze a működési zavarokat, a Dongfeng a rugalmasságot, a flexibilitást, és a konkrét kihívásokra való gyors reagálást preferálta…” [32]

A Dongfeng vezetője által megfogalmazott – fent kiemelt – szabályokról szóló definícióval a robotok vezérlő programjai nem tudnak mit kezdeni, de nem is szabad megengednünk, hogy ilyen irányba tartson a fejlődésük – fejlesztésük!

A profitorientáltság miatt **a termelés kikerülése kevésbé fejlett országokba** korunk trendjének is nevezhető. Elsősorban a munkaigényes, monoton, veszélyes, környezetre és a munkásokra ártalmas munkák „exportálása” vált divattá. A fejlett ipari országokban érvényben lévő szigorú előírások miatt ezeket a munkafolyamatokat robotokkal kellene elvégeztetni…

5.2 Visszalépés?

Érdekes probléma jelentkezik az új, nemzetközi támogatottságú STOVL[13] JSF[14] (F-35B) repülőgépek (8. kép) új rendszereinek fejlesztésénél / tesztelésénél: *„Már 1990-ben elkezdett a brit Védelmi Értékelő és Kutató Ügynökség DERA (Defence Evaluation and Research Agency) a STOVL kategóriájú repülőgépek új vezérlő rendszerén dolgozni. Teszt-platformként a **kétüléses** … Harrier T2 (XW175)-öt* (9. kép) *választották. …a hátsó pilótatérbe szerelték a teljesen elektronizált FBW (Fly By Wire) irányítórendszert, míg az első fedélzeten megmaradt a hagyományos rendszer. Így a hátsó ülésen a berepülő pilóta tesztelheti az új irányító elemeket, míg az első kabin pilótája segít az összes rendszer megfigyelésével, szükség esetén lekapcsolhatja az elektronikus vezérlést és átveheti a teljes irányítást a gép fölött. A VAAC Harrier **az egyetlen STOVL repülőgép, amelyik rendelkezik ezekkel a képeségekkel**…* Különféle, hosszan tartó tesztsorozatok után *„2001. június 1-én bejelentette a QinetiQ vállalat, a DERA ügynökég utódcége, hogy a VAAC Harrier segítségével megkezdte az **automatikus visszatérés rezsimjé**nek a tesztelését. … Ez még csak az első lépés volt az új JPALS (Joint Precision Approach Landing System) megközelítő és leszálló fejlesztési programban a STOVL kategóriájú repülőgépek számára. A jövőben ez a rendszer teszi majd lehetővé a repülőgép-anyahajók fedélzetére történő teljesen automatikus leszállást. … Az új technológiának a jövőben érvényesülnie kellene a* (hajó-) *fedélzeti pilóta nélküli eszközöknél is.”*[15] [33]



8. kép F-35B [34]



9. kép Harrier [35]

[13] STOVL- **S**hort **T**ake **O**ff and **V**ertical **L**anding = rövid kifutásra és függőleges leszállásra alkalmas (repülőgép)
[14] JSF- **J**oint **S**trike **F**ighter = Közös Csapásmérő Vadászrepülőgép
[15] az idézetet magyar nyelvre fordította: KB

A bizony már eléggé „öregecskedő” Harrierek tehát még mindig kitűnő szolgálatot teljesítenek. Vészesen közeledő kivonásukkal viszont megszűnik ennek a biztonságos, pilótás-robotos tesztelésnek a lehetősége, mivel **a JSF-ek csak együlésesek**. Nem lesz meg a lehetősége annak, hogy a fedélzeten lévő, a gép minden rezdülését érző-értő ember időben és hatékonyan beavatkozhasson. Pozitívum, hogy emberélet ugyan nem lesz veszélyeztetve, viszont nem lehet „fázisokban” tesztelni – mindennek működnie kell már az első felszálláskor. A tesztek így törvényszerűen elhúzódnak, hiszen egy repülőgép esetleges elvesztése (pl. az F-35B esetében) állam-költségvetési tételt jelenthet… A tesztek „karcsúsítása”, leegyszerűsítése (pl. az állandó időhiány miatt) viszont a rendszer biztonsága ellen dolgozna. A berepülő pilóták különleges státusszal bírnak, óriási tapasztalattal rendelkeznek, az új gépek minden porcikáját ismerik. Egy először felmerülő hiba esetén is a pillanat tört része alatt kell reagálniuk – erre a robotok képtelenek. Hiába sokkal gyorsabbak, ha a programjaikban, memóriájukban nem szereplő új problémát esetleg nem is érzékelik…

6 MIKOR NEM HASZNÁLUNK / NEM HASZNÁLHATUNK ROBOTOKAT?

A fenti fejezetekben ismertetett példák alapján összefoglalom az egyes szempontokat, befolyásoló tényezőket:

- nincs
- van, de nem megfelelő (pl. teljesítmény, védettség, energiaigény)
- az adott terepre nem megfelelő a terepjáró képessége, akadályleküzdő képessége
- drága, üzemelési költségek
- össz- gazdaságosság (+karbantartási költségek, programfejlesztések, stb.)
- élettartam
- hibaszázalék
- az elvégzett munka minősége
- a gép számára megoldhatatlan problémák
- részfeladatokra szabott programokat kellene számára kifejleszteni
- emberek foglalkoztatása
- támogatások rendszere
- társadalmi elfogadottság
- környezetvédelmi szempontok
- károsanyag-kibocsátás ⇔ zárt tér
- taktikai megfontolások
- felderíthetőség (zaj, fény, méretek, más árulkodó jelek)
- engedélyeztetési problémák
- ember felügyelete szükséges
- pszichológiai problémák
- **biztonsági szempontok**

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Már ma, úgy a civil-, mint a katonai célú robotfejlesztések Achilles sarkaként jelenik meg a biztonság kérdése. Többkörös / többszintes biztonsági intézkedésekkel kell elérnünk, hogy a gépek, azok vezérlő programjaik, a be- és kikapcsoló gombjaik mindig az emberek felügyelete alatt maradjanak. Az ember viszont ne tudja önhatalmúan kiiktatni az automatikus biztonsági rendszereket. Ameddig felhasználóként, felelősségünk teljes tudatában döntünk a mindenkori önműködő rendszerekről, a hozott „robottörvényeket” betartjuk és betarttatjuk

(természetesen a robotokkal is), békében élhetünk együtt az újabb- és újabb generációs / egyre fejlettebb segítőinkkel.

A profitorientált gazdasági mérlegelések miatt számolni kell a termelés további exportjával, olyan országokba, amelyekben az ipari robotok helyett embereket alkalmaznak. A „civilizációk összecsapása" a másik oldalon azt is eredményezheti, hogy országok – amelyek nem tudják kiaknázni a robothadviselés nyújtotta lehetőségeket – még inkább kiszolgáltatott helyzetbe kerülnek.

Közismert, hogy „tankokkal nem lehet békét csinálni", ezt tovább gondolva: „robotokkal még kevésbé". Az ember kapcsolatépítő- békítő szerepe tehát megmarad, a robotok viszont hatékony segítői lehetnek.

Ember helyett robot? Az eddigieket összegző válaszom: Igen, de sohasem szabad szemünk elől téveszteni: A gépek vannak értünk, és nem mi a gépekért. Nem szabad engednünk, hogy ez bármikor is megforduljon, hogy végső esetben a robotok dönthessenek például a robothadviselés etikai kérdéseiről! => **Robot helyett ember!**

Várhegyi tanár úr az előadásom utáni szünetben félrehívott, és jótékony tanáccsal látott el, mely szerint: Rosszul tettem fel a kérdést, nem emberek és robotok között kell döntenünk, hanem emberek, illetve **robotok ÉS emberek** között… Mindig így legyen!

Hivatkozott irodalom

(Az internetes hivatkozások utolsó letöltési dátuma: 2010. 11. 27.)

[1] K.B. A robothadviselés etikai kérdései I. Harci robotok; 2009. december http://hadmernok.hu/2009_4_koleszar2.pdf

[2] K.B. A robothadviselés etikai kérdései II. Katonai erkölcs; 2010. március http://hadmernok.hu/2010_1_koleszar.pdf

[3] http://robothadviseles.hu/robot10.html

[4] Play film Discovery Communikations, Inc. Corbis-Sygma – MMVI; http://www.youtube.com/watch?v=XZYbP50CG44

[5] Робот СТР-1 / Фото: Специализированный транспортный робот дезактивирует кровлю ЧАЭС http://chornobyl.in.ua/robot-str.html

[6] Sz.n. Bionika; 2010.08.29. http://hu.wikipedia.org/wiki/Bionika

[7] Photo: © Igor Kostin/NOVOSTI - Liquidators on the roof of Reactor 3 http://www.chernobylee.com/articles/chernobyl/interview-with-a-chernobyl-liquidator-sergei-b---part-i.php

[8] (anarki) Újra kell írni a robotika három törvényét; 2009. július 28. http://index.hu/tudomany/2009/07/28/ujra_kell_irni_a_robotika_harom_torvenyet/

[9] Miklósi Ádám: Érzelmet a gépekbe! 2010.09.02. http://hetivalasz.rcom.hu/tudomany/erzelmet-a-gepekbe-21972/

[10] Békés Sándor, dr. Bod Lajos, dr. Bán István és Homonnay Zsombor; Megjelent 1998-ban a Magyar Vadászlap januári számában. http://www.vadasz.info.hu/etika/etikaikodex.html

[11] Pataky I. Címszavak és gondolatok – ismét a katonai etikáról; 2007.6.12. http://www.regiment.hu/hirek/kiadvanyok/uj_honvedsesegi_szemle/cimszavak_es_gondolatok_

[12] Barta BT cég honlapja; Rádió távirányítású fűkaszáló gép; http://www.spider-barta.hu

[13] Photos of Spider in action. 2010.04.27. http://californiaspidermower.com/?page_id=121

[14] Juhász Attila: Mesterséges mesterséges intelligencia; Linuxvilág, 2006.október, Kiskapu Kft, p. 13; http://www.linuxvilag.hu/content/files/cikk/69/cikk_69_13_14.pdf

[15] Sz.n. Apollo-Program / A Hold meghódítása; 2010.11.24. http://hu.wikipedia.org/wiki/Apollo-program

[16] Shatchman N. Exoskeleton Strength; 2004.12.12. Copyright 2004 The New York Times Company; https://www.nytimes.com/2004/12/12/magazine/12EXO.html

[17] (Bharat) Raytheon's Sarcos XOS 2 military exoskeleton adds superhuman powers / Raytheon Sarcos XOS 2 exoskeleton Picture Gallery 2010.09.29 http://www.gizmowatch.com/entry/raytheons-sarcos-xos-2-military-exoskeleton-adds-superhuman-powers/

[18] gd: Lockheed Martin HULC robotic exoskeleton will operate longer; 2010.01.22. http://www.robaid.com/bionics/lockheed-martin-hulc-robotic-exoskeleton-will-operate-longer.htm

[19] Idegen szavak és kifejezések szótára, Szalay Könyvkiadó Kisújszállás ISBN 963 237 203 8; p. 95

[20] U.o. p. 238

[21] U.o. p. 287

[22] Sz.n. A tachográfrendelet változásai; SatNet Kft. ©; 2006.06.15. http://www.cegesauto.hu/cikk/54

[23] Lukáš Visingr: Turbovrtulové bojové letouny na vzestupu (Turbólégcsavaros harci repülőgépek emelkedőben/terjedőben); ATM/Praha, ISSN 1802-4823; 9/2009 p. 45

[24] (Aleks) Cessna AC-208B Combat Caravan – Iraqi Air Force (IqAF) Sobchak Security; 2010.04.15. http://sobchak.wordpress.com/2010/03/15/ac-208b-combat-caravan-iraqi-air-force/

[25] The Aviation Forum; (Grey Area) 2010.08.11. http://forum.keypublishing.com/showthread.php?t=102501

[26] Hans-Joachim Ruff-Stahl: Der menschliche Faktor im zukünftigen Kriegsbild; Strategie und Technik, Juni 2008; p. 46

[27] Dr. Munk Sándor: Helyzetismeret-bázisok a katonai vezetésben, helyzetinformációk gyűjtése és feldolgozása. Tanulmánygyűjtemény, válogatás a HM 2001. évi kutatási eredményeit összegző tanulmányokból, pályázatokból, Budapest, ISBN 963 7037 44 6, p. 151

[28] Sz.n. Hibázott a GPS, eltévedt a mentő, meghalt a beteg; 2010.10.08. http://www.hirado.hu/Hirek/2010/10/08/20/Tevedett_a_GPS_eltevedt_a_mento_meghalt_a.aspx

[29] Pogácsás Imre: A pilóta nélküli repülőeszközök, avagy egyenes út a robothadviselésig? Repüléstudományi közlemények 2008/2

http://www.szrfk.hu/rtk/folyoirat/2008_2/2008_2_Pogacsas_Imre.html

[30] Hajdú Ferenc: Kiberháború; Élet és Tudomány 2010/43, ISSN 0013-6077, p. 1347

[31] Huntington, Samuel P. A civilizációk összecsapása és a világrend átalakulása, Európa Könyvkiadó Kft. 2005 ISBN 963-07-7665-0

[32] Clément Ruffier: Francia robot – kínai munkás; A szerző, Clément Ruffier, szociológus. A szöveg egy szociológiai és társadalomtudományi doktori értekezés kivonata, melynek címe: Sociologie de la carriere des objets techniques – Le cas du camion dans le transfert de techniques entre la France et la Chine (A műszaki tárgyak útjának szociológiája – A teherautó esete a Franciaország és Kína közti technológia-transzferrel). Lyon, 2008. Fordította: Sipos János és Huszein Evin

http://www.magyardiplo.hu/index.php?option=com_content&view=article&id=153:francia-robot-kinai-munkas&catid=52:2010-januar&Itemid=28

[33] Keijsper Gérard: Harrier pro JSF (46-48) přel. Soušek Tomáš ATM 2010/4, pp. 46-48, Aeromedia Praha, ISSN 1802-4823

[34] Diaz Jesus: The History Behind the F35-B Vertical Lift: from Napkin to First Supersonic Plane, 2008.04.22. http://gizmodo.com/382151/the-history-behind-the-f+35b-vertical-lift-from-napkin-to-first-supersonic-plane

[35] Vic Flintham: Hawker Harrier; XW175, the second development T Mk 2 http://www.boland-devries.nl/dinkies/_reals/harrier.htm

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Kovács László
kovacs.laszlo@zmne.hu

Sipos Marianna
sipos.marianna@zmne.hu

A STUXNET ÉS AMI MÖGÖTTE VAN:
TÉNYEK ÉS A CYBERHÁBORÚ HAJNALA[1]

Absztrakt

A Stuxnet nevű féreg hatalmas riadalmat okozott 2010 nyarán illetve kora őszén. A riadalom oka elsősorban az volt, hogy ez volt az első olyan rosszindulatú program, amely ipari létesítmények vezérlő szoftvereit támadta meg. Jelen írás nagyon röviden bemutatja magát a Stuxnet-et, és elemzi azokat a várható hatásokat, amelyek az információbiztonságban e féreg után felmerülhetnek. Az írás következő részében (a Hadmérnök következő számában) a komplex információbiztonság és a kormányzat lehetséges szerepe a védelemben kerül bemutatásra.

A worm called Stuxnet caused great alarm in summer and the early autumn of 2010. The main reason of the panic was that it was the first malicious program, which challenged the software to control industrial plants. This paper briefly describes itself the Stuxnet, and analyze the potential effects that may arise after this worm on the field of information security. The next part of this paper (planned in the next issue) will focus on the complex information security and the role of government on this field.

Kulcsszavak: *Stuxnet, zero-day, információbiztonság, cyberhadviselés, ipar, PLC, folyamatirányítás, SCADA ~ Stuxnet, zero-day, information security, cyberwar, industry, PLC, process controll, SCADA*

[1] Jelen publikáció a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíjának támogatásával készült.

BEVEZETŐ

2010 őszén rendkívül aggasztó hírről adtak tájékoztatást a világsajtó különböző orgánumai. Egy olyan rosszindulatú program gyors terjedéséről érkeztek beszámolók, amelyek nem az egyszerű otthoni felhasználókat vette célba, hanem az elvileg jól őrzött és komoly, nagy biztonsági rendszerekkel rendelkező ipari létesítményeket.

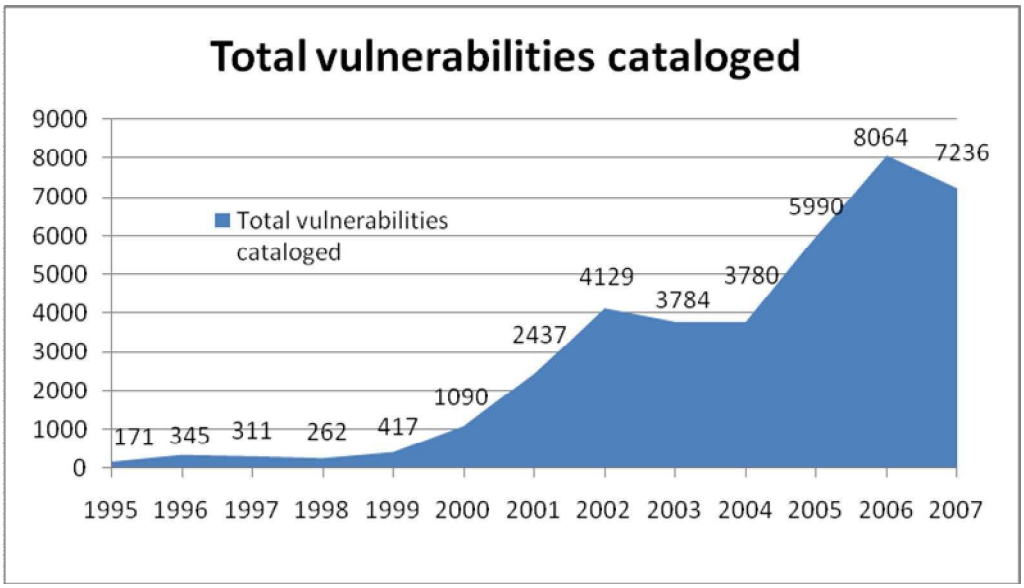
A Stuxnet névre keresztelt féreggel kapcsolatosan nagyon sok találgatás látott napvilágot. E találgatások oka elsősorban e program újdonságában keresendő. A rosszindulatú programok több évtizedes történetében ez az első olyan szoftver, amely nagy tömegben ipari létesítmények vezérlő szoftverei működését támadta.

A találgatások politikai felhangoktól sem voltak mentesek, hiszen a féreg előfordulási gyakorisága és észlelése Iránban volt a legmagasabb. Ez rögtön szemet szúrt a különböző médiumoknak, és rögtön hírül is adták: a féreg célpontja az iráni atomlétesítmények, konkrétan azok működésének leállítása. Ezeket a találgatásokat az informatikai biztonsági cégek elemzései még részben alá is támasztották, hiszen nagyon gyorsan kiderült valóban olyan ipari vezérlő szoftverek ellen készült a Stuxnet, amelyeket Irán is használ pl. a bushehri atomerőműben, vagy a natanzi centrifugáinál.

Jelen írás röviden felvázolja a Stuxnet működését és összetevőit, majd elemzi annak hatásait a különböző szoftverkörnyezetekben. Az elemzés utánajár azoknak a kérdéseknek, amelyek a Stuxnet hatása mögé engednek bepillantást.

A STUXNET

Az elmúlt évtizedekben az informatikai támadások – és ezzel együtt a rosszindulatú szoftverek száma – komoly mértékben nőtt. Természetesen a támadások az addig még nem ismert, vagy nem megfelelően kezelt sérülékenységek ellen irányulnak, illetve ezeket használják ki. [1] Az 1. ábra a CERT Statistics által katalogizált sérülékenységeket mutatja a 1995-től 2007-ig.



1. ábra. A CERT Statistics által katalogizált sérülékenységek 1995-2007-ig [2]

2010 júniusában a VirusBlokAda[2] cég fedezte fel azt a férget, amely a Stuxnet nevet kapta.

Az már a felfedezés utáni első elemzések során kiderült, hogy a Stuxnetet ipari folyamatirányító rendszerek ellen fejlesztették ki. Egészen pontosan a féreg a Siemens SIMATIC WinCC HMI WIMATIC Step7 által felügyelt ipari rendszereket célozta meg. [3] A dolog érdekessége, hogy ezek a szoftverek Windows operációs rendszeren futnak, tehát a Stuxnet Windows szervereken terjedt.

Ha a szerveren nem futott a fenti vezérlők valamelyike, akkor a féreg felvette a kapcsolatot az egyik központi szerverrel, elküldte neki a gép adatait, de ezen kívül ezt a gépet csak továbbterjedésre használta. Ha megtalálta a fenti ipari vezérlő szoftverek valamelyikét, akkor a WinCC adatbázis szoftverhez kapcsolódott annak kódjába előre definiált (hardcoded) default jelszóval.

A Stuxnet végső célja ipari vezérlő rendszerek automatikus folyamatainak újraprogramozása volt. Elsősorban PLC[3] szoftvereket támadott, bár a múltidő használata nem teljesen helyes, hiszen a 2010 őszi események után ma is kapunk híreket a Stuxnetről, illetve annak alkalmazásáról. A WinCC/Step 7 szoftver volt mindezek közül az elsődleges, amelyet a Stuxnet megcélzott. Ez a szoftver adatkábelen keresztül kapcsolódik a PLC-hez és eléri a memória tartalmat, képes folyamatokat újrakonfigurálni, programokat feltölteni és a végrehajtás során rendelkezik bizonyos nyomkövetési funkciókkal is. Ha a PLC már programozásra került, akkor lekapcsolható róla, és a PLC már önmagában is képes a működésre. A Stuxnet e szoftver segítségével juttatta be kódblokkjait a PLC-be, majd ezeket el is rejtette.

A cél a működés szabotázsa volt, valamint az, hogy hosszú ideig lehetőleg ne fedezzék fel. Ez fél-, egyes források szerint egy évig sikerült is, miközben az eredeti Stuxnet-et továbbfejlesztették. Különböző források szerint a 2009. júniusi megjelenés tűnik a legvalószínűbbnek, ugyanakkor a Kaspersky 2009. júliusi, míg a Symantec 2010. januárról beszél. [3] [4]

A közvéleményt foglalkoztató kérdések mellett számos szakmai kérdés is felmerült. Mi az, amiben a Stuxnet féreg túlmutat az eddigi támadásokon? Miért foglalkozik vele ilyen szinten a média? Miben különleges a Stuxnet támadása az eddigi incidensekhez képest? Jelentheti ez a hadviselés egy új ágának megszületését?

A 2. ábra a nemzetközi sajtó féreggel kapcsolatos megnyilvánulásait mutatja, hiszen a világ különböző országainak közismert, hitelesnek elfogadott újságai, hírforrásai kiemelten foglalkoztak a témával.

A szakmai elemzőket – legyenek azok biztonságpolitikával, vagy akár informatikával, illetve információbiztonsággal foglalkozók – szintén felvillanyozta a Stuxnet megjelenése.

Az egyik hazai biztonságpolitikai portálon Berzsenyi Dániel és Szentgáli Gergely elemzésükben a következőket mondják: „A 2010-es év és a Stuxnet felbukkanása új mérföldkővé válhat a virtuális világ hackerek dominálta szegmensének történelmében.” [3]

---

[2] A VirusBlokAda céget 1997-ben alapították Fehéroroszországban. Alapvető tevékenységi köre a víruskereső szoftverek gyártása, illetve az ehhez kapcsolódó szoftverelemző és értékelő munka. Honlapjuk szerint a Vba32 nevű terméküket sikeresen alkalmazzák a Belarusz Köztársaság Nemzeti Bankjában, illetve számos fehérorosz szervezetnél és vállalkozásnál. A Stuxnet felfedezése meghozta a világhírt is a cégnek. [16]

[3] A PLC - Programmable Logic Controller, azaz programozható logikai vezérlő. PLC-ket nagy számban az ipari szabályozástechnikában, a különböző villamos, illetve az ilyen módon működtetett folyamatok irányításában használják. Ezeket az ipari folyamatokat – pl. szerszámgépek, vagy gyártósorok vezérlése – a PLC-ket megelőzően logikai hálózattal, vagy relés rendszerekkel oldották meg. Ezek egyik igen komoly hátránya az volt, hogy sok alkatrészből álltak, hibakeresésük bonyolult, valamint fejlesztési igény esetén módosításuk nehézkes volt. A PLC-k szabványosított be- és kimenettel rendelkeznek. Kompakt felépítésük, valamint az említett szabványosítás lehetővé teszi az egyszerű szabályozási rendszer megépítését, valamint az üzembiztos működést, és a program módosításával a szabályozás későbbi megváltoztatását is.

A Symantec informatikai biztonsági elemzője, O Murchu jelentette ki: „Soha nem láttunk ilyet eddig”, és ehhez a kijelentéshez csatlakozott a Kaspersky is, hiszen az ő elemzéseikben és rosszindulatú szoftverek elleni munkájukban sem találkoztak még ehhez hasonlóval. [4]



2. ábra. Stuxnet a médiában.

A 4 zero day exploit és más módszerek

A Stuxnet nem úgy működik, mint egy szokásos kártékony program. Nem lop személyes adatokat, nem használja a hitelkártyák információit, nem nyúl a bankszámlákhoz, nem teszi tönkre a fertőzött gépek szoftvereit és hardverjét. Nem fenyeget a DoS támadással, mint egy bűnszervezet, váltságdíjat követelve. A Stuxnet magára a szabotázsra készült, titokban terjedve. [5]

A Stuxnet felfedezői és első elemzői megdöbbenve tapasztalták: a féreg négy, eddig még fel nem fedezett biztonsági hiányosságot, azaz sebezhetőséget használ ki. „4 zero-day-t használ, ez valóban, igazi őrület” állítja O Murchu. [4] „Hihetetlen, a Stuxnet 4 zero-day sérülékenységet használ ki, ami példa nélkül álló” áll a Symantec biztonsági jelentésében. [6]

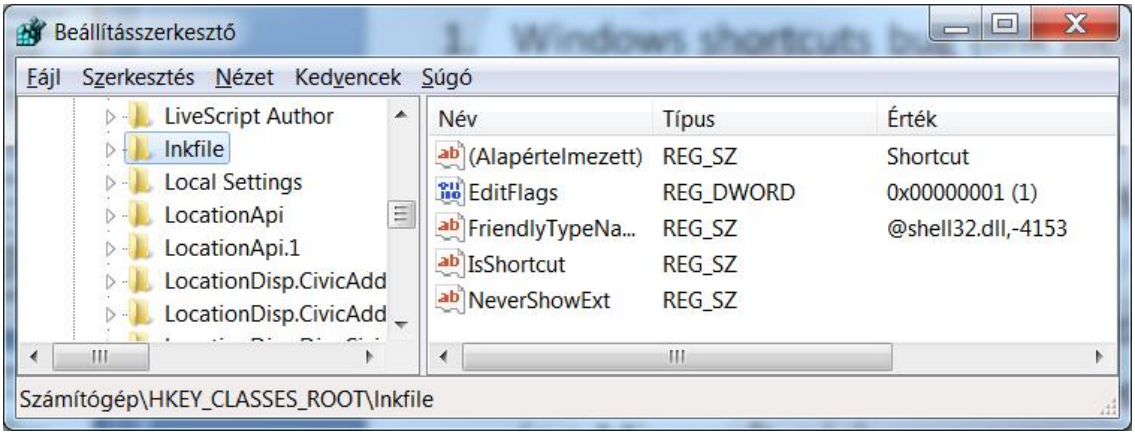
A Zero-day bug, azaz a nulladik napi támadás javítatlan (unpatched) biztonsági rést jelent. A kifejezést azokra a számítógépes biztonsági fenyegetésekre (hibákra) használják a szakemberek, amelyek egy adott számítógépes alkalmazás még felfedezetlen, nem publikált sebezhetőségét jelentik. Egy rosszindulatú program jellemzően egy zero-day bug-ot használ ki, hisz egy újonnan felfedezett sérülékenység önmagában is jelentős érték, mivel rendkívül bonyolult a felfedezése. Természetesen a szoftvergyártók igyekeznek biztonsági rések nélkül létrehozni programjaikat és a felfedezett sérülékenységet minél előbb egy javító csomaggal megszüntetni. Általában egyetlen zero-day bug is komoly veszélyt jelent, hisz a megtámadott alkalmazás készítőjének nincs tudomása e sérülékenységről, vagy még nem sikerült javítást készíteni hozzá, tehát még nincs védelem ellene.

A Stuxnetben a következő 4 zero-day bug-ot fedezték fel:

1. Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (BID 41732) CVE-2010-2568: [7]

Ez egy Windows shortcuts bug, melyet szokás link fájlnak is nevezni, mert a fájlok kiterjesztése .lnk, és a megjelenített ikonhoz csatolja, linkeli az alkalmazást, vagy a mappát. Használható helyi fájlok vagy URL-ek gyors eléréséhez. Mindkét esetben egy meggörbült nyíl ikon látható a hivatkozás ikonjának bal alsó sarkában, és nem szerepel a kiterjesztés a név mögött. Ez a kiterjesztés rejtve marad a Windows Explorer felhasználói számára, még akkor is, ha az ismert fájlok kiterjesztésének elrejtése opciót kivesszük a megjelenítésből, mivel elrejtését, amint azt a 3. ábrán láthatjuk, a registryben a HKEY_CLASSES_ROOT\lnkfile mappa NeverShowExt tulajdonsága vezérli. Az IsShortcut tulajdonság váltja ki a bal alsó sarokban a görbült nyíl ikon megjelenítését. Ezt a technikát használja ki a féreg az USB-ről a számítógépre való feljutáshoz.

2. Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (BID 43073): [8]
   Nyomtató puffer szolgáltatás távoli kód végrehajtással. Ennek segítségével másolta át magát a fertőzött gépről egy másikra. Ez a sérülékenység teszi lehetővé, hogy egy fájlt írhassunk a még tiszta kapcsolódó gép %System% könyvtárába.
3. Windows Win32k.sys Local Privilege Escalation vulnerability (MS10-073): [15]
   EoP (elevation of privilege) bug, vagy local privilege escalation vulnerability, magasabb hozzáférési szint engedélyezés. A sérülékenység a Windows Kernel-Mode meghajtóinál engedélyezheti a magasabb hozzáférést.
4. Egy további EoP bug: [4]

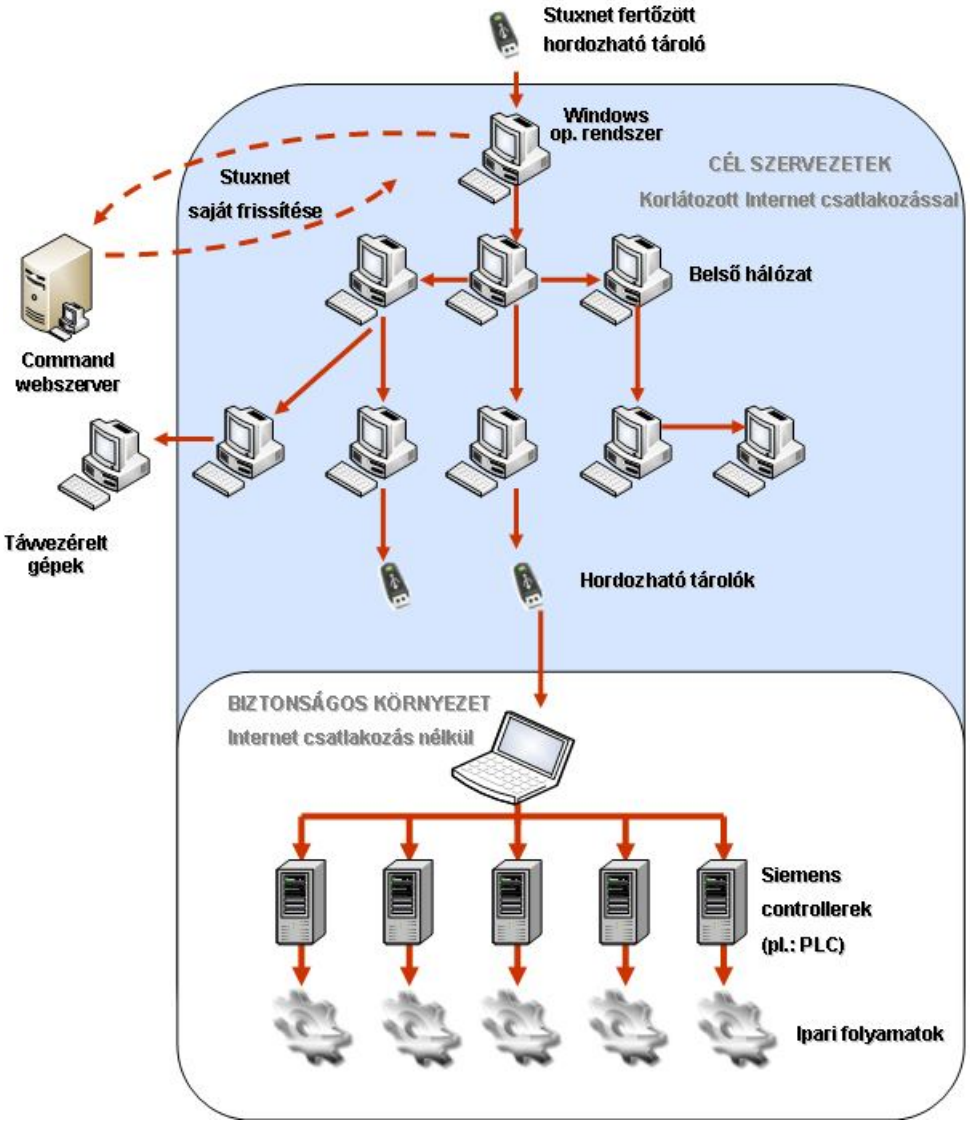


3. ábra. Link fájlok beállításai a registryben.

Ezen kívül a Stuxnet használta még a Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874) sérülékenységet, melyet az a notorious Conficker féreg is használt, amely 2008-2009 fordulóján gépek millióit fertőzte meg. A Panda Security a Global ThreatWatch oldalán narancsjelzésűre minősítette, amely azt jelenti, hogy figyelemre méltó veszélyt jelent. [9] [10] [11]

Ugyanakkor érdemes megjegyezni, hogy ezt a sérülékenységet már 2008.október 23-án az MS08-067 „an emergency pach" frissítésében javította a Microsoft. [12]

Mindezeken túl a féreg kihasznált egy eddig – szintén – felderítetlen sérülékenységet a Siemens felügyelő szoftverben. Mindezeken túl legalább két lopott digitális aláírással rendelkezett, így legitimnek tűnt.



4. ábra. A Stuxnet terjedése a belső hálózaton [17]

A Stuxnet működése

A féreg másolatot készített saját magáról és létrehozta az .lnk fájlokat is, amelyek erre a másolatra mutatnak. Amikor egy alkalmazás, amely ikonokat tud megjeleníteni, pl. a Windows Explorer böngészi a meghajtót, a link fájl futtatja a férget. Ezzel a módszerrel USB-n keresztül terjed, tehát fertőzött USB-vel a zárt hálózatra is feltelepül. Mint tudjuk a zárt hálózatok szoftvereinek karbantartását többnyire USB-k segítségével oldják meg.

Az USB-t használó rosszindulatú szoftverek leggyakrabban az AutoRun funkciót felhasználva jutnak a számítógépre. Természetesen javasolt ennek a funkciónak a kikapcsolása védett rendszerek esetén, ennek ellenére a Stuxnet így is terjedhetett. [14]

Kikapcsolt AutoRun esetén a link fájlok futtatási funkciójában felfedezett 1. zero-day bugot kihasználva jutott fel az USB meghajtóról a számítógépre. A hálózaton a 2. zero-day bug segítségével terjedt tovább.

A fertőzött USB a következő fájlokat tartalmazta:

- Négy darab .lnk fájlt:
  - Copy of Shortcut to.lnk;
  - Copy of Copy of Shortcut to.lnk;

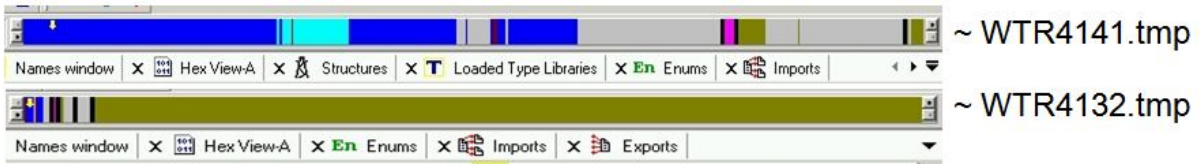
    - Copy of Copy of Copy of Shortcut to.lnk;
    - Copy of Copy of Copy of Copy of Shortcut to.lnk;
- valamint a következő valójában dll fájlokat:
    - ~WTR4141.tmp (~25Kb);
    - ~WTR4132.tmp (~500Kb).

Ezen fájlok nevei rögzítettek a kódban (hardcoded). Amikor egy ikonokat megjeleníteni tudó alkalmazás futni kezd, a féreg .lnk fájljai az ikonok megjelenítése helyett a ~WTR4141.tmp kódját hajtják végre ezzel átadva a vezérlést a féregnek.

A kisebb .dll feladata a nagyobb betöltése, de előtte még elrejti saját magát úgy, hogy a kernel32.dll és az ntdll.dll fájlkezelő függvényeiben beállítja, hogy az '.lnk'-ra végződő és a '~WTR'-el kezdődő valamint '.tmp'-re végződő fájlokat ne mutassa meg. Tehát minden ilyen fájlt elrejt. [13] Emiatt rögzítettek (hardcoded) a fájlnevek.

Ezután a kisebb .dll betölti a nagyobb .dll-t a memóriába, de nem a LoadLibrary API felhasználásával, ahogyan a szokott módon a .dll-ek betöltődnek, hiszen normál esetben a LoadLibrary kivételt dobna, mivel nem találná meg a betöltendő fájlokat, amiket a Stuxnet már elrejtett. Az Ntdll.dll figyeli a LoadLibrary-t és speciális fájlnév hívásakor átveszi az irányítást. [14]

Az 5. ábrán láthatjuk a két dll fájl szerkezetét. Az első, kisebb méretű fájl kis fehér nyíllal jelzett kék területe a kód, itt ez a nagyobb méretű, míg a második .dll-ben a khaki színű adatszegmens a nagy terület, hisz ez tartalmazza a kódolt valódi férget. A 2. dll kisméretű kódszegmense szinte csak a kicsomagolás kódját tartalmazza.



5. ábra. A dll fájlok szerkezete, kék a kódszegmens, khaki az adatszegmens.

A ~WTR4132.tmp a betöltés után átveszi a vezérlést és kicsomagolja a memóriába a valódi támadást végző dll fájlt.

A féreg az operációs rendszer típusának és verziójának ellenőrzése után megnyitott egy rejtett ablakot, az ablak osztályának neve: 'AFX64c313'. Ez az ablak arra várt, hogy egy USB drivert tegyenek a gépbe. Mielőtt megfertőzte volna az új USB-t, leellenőrizte, hogy az aktuális dátum még ne legyen 2012. június 24. A fertőzés nem lehetett 21 napnál régebbi; a meghajtón legalább 5 MB szabad helynek kellett lennie; valamint a meghajtón legalább 3 fájlnak már fent kellett lennie …

A Stuxnet ha internet elérést talált, külső szerverekhez kapcsolódott. A fertőzés elején ezek a szerverek a www.mypremierfutbol.com Malaysiai és a www.todaysfutbol.com Dániai szerverek voltak, de időközben változtak. A féreg külső szerverekhez kapcsolódva frissíteni is tudta magát, és peer-to-peer frissülésre is képes volt. Peer-to-peer frissülésnek ebben az esetben azt a folyamatot hívjuk, amikor két vírus találkozásakor a frissebb él tovább.

A Stuxnet terjedése során ellenőrizte a gépre telepített vírusellenőrző programokat és a gépen található vírusirtó szoftvertől függően választotta ki, mely engedéllyel rendelkező futó folyamatba injektálja be magát, ráadásul további, már futó folyamatba is át tudta magát injektálni. [13]

Amint a féreg aktívvá vált a gépen, első feladata saját fájljainak elrejtése volt. Bizonyos feltételek esetén, ha már fertőzött volt az adott USB meghajtó, akkor letörölte a féreg saját magát. Ugyanez igaz volt abban az esetben is, ha az USB meghajtó már további 3 gépet is

megfertőzött, azaz a Stuxnet ebben az esetben is letörölte magát. Az utóbbi két technikával jelentősen csökkentette a felfedezésének esélyét. [14]

A Stuxnet, amint azt korábban említettük 2012. június 24 után nem fertőz tovább. [14]

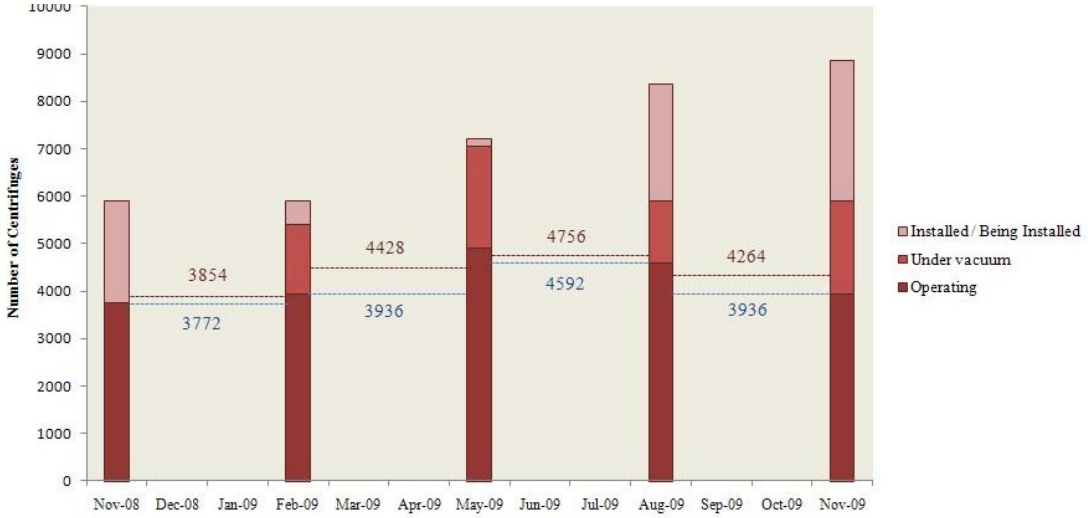
AMI A STUXNET MÖGÖTT VAN

Jelen írás is számos olyan kérdésnek adott hangot, amely a Stuxnet valódi céljait vagy akár létrehozóit érintette, mindazokon túl, hogy nagy vonalakban ismertette a féreg felépítését és működését.

Bruce Schneier információbiztonsági guru szerint a Stuxnetet létrehozni meglehetősen drága munka volt. Becslések szerint 8-10 nagyon jól képzett programozó, minimum hat hónapos munkája van benne. Ezen kívül ott van még a tesztelés kérdése is, amely csak egy jól felépített laborban történhetett, hiszen ez elengedhetetlen lehetett a féreg útjára bocsátása előtt. A zero-day exploitok kérdése is érdekes, hiszen ezek közül egy is komoly értéket képvisel. Akárki is írta a Stuxnetet – mondja Schneier –, egy csomó pénzt volt hajlandó költeni rá. [18]

2011 januárjában a New York Times (NYT) adott elsőként hivatalosan hírt arról, hogy a Stuxnet mögött Izrael áll, hiszen mindezidáig a féreg forrásáról csak feltételezések és találgatások léteztek. A NYT cikke összhangban áll Schneier előbb idézett véleményével, hiszen a cikk szakértőkre hivatkozva szintén megemlíti, hogy a férget olyan ipari létesítményben kellett tesztelni, mint a későbbi célpontok. Ez a létesítmény pedig nem más, mint az izraeli Negev sivatagban lévő Dimona komplexum, amely köztudottan az izraeli nukleáris kutatás központja. Itt tesztelték és próbálták ki az urándúsítás elengedhetetlen kellékein, az izotópcentrifugákon, illetve ezek irányító szoftverein a Stuxnetet. A cikk kitér arra is, hogy Hillary Clinton és a nemrég nyugdíjba vonult Moszad vezető, Meir Dagan egymástól függetlenül, de nagyjából azonos időben kijelentették: remélik az események az iráni atomprogramot akár több évvel is visszavetik. Ez természetesen arra is következtetni enged, hogy az akció nemcsak Izrael magánakciója volt, hanem az USA is hathatósan közreműködött. [19]

Ezzel összefüggésben érdekes összehasonlító adatsor jelent meg a Federation of American Scientists egyik oldalán. E szerint a működő iráni centrifugák száma jelentősen visszaesett 2009 novemberére. (6. ábra) [20] [21] [22]



6. ábra. Az iráni izotópcentrifugák számának alakulása a Stuxnet terjedése idején. [20]

Az események során a média hatalmas érdeklődése szinte nyilvánvaló volt, hiszen a Stuxnet, pontosabban annak veszélyessége miatt rendkívül sok egyéb kérdés is felmerült.

Gyakran elhangzott a kérdés: most kezdődött az információs háború kora? Erre a kérdésre azonban nem egyértelmű a válasz. A cyberhadviselés első és igen komoly – akár az olyan nemzetközi politikai vagy katonai szervezetet, mint a NATO-t is komolyan érintő – eseménye a 2007-es észtországi konfliktus volt. Már akkor számos olyan kérdés vetődött fel, amelyekre azóta sem igen kaptunk választ.

Ezekre a kérdésekre keresi a választ jelen írás következő része, amely többek között a komplex információbiztonság szerepét, valamint az állam ezen a téren megvalósítandó feladatait tervezi elemezni.

2011. február elején, az immár 47-ik alkalommal megrendezésre kerülő Munich Security Conference különös aktualitást ad ezeknek a kérdéseknek. A konferencián, amelyen államfői, illetve külügyminiszteri szinten képviselteti magát sok vezető hatalom (pl. az USA, Nagy-Britannia, Oroszország, Németország), első ízben kerül sor nagyhatalmak részéről annak tisztázására, hogy hol kezdődik a háború a cybertérben. Ezen kívül a program kitér arra is, hogy meg kell teremteni a cybertérben is a genfi, illetve a hágai egyezményekhez hasonlóan a cyberhadviselés szabályait. [23]

(*Folytatjuk ...*)

IRODALMI HIVATKOZÁSOK

[1] A. Householder, K. Houle, C. Dougherty: Computer Attack Trends Challenge Internet Security. Computer magazine, IEEE Computer Society (2002 April) pp. 5-7. http://csdl2.computer.org/comp/mags/co/2002/04/r4s05.pdf

[2] CERT Statistics. http://www.cert.org/stats/#vuls

[3] Berzsenyi D, Szentgáli G.: STUXNET: a virtuális háború hajnala. http://www.biztonsagpolitika.hu/?id=16&aid=932&title=STUXNET:_a_virtu%C3%A1lis_h%C3%A1bor%C3%BA_hajnala (2010. október 7)

[4] G. Keizer: Is Stuxnet the ’best’ malware ever? http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_?

[5] B. Schneier: *Schneier on Security, Stuxnet*, http://www.schneier.com/blog/archives/2010/10/stuxnet.html

[6] W32.Stuxnet, Symantec Security Response, http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-071400-3123-99&tabid=2

[7] Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (bugtraq ID 41732), (CVE-2010-2568) Security Focus, http://www.securityfocus.com/bid/41732, Published: Jul 15 2010, Updated: Aug 11 2010, Detected: VirusBlokAda.

[8] Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (BID 43073). Security Focus, http://www.securityfocus.com/bid/43073, Published: Sep 14 2010, Updated: Sep 27 2010, Detected: Microsoft.

[9] Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874), Security Focus, http://www.securityfocus.com/bid/31874, Published: Okt 22 2008, Updated: Feb 9 2009, Detected: Microsoft

[10] G. Keizer: 'Huge increase' in worm attacks plagues unpatched Windows PCs, Computerword, http://www.computerworld.com/, Computerword Inctitute, (2009. January 12.) http://www.computerworld.com/s/article/9125737/_Huge_increase_in_worm_attacks_plagues_unpatched_Windows_PCs

[11] Global ThreatWatch, http://www.pandasecurity.com/homeusers/security-info/gtw/ Panda Security Press, http://press.pandasecurity.com/

[12] Microsoft Security Bulletin MS08-067 – Critical Vulnerability in Server Service Could Allow Remote Code Execution (958644), TechNet, http://www.microsoft.com/technet Microsoft Corporation http://www.microsoft.com (2008. October 23.) http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

[13] N. Falliere, L. O Morchu, E. Chien: Win32.Stuxnet Dossier, Symantec Security Response, Symantec AntiVirus Research Center, (Nov. 2010) http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[14] L. O Murchu: W32.Stuxnet Installation Details, Symantec blogs, http://www.symantec.com/connect/blogs/w32stuxnet-installation-details

[15] Microsoft Security Bulletin MS10-073 – Important, Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957), (2010, October 12.) http://www.microsoft.com/technet/security/bulletin/ms10-073.mspx

[16] http://www.anti-virus.by/en/index.shtml

[17] http://www.nytimes.com/ imagepages/2011/01/16/world/16stuxnet_g.html?ref=middleeast

[18] Schneier on Security. A blog covering security and security technology. Stuxnet. http://www.schneier.com/blog/archives/2010/10/stuxnet.html

[19] W. J. Broad, J. Markoff, D. E. Sanger: Israeli Test on Worm Called Crucial in Iran Nuclear Delay. In: New York Times, 2011. január 15. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&scp=2&sq=stuxnet&st=cse

[20] http://www.fas.org/blog/ssp/wp-content/uploads/NumberCentrifuges1.jpg

[21] Kim Zettes: Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage. In: Wired, 2010.november 15. http://www.wired.com/threatlevel/2010/11/stuxnet-clues/

[22] Mit buherál a Stuxnet? http://buhera.blog.hu/2010/11/14/mit_buheral_a_stuxnet

[23] Munich Security Conference (Münchener Sicherheitskonferenz) http://www.securityconference.de/

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Kun István
kunistvan47@gmail.com

Szász Gábor
szaszg@gdf.hu

INFORMÁCIÓVESZTÉS ADATVESZTÉS NÉLKÜL

Absztrakt

Az információbiztonság nemcsak az adatok biztonságát igényli, hanem az adatfrissítés és adatértelmezés adekvátságának megőrzését is változó körülmények közepette. Az információvá transzformálást nemcsak az illetékes szakértők, hanem az erőforrásokat végső soron biztosító laikus köznép is elvégzi sajátos szempontjai szerint. Ha a kockázati eseménnyel kapcsolatos döntések során nincsenek tekintettel erre a körülményre, akkor nem várható optimális eredmény.
A kockázat laikus és szakértői megítélése az idő emberi érzékelését leíró pszichológiai törvényen alapszik. Ez a megközelítés alkalmas a laikusok veszélyérzetének jellemzésére, ha a kockázati esemény várhatóan bekövetkezik valamikor a jövőben. A laikusok véleményét figyelembe vevő döntéseknek, amelyek gyakoriak a demokratikus társadalmakban, ilyen jellegű ismereteken kell alapulniuk. Az elméleti modellt alátámasztják azok az adatok, amelyeket egy valóságos közvélemény-kutatásban gyűjtöttek össze. Végezetül egy matematikai modell megmutatja a laikus és szakértői vélemények közötti konfliktus kialakulásának valószínűségét.

Information security needs not only the security of data but also the preservation of the adequacy of data updating and data interpretation among variable circumstances. Transforming data into information is carried out not only by competent experts but also by laymen finally ensuring resources, according to their special points of view. If risk decisions do not observe this fact, then no optimal result can be expected.
Lay and expert judgement of risk is studied based on the empirical psychological law of human perception of time. This approach is appropriate for the characterisation of laymen's feeling of danger for a risk event due to occur some time in the near or distant future. Decisions considering laymen's opinion, frequent in democratic societies, must rely on this kind of knowledge. The theoretical model is supported by the data collected in a real poll. Finally,

a model is given to compute the probability of a conflict between lay and expert opinions.

Kulcsszavak: *kockázatbecslés, szubjektív időérzékelés, adatok elavulása, véleménykonfliktus modellezése ~ risk estimation, subjective perception of time, obsolescence of data, modelling conflict of opinions*

BEVEZETÉS

Az informatikai biztonság problémakörének egyik alapvető területe az információvesztés, amely a tudást reprezentáló adatbázisokat fenyegető egyik legfőbb veszély. Az információvesztést általában az információt hordozó adatok elvesztéséhez, vagyis hozzáférhetetlenné válásához kapcsoljuk. Az ilyen adatvesztés az információs rendszer hardver és/vagy szoftver eredetű meghibásodásának következménye.

Az információvesztés azonban más módon is bekövetkezhet: az adatok hozzáférhetők maradnak, de a bennük rejlő információ használhatatlanná válik. Ennek oka pedig a konfliktus valamilyen egyéb eredetű, de ugyanarra vonatkozó, lényegesen eltérő következtetésre módot adó információval. Ilyen konfliktushelyzet keletkezik például az alábbi esetekben:

- a laikus közvélemény helyesen működő veszélyérzete ellentmond a szakemberek véleményének;
- valamilyen közönséges rémhír eltorzítja a laikusok veszélyérzetét;
- a felhalmozott tapasztalatok a körülmények megváltozása miatt érvényüket vesztik.

Mivel pedig autentikusnak tekintett, komoly következményekkel járó döntéseket megalapozó információk degradálásáról, erkölcsi lenullázásáról van szó, ez a jelenség súlyos biztonsági kérdéseket vet fel. A cikkben ennek a jelenségnek a matematikai modellezésével foglalkozunk.

A problémát felismerve a magyar hidrológusok lépéseket tettek a laikusok bevonására a döntéselőkészítő folyamatba. Például nemzetközi konferenciát szenteltek ennek az új megközelítésnek, lásd (Gayer, 1999). A közvélemény áldozatvállalási hajlandósága a hatalmas anyagi terhekkel járó árvízvédelmi beruházásoknál a tervezés fontos részévé válik. És nem utolsó sorban a laikusok kockázat-megítélése bizonyos esetekben reálisabb a szakemberekénél.

Miközben tárolt adatainkat biztonságban tudjuk, mégis veszíthetünk információt, ha a körülmények megváltozása miatt azok az ismérvek, amelyek aktuális értékei a tárolt adatok, elveszítik relevanciájukat. Az információ ugyanis – szűkebb, antropomorf értelemben – a tudati reprezentáción a jelentéssel végrehajtott transzformáció eredménye, azaz az agy terméke. A mentális reprezentáció és a jelentéssel végzett transzformáció egyaránt eltér a szakértőknél és a laikusoknál. A katonai és a civil biztonság területén egyre fontosabbá válik a szakértői és a laikus információmódosulás eltérő véleményben megnyilvánuló konfliktusának kezelése, a konfliktus valószínűségének becslése. Közismert, hogy egy-egy háborút nemcsak a harctéren lehet elveszíteni, hanem a lakosság megváltozott véleménye miatt a hátországban is. Most azzal nem foglalkozunk, hogy az egyes háborúk kimenetele történelmileg progresszív volt-e, és ebben a katonai szakértők, avagy a lakosság álláspontja tekinthető-e helyesnek. Éppen ezért példáinkat a civil biztonság – remélhetőleg érdeksemleges – területéről vesszük.

Tömegjelenségek esetében, amikor a körülmények hosszabb távon kevéssé változnak, az összegyűjtött tapasztalatokon alapuló szakértői vélemények alkalmazása teljesen helyénvaló. A helyzet azonban teljesen más extrém eseményeknél, ahol maga az extrémitás kérdőjelezi meg az ismétlődő események megfigyelésekor szerzett adatok rendszerezésén alapuló szakértői vélemények látszólagos fölényét.

A Bayes-típusú módszereket széles körben alkalmazzák természeti folyamatok paramétereinek becslésére. A fent említett esetben az ilyen jellegű statisztikai okoskodás nem helyénvaló. Ennek oka az, hogy a Bayes-típusú módszerek a statisztikai becslések fokozatos javításával közelítik a stabil folyamat-paramétereket, és ehhez minden iterációs lépésben új megfigyeléseket használnak. Csakhogy amikor a vizsgált folyamat jellege megváltozik, akkor ezzel együtt a lényeges paraméterek struktúrája is megváltozik, a Bayes-típusú módszerek viszont nem tudják követni az ilyen változásokat. Erre a jelenségre mutat rá (Kun és Szász, 2005).

KOCKÁZATÉRTÉKELÉS

Feltételezzük, hogy a laikusok veszélyérzete illetve biztonságtudata a kockázati esemény első bekövetkezéséig terjedő időintervallum hosszának emberi érzékelésén alapul.

A pszichológiában jól ismert, hogy a szakemberek minden szituációt rögzített, kipróbált, logikailag koherens sémák alkalmazásával értékelnek ki, míg a laikusok laza asszociációkra alapozzák véleményüket. Ugyanakkor azonos kockázati szituációk megítélésében a laikusok fontosabbnak érzik a kockázat térbeli és időbeli inhomogenitását, mint a szakemberek.

Amikor egy laikus értesül egy döntési szituációról, és hallja egy kedvezőtlen esemény gyakoriságára vagy a különböző akciók hatásainak valószínűségében mutatkozó különbségre vonatkozó szakértői véleményt, akkor veszélyérzete a korábban szerzett információktól függően alakul. Az előzetes információ viszont nem függ közvetlenül az objektív valószínűségtől.

A kognitív folyamatok pszichológiai hátterét tárgyalja röviden (Ezhkova, 2004). A szellemi aktivitás dinamikus sztereotípiáinak fogalmát Pavlov (1932) vezette be, és Anohin (1998) valamint Sudakov (2002) tisztázta az előzetes információ szerepének biokémiai alapjait.

Az a tény, hogy a megszerzett információnak a laikusok tudatában rögzült változata függ a korábbi tapasztalatoktól, összhangban van az információ modern felfogásával, amely a legutóbbi 15 évben alakult ki: az információ a valóság belső reprezentációja transzformációjának eredménye, ahol a transzformációt úgy értjük, hogy valamilyen jelentést fűzünk a reprezentációhoz.

A biztonság szintjét a kockázati esemény első bekövetkezéséig eltelő időszakasz hosszával mérjük. (Mivel főleg kis valószínűségű kockázati eseményekkel foglalkozunk, vagyis nem tömegjelenségekkel, ezért elhanyagolhatjuk a kockázati esemény ismételt előfordulását.)

A Fechner-Weber pszichológiai törvény jó közelítést ad az érzékelési szintre, és hasonlóképpen a mennyiségek kognitív reprezentációjára. Ez a törvény jól ismert, klasszikus eredmény.

$$s \cong k \left| \ln \frac{r}{r_0} \right|$$

ahol:

r az inger szintje;
r_0 a pontos érzékelés alsó küszöbszintje;
s az adott inger érzékelt szintje,
k arányossági tényező.

Kockázatbecslési szituációban:

- Ingernek tekintjük a t feltételezett hosszúságú időintervallumot két egymást követő kockázati esemény között. (Pl. egy adott típusú atomerőművi baleset egy adott erőműben minden $t = 10000 = = 10^4$ éves működés alatt, egy másik típusú baleset minden $t = 100000 = 10^5$ éves működés alatt egyszer fordul elő; t_0 egy évet jelent.)
- Válasz a t érték emberi érzékelési szintje, amelyet $s(t)$ jelöl (a példában a biztonságérzet csak 4-ről 5-re növekszik).

A Fechner-Weber törvény alkalmazásával

$$s(t) \cong k \ln \frac{t}{t_0}$$

Ennek alternatív formája:

$$s(t) = \ln t + 1$$

azt fejezi ki, hogy az emberek a jövőbeni kockázatokat „perspektivikus" módon szemlélik. Ez azt jelenti, hogy minél távolabb van időben a kockázati esemény, annál kevésbé aggasztja az embereket. (Az 1 konstans szerepe, hogy biztosítsa az $s(0) = 1$ relációt, amelyet igazol az a tapasztalat, hogy az emberek egy időegységet ténylegesen egyetlen időegységként érzékelnek.)

Az előbbi gondolatmenetet igazolja a „kognitív relativitás" elve (Ezhkova, 2004), amely a következőt állapítja meg az ilyen szituációkra: "Két, különböző helyzetben levő megfigyelő különböző mérési eredményekhez jut, ide értve az időt is. Ez magyarázza az idő érzékelésének relativitását: a különböző életciklusok miatt mindegyik entitásnak saját időérzete van, amelyben az érzékelési különbségeket a tapasztalat alakítja ki."

A mindennapi életben a kockázatelemzés legfontosabb eleme annak eldöntése, hogy a kockázati esemény bekövetkezhet-e egy meghatározott időszakon – nap, hónap, év stb. – belül.

Az időegységet úgy kell ésszerűen megválasztani, hogy az emberek számára legfontosabb időperiódus legyen. Mint (Ezhkova, 2004) rámutat, a laikusok és a szakemberek különbözőképpen választják meg a megfelelőnek tartott időperiódust.

EGY PÉLDA

A Tisza völgye magában foglalja Magyarország mezőgazdasági területének jelentős részét. A vízhozam erős ingadozása (1:600) és az évi csapadék alacsony szintje (400-600 mm/év) a terület vízmegtartó képességében speciális helyzethez vezet. Az Alföldön ugyanabban az évben egyaránt előfordulhat árvíz, belvíz és aszály, amelyek külön-külön is pusztító hatásúak. A vízmegtartó képességnek kellene egyszerre megoldani az árvízvédelmet, a belvíz elvezetését és az öntözést.

A következő táblázat annak az eseménynek az érintett lakosság szerinti valószínűségét tartalmazza, hogy az árvízvédelmi gát magasságát meghaladó vízszint alakul ki (lásd (Vári, 2000)).

	Alsó-Tisza 2.54 öblözet	Felső-Tisza 2.55 öblözet	Felső-Tisza 2.57 öblözet	Teljes minta
25 % alatt	89,2	31,9	59,7	59,4
26 - 50 %	8,5	35,8	17,9	21,3
51 % felett	2,4	32,3	22,4	19,4

Az adatok helyes értelmezéséhez tudnunk kell, hogy a 2.57 öblözetet korábban jóval többször pusztították árvizek, mint a 2.55 öblözetet, bár a táblázat a lakosság félelmét éppen a fordított irányban mutatja.

Ennek oka az, hogy a 2.55 öblözetben az utolsó közvetlen tapasztalat időben jóval közelebbi: 1998 illetve 1970. Az adatok tehát alátámasztják az idő perspektivikus szemléletének elméletét. Abban viszont nincs különbség, hogy az időbeli távolság a múltra vagy a jövőre vonatkozik.

LAIKUS KONTRA SZAKÉRTŐI VÉLEMÉNY

Egy nagy építési projekt – legyen a célja akár árvízvédelem, akár energiatermelés vagy bármi más – mindig tartalmaz egy olyan lépést, amikor a laikus és szakértői véleményeket ütköztetni kell. Súlyos társadalmi feszültségek keletkezhetnek abból, ha a közvéleményt nem győzik meg a projekt ésszerűségéről.

A következőkben egyszerű matematikai modellt írunk fel erre a szituációra. A módszert gyakran használják az alkalmazott megbízhatóság-elméletben, ahol SSI (strength-stress interference, magyarul: igénybevétel–teherbírás átfedés) néven ismert. Az egyik különbség az, hogy a mérnöki gyakorlatban normális eloszlásokat használnak, esetünkben viszont egyenletes eloszlás használata célszerű. A másik pedig az, hogy a sűrűségfüggvények átfedési területe nem a meghibásodás valószínűségével, hanem a konfliktus elkerülhetősége valószínűségével arányos.

A laikus és szakértői vélemények egyaránt szóródnak. Ezt Smith (2002) úgy magyarázza, mint a kognitív folyamat belső természetének, Ezhkova (2004) pedig, mint korábban láttuk, a kognitív relativitásnak a következményét.

Mindkét közösségben különálló csoportok vannak. A vélemények egy csoporton belül rendszerint egy jól meghatározott érték körül koncentrálódnak, de a különböző csoportok véleménycentrumai egymással nincsenek összefüggésben. A csoportok létrejötte az úgynevezett „információs zuhatagok" kialakulásának tulajdonítható: a határozott véleményt képviselő egyének mintául szolgálnak a véleményükben bizonytalanok számára, akik adott esetben akár saját személyes tapasztalataiknak ellentmondó álláspontot is hajlamosak elfogadni. Minél többen fogadtak már el egy véleményt, annál könnyebben csatlakoznak hozzá a bizonytalanok. Ez magyarázza a rémhírek terjedését. Lásd (Bikhchandani *et al*, 1998).

Rendszerint csak általános tendenciák vannak, mégpedig számos tényező alapján, amelyek között a vélemények, megalapozottabb modell hiányában, egyenletes eloszlásúnak tekinthetők. (Ez az ok, amely miatt egyenletes eloszlást használunk, szemben a gépészeti gyakorlattal, ahol sok, önmagában nem számottevő véletlen tényező hatására jön létre a kiválasztott műszaki ismérv tapasztalati értékének természetes szóródása egy elméleti várható érték körül.) Mégis, a szakértői vélemények szóródása általában jóval kisebb, mint a laikus véleményeké.

A problémát a közvélemény szempontjából közelítjük meg. Az egyszerűség kedvéért csak egyetlen fajta kockázati eseményt tételezünk fel. A közvélemény biztonságérzetét most a kockázati esemény első bekövetkeztéig eltelő időszakasz hosszával mérhetjük.

Feltételezzük, hogy ennek az időszakasznak a hosszát illetően számos független vélemény van, amelyek egyenletes eloszlást követnek a $[T_1, T_2]$ intervallumon. A közvélemény ezeket az értékeket a Fechner-Weber törvény szerint érzékeli.

Legyen τ_l az a véletlen változó, amely kifejezi a laikus véleményt. τ_l egyenletes eloszlású a $[T_1, T_2]$ Intervallumon. Valójában viszont τ_l érzékelt nagyságának eloszlását (vagyis logaritmikus transzformáltját) szeretnénk ismerni. Legyen $F_l(T)$ τ_l eloszlásfüggvénye. Akkor

$$F_l(T) = P(1 + \ln \tau_{\cdot} < T) = P(\tau_{\cdot} < e^{T-1}) =$$
$$= \begin{cases} 0 & T < 1 + \ln T_1 \\ \dfrac{e^{T-1} - T_1}{T_2 - T_1} & 1 + \ln T_1 < T < 1 + \ln T_2 \\ 1 & T > 1 + \ln T_2 \end{cases}$$

Hasonló reláció igaz az ugyanazon tárgyra vonatkozó szakértői véleményre. Az utóbbi vélemények – amelyeket a τ_e véletlen változó ír le – szintén egyenletes eloszlásúak a $[T_3, T_4]$ intervallumon, miközben a laikus vélemény esetében a logaritmikus transzformáltat vesszük figyelembe.

A fenti paraméterek ismeretében úgy definiáljuk a C (a *Conflict* rövidítése) véletlen eseményt, hogy a laikus vélemények rövidebb kockázatmentes időszakaszt várnak, mint a szakértői vélemények. Ha $f_e(T)$ jelöli τ_e sűrűségfüggvényét, akkor:

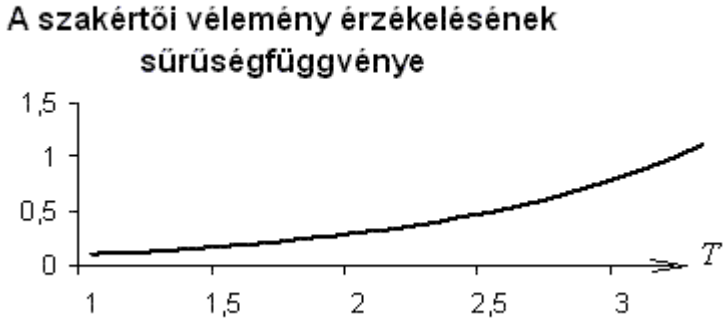
$$P(C) = \int_0^{\infty} F_l(T) f_e(T) dT$$

Az integrál explicit módon kiszámítható, de ez a T_i, $i = 1,\ldots,4$. változók számos lehetséges konstellációja miatt bonyolult diszkussziót igényel.

Ehelyett numerikus szemléltetést adunk a modellről.



1. ábra. A laikus vélemény érzékelésének eloszlásfüggvénye

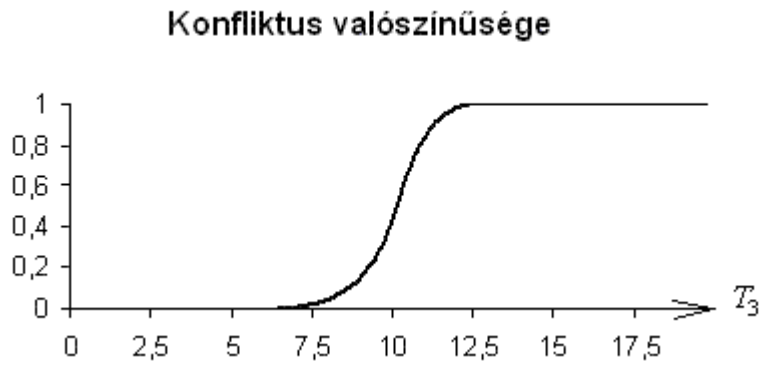


2. ábra. A szakértői vélemény érzékelésének sűrűségfüggvénye

A szakértői vélemények koncentráltabbak (a 0–3,5 intervallumban szóródnak), mint a laikus vélemények (a 7,5–12,5 intervallumban szóródnak).

Most kiszámítjuk $P(C)$ értékét fix T_1 és T_2 esetében, amikor $T_4 - T_3$ úgyszintén fix, de T_3 különböző értékeket vehet fel. Valójában a szakértői vélemények sokkal koncentráltabbak, mint a laikus vélemények, csak a vizuális szemléltetés kedvéért járunk el így. (Válságos helyzetben a szakértői vélemények szóródása megnövekedhet, amikor szakmai viták robbannak ki a stábban. A határozott cselekvés megalapozása érdekében a parancsnoknak kell koncentrálnia a véleményeket. A parancs végrehajtásakor megváltozó körülmények egy marginális vélemény ésszerűségét kidomboríthatják. Ilyenkor a végrehajtó személyes bátorságán múlik a helyes irányú módosítás. A parancs ellenében, de ésszerűen cselekvő katona elismerésére szolgált a Mária Terézia-rendjel.)

Konfliktus-valószínűségek különböző T_3 értékekre:



3. ábra. Konfliktus valószínűsége

Ha van valamilyen elképzelésünk a szakértői és laikus vélemények közelítő értékeiről, akkor megkonstruálhatjuk a fenti ábrákat, vagy kiszámíthatjuk az ábrák alapjául szolgáló függvények számszerű értékeit. Ilyenkor előreláthatjuk a jövőbeni konfliktusok mértéket, és felkészülhetünk a konfliktusok kezelésére.

ÖSSZEFOGLALÁS

Az információbiztonság nemcsak az adatok biztonságát igényli, hanem az adatfrissítés és adatértelmezés adekvátságának megőrzését is változó körülmények közepette. És annak is tudatában kell lennünk, hogy az információvá transzformálást nemcsak az illetékes szakértők, hanem az erőforrásokat végső soron biztosító laikus köznép is elvégzi sajátos szempontjai szerint. Ha a döntéshozók nincsenek tekintettel erre a körülményre, akkor elhatározásaik nem járhatnak optimális eredménnyel.

HIVATKOZÁSOK

1. Anohin, I. (1998): *Cybernetics of Functional Systerms*, Moscow.

2. Benedikt, S., Kun, I., Szász, G. (2004): Individual and Collective Risk Perception in Decision Criteria. Robert Trappl, editor, *Cybernetics and Systems 2004*, University of Vienna and Austrian Society for Cybernetics Studies, Vol. 1: 321-325.

3. Bikhchandani, S., Hirshleifer, D., Welch, I. (1998): Learning from the Behavior of Others: Conformity, Fads, and Informational Cascades. *Journal of Economic Perspectives* 12, No. 3: 151-70.

4. Ezhkova, I. (2004): Notes on Cognitive Relativity, Rationality and Clarity. Robert Trappl, editor, *Cybernetics and Systems 2004*, University of Vienna and Austrian Society for Cybernetics Studies, Vol. 1: 326-331.

5. Gayer, J., ed. (1999): Participatory process in water management (PPWM) *Proceedings of the Satelite Conference to the World Conference on Science* (Budapest, Hungary 28-30 June 1999) Technical Documents in Hydrology, No. 30.

6. Kun, I., Szász, G. (2005): A kockázat entrópia alapú megközelítése. *Informatika*, vol. 8)(2005) No. 1: 44-46.

7. Pavlov, I. (1932): Dynamic Stereotypes. *Proceedings of the 10-th International Congress in Psychology*. August 24, 1932, Copenhagen.

8. Smith, V. (2002): Constructivist and Ecological Rationality in Economics. The Nobel Prize Lecture in Economics, December 8, 2002.

9. Sudakov, K. (2002): *Dynamic Stereotypes*, Moscow, PER SE, 2002.

10. Vári, A. (2000): Risk Evaluation and Willingness to Make Sacrifices in Three Zones of the River Tisza. In: Rozgonyi, T., Tamás, P., Tamási, P., Vári, A. (Eds), *A tiszai árvíz. Vélemények, kockázatok, stratégiák*, MTA Szociológiai Kutatóintézet, , Budapest: 33-64.

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Kuris Zoltán
Zoltan.Kuris@bm.gov.hu

A KOMPLEX INFORMÁCIÓVÉDELEM ÚJ IRÁNYAI A NEMZETI MINŐSÍTETT ADATOK VÉDELMÉVEL ÖSSZEFÜGGÉSBEN

Absztrakt

Jelen közleményben a szerző áttekinti a közelmúltban megjelent minősített adatok kezeléséről szóló törvényt, és a hozzá kapcsolódó három kormányrendeletet, valamint annak hatásait a nemzeti minősített adatok kezelésére. Az elemző értékelés különös figyelemmel vizsgálja a hazai információvédelmi szakma irányelveihez és a nemzetkőzi minősített adatok kezeléséhez fűződő koherenciát. A szerző igyekszik feltárni a szabályozási rendszerben megjelenő anomáliákat és előre jelezni a tovább lépés irányát és lehetőségeit.

In this work, the author analyses the law on the protection of qualified data and the three governmental regulations concerning its execution. The effects of the law on information protection are also analysed. The minor faults and the options of correction are also described as well as the state of domestic information protection. The importance of the formation of the new view and the fact that the event is important for home professional circles are justified, too.

Kulcsszavak: *komplex információbiztonság, minősített adat ~ complex information security, classified information*

BEVEZETÉS

Az információvédelem szakterületén, a közelmúltban történelmi jelentőségű változások következtek be. Hosszú idő után, az Európa Tanács 2002-ben megfogalmazott irányelveivel összhangban 2009. december 14-én az Országgyűlés megalkotta a minősített adat védelméről szóló 2009. évi CLV. törvényt.(a továbbiakban mavtv.) E törvény – az előzőekhez képest – alapjaiban más szemléletmódot tükröz a minősített adatok védelmével összefüggésben. A törvény egységes keretek között szabályozza a nemzeti és a külföldi minősített adatok kezelését. Meghatározza a minősítéssel védhető közérdek fogalmát és tartalmát. Ugyanakkor ezzel összefüggésben bevezeti a kármérték alapú minősítés gyakorlatát is. Rendkívüli jelentőségű az a tény, hogy az mavtv. megjelenését követően, a Kormány három kormányrendeletben szabályozta, a Nemzeti Biztonsági Felügyelet működését, a minősített

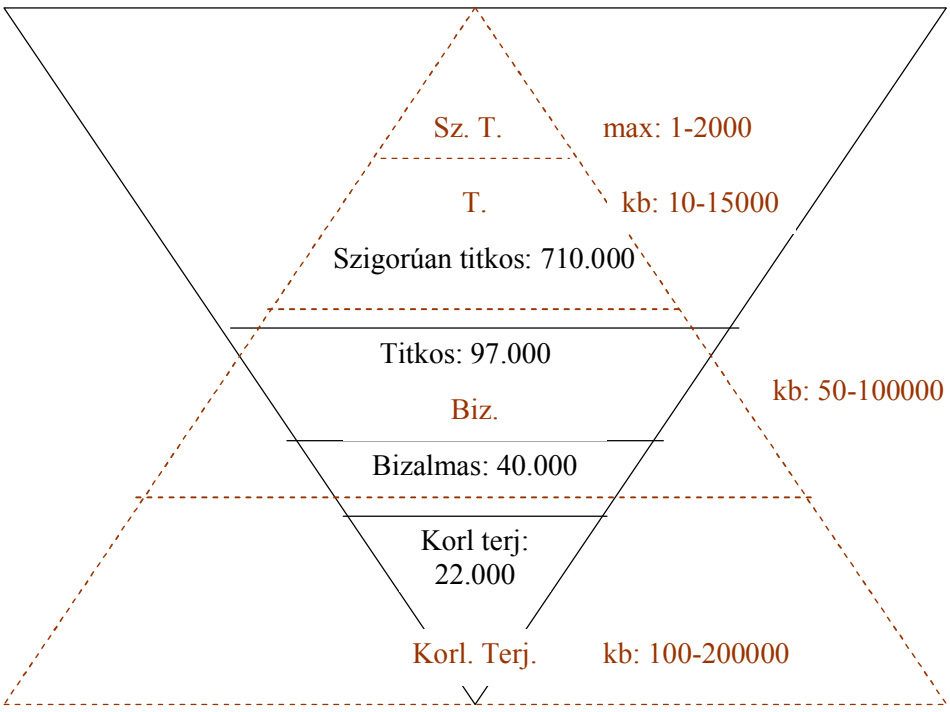
adat kezelésének rendjét, a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység és annak hatósági szabályait, illetve, az ezzel összefüggő iparbiztonsági területet is. Az előző időszakhoz képest megállapítható, hogy a nemzetkőzi szabályozókhoz igazodva, a koherenciára való törekvés egyértelműen nyomon követhető. A minősített adatok kezelésével összefüggő szabályozók között logikai és gyakorlati szinten megjelennek a komplex információvédelmi elvek. Ugyanakkor apróbb szabályozási ellentmondásokat is fel lehet lelni a minősített adatot kezelő szerezet vezetőjének hatáskörét illetően, abban az esetben, ha hierarchikus szervezetben történő szakirányítási szinten elemezzük a gyakorlati megvalósítást. További ellentmondások lelhetők fel az elektronikus információvédelem szabályozásának területén, különösen a kisugárzás védelem megvalósításának szabályozását illetően. Ugyanakkor vitathatatlanul történelmi jelentőségű eseményről van szó az információvédelmi szakmát illetően. Különösen igaz ez a megállapítás akkor, amikor a kritikus infrastruktúra védelmének területén fogalmazódik meg az igény egy olyan infokommunikációs, információs riasztási rendszer, illetve vezetésirányítási, kommunikációs rendszer szükségességét illetően, amely az érzékeny adataik védelmének érdekében információbiztonsági szempontból is megalapozottak. Napjainkban már hazai szektorokból is „figyelemfelkeltő jelzések" érkeznek azzal összefüggésben, hogy infrastruktúrájukat célzó kihívások és kockázatok észlelhető fenyegetések felé hajlanak. Ezekre a figyelmeztető jelekre célszerű odafigyelni és együttműködést kell kialakítani a kritikus infrastruktúrák védelmének érdekében. Ebben a globális környezetben szükségszerűen felértékelődik a minősített információ előállításával, gyűjtésével, tárolásával, feldolgozásával, továbbításával összefüggő információvédelmi tevékenység nemzeti és nemzetközi szintű koherens szabályozórendszer keretei között történő működtetése. Már pedig ha az igény a hazai szektorok felől egyre fokozódik az információvédelmi megoldások irányába, akkor az információvédelmi szakembereknek fel kell készülni az igények szakszerű kielégítésére. Természetesen szükségszerű az, hogy a jelenséget tudományos műhelyekben feltárjuk, elemezzük, modellezzük és hatékony védelmi rendszert tervezzünk és alkalmazzunk a nemzet biztonságát alapvetően befolyásoló szektorokban. Ez tehát az információvédelmi szakemberekkel szemben támasztott alapvető igény, és ennek kielégítése nem egyszerű feladat, ugyanakkor ennek szükségességére fel kell hívni az arra illetékesek figyelmét. Irányadó szakemberek szerint is megállapítható az, hogy a megfogalmazódó igények szakszerű kielégítésének kereteit teremti meg az írásműben ismertetett, értékelő elemzés tárgyát képező szabályozó rendszer.

A létfontosságú infrastruktúra védelmének érdekében használt – információ gyűjtésére, feldolgozására, tárolására és továbbítására – alkalmazott infokommunikációs rendszerek és azok információvédelmi jellemzői alapvetően befolyásolják a védelmi intézkedések eredményességét. Ennek okán célszerű összefoglalni a fentiekben felvázolt új, komplex információvédelmi irány tartalmát és összefüggéseit, illetve annak hatásait, következményeit a kritikus infrastruktúra és információs infrastruktúra védelmével összefüggésben.

AZ ÚJ ÍRÁNY ALAPJA A MINŐSÍTETT ADAT VÉDELMÉRŐL SZÓLÓ TÖRVÉNY

A minősített adatok védelméről szóló 2009. évi CLV törvényt (a továbbiakban Törvény) az Országgyűlés 2009. december 14-i ülésnapján fogadta el. Általános rendező elvek között megjelenik a Magyar Köztársaság érdekeinek védelme, a nemzetközi kötelezettségvállalások teljesítése a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvénnyel, valamint az elektronikus információbiztonságról szóló törvénnyel való összhang. Az törvényben ugyancsak jól kimutatható a külföldi minősített adatkezelési szabályokkal való

koherencia, az egységes elvek terminológiai megközelítés és az egységesített minősítési szintek.
Az is megállapítható, hogy a komplex információbiztonsági alapelvek szintén megjelennek az Törvényben. Ilyen alapelvek: a szükségesség és arányosság elve, a szükséges ismeret elve, a bizalmasság elve, a sérthetetlenség elve, valamint a rendelkezésre állás elve. Az irányelvek már világosan előrejelzik a törvény legalapvetőbb üzenetét, a túlminősítés elkerülése érdekében történő szabályozási elvek érvényesítését (1. ábra). Apróbb értelmezési anomáliát jelenthet a „sérthetetlenség elve" szóhasználat, amely helyett célszerűbb lenne a szakmai körökben elfogadott „sértetlenség elve" kifejezés használata.
A törvény – többek között – rögzíti a nemzeti minősített adat, külföldi minősített adat és az elektronikus adatkezelő rendszer fogalmát, ezzel elősegítve az egységes értelmezést.
Az információvédelmi szakemberek számára igen fontos és figyelemre méltó új elem a minősítéssel védhető közérdek és az ezzel összefüggő alapvetően kár alapú megközelítés (2. ábra). Ezzel összefüggésben a Törvény egyértelműen meghatározza, hogy az adat mely esetekben védhető minősítéssel. A Törvény új minősítési szinteket állapít meg úgymint „Szigorúan titkos" „Titkos" „Bizalmas" és „Korlátozott terjesztésű". Ezek a minősítési szintek megfelelnek a külföldi minősített adat minősítési szinteknek (3. ábra). Ez egy igen fontos lépés az előirányzott koherencia területén. A minősítések érvényességi ideje is lényegesen csökkent, illetve a felülvizsgálatok száma is korlátossá vált (4. ábra). Ez is tükrözi és elősegíti a túlminősítés és a túlzott idejű minősítés fenntartása elleni küzdelmet. Külön szakasz foglalkozik a minősített adat felülvizsgálatának és felülbírálásának szabályaival, egyértelművé téve ezzel a szabályozást. Ugyanakkor – egyes szakemberek szerint – a minősítő számára a melléklet nem ad megfelelően egyértelmű támpontokat a minősítési szint megállapításának vonatkozásában. A törvény újra szabályozza a minősítési szintekhez kapcsolódó nemzetbiztonsági ellenőrzések rendszerét (5. ábra) és a büntetőjogi szankciórendszert is differenciálja az egyes minősítési szintekhez igazodóan (6. ábra).



1. ábra. A túlminősítési piramis talpra állítása [9]

„Szigorúan titkos!”	**rendkívül súlyosan károsítja a minősítéssel védhető közérdeket**
„Titkos!”	**súlyosan károsítja a minősítéssel védhető közérdeket**
„Bizalmas!”	**károsítja a minősítéssel védhető közérdeket**
„Korlátozott terjesztésű!”	**hátrányosan érinti a minősítéssel védhető közérdeket**

2. ábra. Kár alapú megközelítés (1) [9]

„Szigorúan titkos!”	**a Magyar Köztársaság szuverenitásának megsértése, nagyszámú emberi élet veszélyeztetése;**
„Titkos!”	**közvetlen életveszély okozása, ellehetetleníti az állami vagy közfeladatot ellátó szerv rendeltetésszerű működését;**
„Bizalmas!”	**az állam érdekérvényesítő képességeit hátráltatja, gátolja valamely legalább öt évi szabadságvesztéssel büntetendő bűncselekmény felderítését**
„Korlátozott terjesztésű!”	**gazdálkodó szervezetek részére jogtalan előnyszerzést tesz lehetővé;**

3. ábra. Kár alapú megközelítés (2) [9]

	Érvényességi idő	Hosz-szabbítás alapesete	Magánszemély jogos érdekével összefügg. A Magyar Köztársaság - honvédelmi, - nemzetbiztonsági, - bűnüldözési vagy - igazságszolgáltatási érdekére tekintettel
„Szigorúan titkos!”, „Titkos!”	**30 év**	1 x 30 év **∑: 60 év**	2 x 30 év **∑: 90 év**
„Bizalmas!”	**20 év**	1 x 5 év **∑: 25 év**	2 x 20 év **∑: 60 év**
„Korlátozott terjesztésű!”	**10 év**	1 x 5 év **∑: 15 év**	2 x 20 év **∑: 50 év**

4. ábra. Az érvényességi idő új szabályozása [9]

„Szigorúan titkos!”	„C” típusú kérdőívhez kötött nemzetbiztonsági ellenőrzés
„Titkos!”	„B” típusú kérdőívhez kötött nemzetbiztonsági ellenőrzés
„Bizalmas!”	„A” típusú kérdőívhez kötött nemzetbiztonsági ellenőrzés
„Korlátozott terjesztésű!”	Nincs szükség nemzetbiztonsági ellenőrzésre

5. ábra.
Az egyes minősítési szintekhez kapcsolódó nemzetbiztonsági ellenőrzések típusai [9]

	„civil” maximum	„hivatalos” maximum
Visszaélés szigorúan titkos minősítésű adattal:	2-8 évig	5-15 évig
Visszaélés titkos minősítésű adattal:	1-5 évig	2-8 évig
Visszaélés bizalmas minősítésű adattal:	- 3évig	1-5 évig
Visszaélés korlátozott terjesztésű minősítésű adattal:	- 1 évig	-3 évig

6. ábra. A büntetőtörvénykönyv változása. [9]

A minősített adat általános biztonságára vonatkozó szabályok

Ebben a fejezetben jelenik meg a szakmai műhelyekben már kialakított komplex információ biztonság rendszere. Jól látszik, hogy az írásmű követi a komplex információvédelmi felosztást – úgymint személyi biztonság; adminisztratív (dokumentum´biztonság; fizikai biztonság; elektronikus biztonság – és annak alrendszereit.

A biztonság alapvető feltételei a Nemzeti biztonsági Felügyelet – mint hatóság - által kiállított adatkezelési engedély, személyi biztonsági tanúsítvány, nemzetbiztonsági ellenőrzés lefolytatása, a végrehajtási rendeletekben kiadott személyi, fizikai, adminisztratív és elektronikus biztonsági követelmények teljesítése. Ez a komplex megközelítési mód – szakmai körökben elfogadott elvek alapján - teremti meg a minősített adatok hatékony védelmének alapjait.

A minősített adat védelmét ellátó szervezetek és személyek

Ebben a fejezetben fogalmazódnak meg a Nemzeti Biztonsági Felügyelet (A továbbiakban NBF) feladatai. Az NBF önálló feladattal és hatósági jogkörrel rendelkező szervezet. Új megközelítésben a minősített adatot kezelő szervezet vezetője felelős a minősített adat védelmi feltételeinek kialakításáért, ugyanakkor a feladatok végrehajtását és koordinálását a minősített adatot kezelő szerv vezetője által kinevezett biztonsági vezető végzi. A Törvény lehetőséget ad, úgynevezett biztonsági felügyelet kijelölésére is, melyet a kinevezett Biztonsági Vezető irányítja. A felvázolt felső szintű szervezeti struktúra hierarchikus rendszere és a kinevezés intézménye biztosítja a minősített adat védelmének érdekében létrehozott szervezet hatékony működését, úgy hogy már itt, meghatározásra kerülnek az alapvető felelősségi körök.

A MINŐSÍTETT ADATOK VÉDELMÉVEL KAPCSOLATOS VÉDELMI INTÉZKEDÉSEK

A minősített adat védelméről szóló 2009. évi CLV. törvényben meghatározott fő irányokat részleteiben a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet, a minősített adat elektronikus

biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V.6) Korm. rendelet és az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendelet szabályozza.

Az iparbiztonsági ellenőrzés és a Telephely Biztonsági Tanúsítvány (a továbbiakban: TBT) kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendelettel összefüggésben az alábbiak kiemelése szükségszerű és elengedhetetlen annak érdekében, hogy a szabályozási folyamat véglegesítésének lehetőségét és alkalmazhatóságát elemezzük. A minősített adatot kezelő gazdálkodó szervezeteknek 2010. április 01-ét követően TBT-t beszerezniük, melynek előfeltétele a legalább két éves működés. A NATO EU TBT kiállítása csak nemzeti TBT birtokában lehetséges. Az iparbiztonsági ellenőrzés két fázisból áll, nevezetesen a nemzetbiztonsági fázisból és a fizikai és adatbiztonsági fázisból. A nemzetbiztonsági fázis az Alkotmányvédelmi Hivatal és Katonai Biztonsági Hivatal, a fizikai és adatbiztonsági fázis pedig az NBF hatáskörébe tartozó tevékenység.
A kiadott TBT azt igazolja hogy:

- az adott gazdálkodó szervezet iparbiztonsági ellenőrzése befejeződött
- adott szintű minősített információk kezelésére (tárolására, feldolgozására)alkalmas
- minősített projektbe biztonsági szempontból bevonható

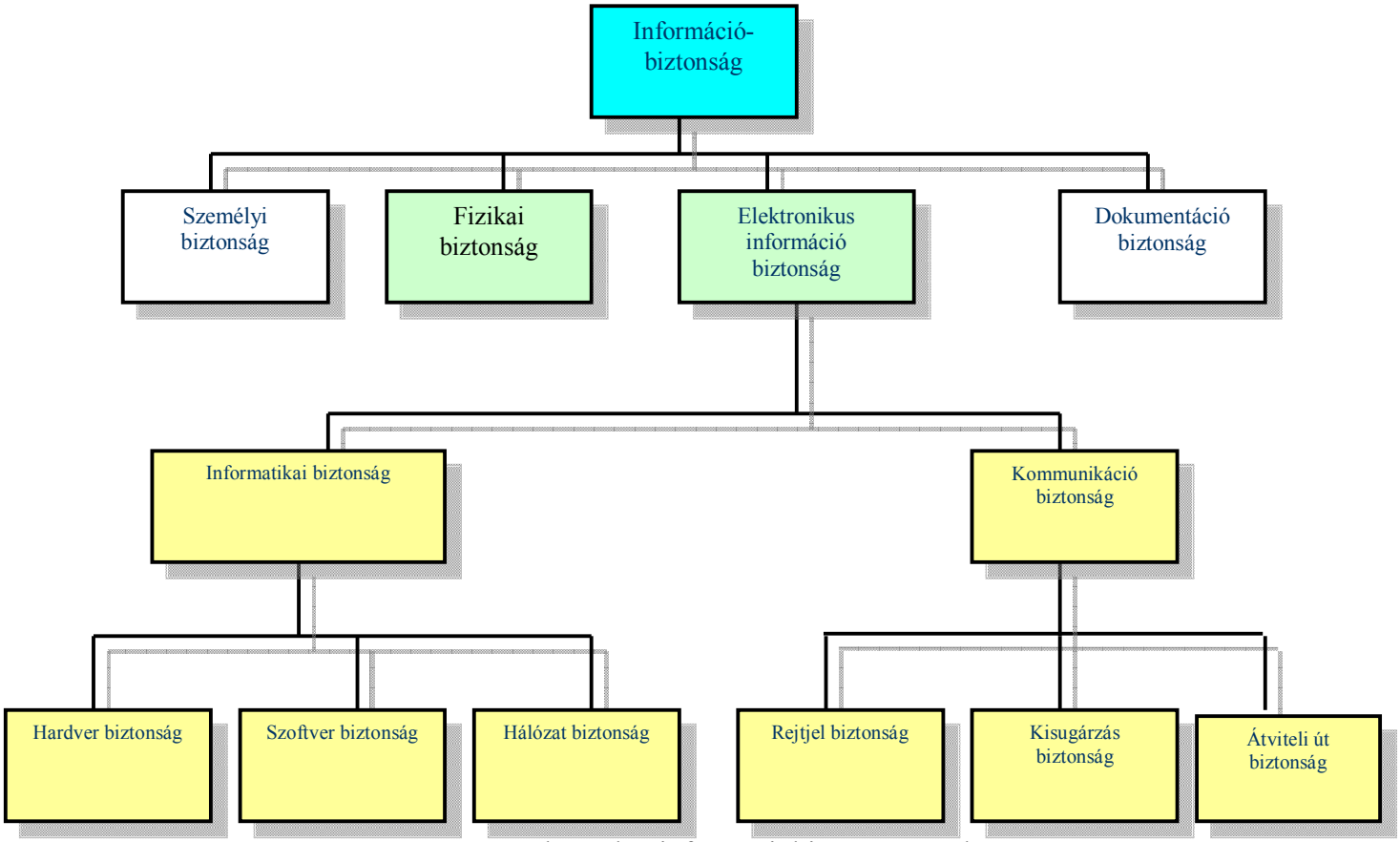
A „Bizalmas" vagy magasabb minősítési szint esetén az érvényes telephely biztonsági tanúsítvány érvényességének igazolását a minősített adatot átadó szerv az NBF-től kéri.
A„Korlátozott terjesztésű" minősítési szint esetén a gazdálkodó szervezet részére a felhasználói engedélyt a minősített adatot átadó szerv vezetője adja ki (előtte meggyőződik, hogy megteremtették-e a KT védelméhez előírt biztonsági feltételeket)
A gazdálkodó szervek a minősített szerződés végrehajtásának biztonsági előírásait Projekt Biztonsági Utasításban szabályozzák.
A Projekt Biztonsági Utasítást a minősített adatot átadó szerv vezetője készíti el a biztonsági vezető bevonásával. A Projekt Biztonsági Utasítás, a minősített szerződés részletes biztonsági előírásait tartalmazza, függeléke a projekt minősítési jegyzék.
A projekt biztonsági utasítás rendelkezik:

- A végrehajtásban részt vevő szervek, a biztonsági szervek és személyek feladat- és hatásköréről,
- a minősített adatok helyszíni tárolásának, bel-és külföldi továbbításának szabályairól,
- a megbeszéléseken, előadásokon történő felhasználás egyedi rendelkezéseiről,
- a minősített adatok alvállalkozónak történő átadásának feltételeiről,
- a minősített szerződés teljesítését követő eljárásrendről (minősített adatok átadónak történő visszaszolgáltatása).

Külföldi gazdálkodó szervezet bevonása esetén a „Bizalmas" vagy annál magasabb minősítési szintű szerződés kötését megelőzően a minősített adatot átadó szerv vezetője az NBF útján be kell hogy szerezze az adott ország nemzeti biztonsági hatóságának igazolását a TBT meglétéről.
Ha a fenti szabályozást összevetjük a jelenleg érvényes szabályozási környezettel és a valós gazdasági környezettel, egyrészt megállapítható, hogy TBT-vel a hazai gazdálkodó szervezetek nagy része még nem rendelkezik, ezért ezen a területen a szabályozás gyakorlati környezetbe való átültetése fontos és elengedhetetlen feladat. Másrészt figyelemmel arra, hogy *az államtitkot vagy szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintő vagy különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló 143/2004. (IV.29.) Korm. rendelet még mindig hatályos,* ezért annak módosítása a

telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendelettel összhangban szükséges.

Ugyanakkor a fentiekben kifejtett megállapításokkal együtt ki lehet jelenteni, hogy a minősített adat védelméről szóló 2009. évi CLV. törvényben és a hozzá kapcsolódó kormányrendeletek a nemzetközi trendnek megfelelően a védelmi intézkedéseket az eddigi tudományos kutatások alapjaira helyezik (1.ábra) . Az alapelvek és előírt védelmi intézkedések tükrözik a Tanács biztonsági szabályzatának elfogadásáról szóló EU Tanács 2001. március 19-i 2001/264/EK határozatában megfogalmazottakat, azzal összhangban vannak.



7. ábra. A komplex információbiztonság rendszere

Megállapítható viszont az is, hogy a 161/2010. (V.6) Korm. rendelet nem intézkedik kellő részletességgel a hardver és szoftverbiztonsági kérdésekről és a „nemzeti TEMPEST" követelményrendszerével összefüggésben ugyan „az engedélyezési eljárások „fejezetében „a TEMPEST követelmények érvényesítése" [3] megemlíti, de részletes követelményeket nem támaszt. Előirányozza a TEMPEST követelményrendszerének rendelkezésre állását, de ilyen nemzeti követelményrendszer még nem érhető el, illetve az NBF jelenlegi álláspontjára figyelemmel az megegyezik a NATO TEMPEST követelményekkel. Ez alapvetően befolyásolja az elektronikus védelmi intézkedések kisugárzás védelmi alrendszereinek rendelkezésre állását, amely egyben a védelmi rendszer egyenszilárdságát is befolyásoló tényezővé válhat. Irányadó szakemberek véleménye szerint ezen a területen is további szabályozás szükséges.
A minősített adatok kezelésére alkalmas elektronikus rendszer teljes életciklusában a feljogosítás előtti, az adatkezelés alatti és a feljogosítás megszüntetése utáni szakaszokra bonthatók.

Ennek megfelelően a személyi biztonság kérdései is három részre tagolhatók [8]:

- az adatokhoz, adatkezelő rendszerekhez történő hozzáférésre feljogosított személyek kiválasztása, a munkakörök meghatározása;
- az adatkezelés, a beosztások változása során az időszakosan visszatérő jellegű biztonsági tájékoztatások, képzések és továbbképzések a felhasználók, a rendszerek üzemeltető és biztonsági feladatokat ellátó állománya számára, valamint a változások nyomon követése és felügyelete;
- az adatkezelési jogosultság megszűnése esetén a hozzáférési jogosultságok törlése.

A jogszabályok a személyi biztonsággal kapcsolatosan általános követelményeket határoznak meg. A minősített adatkezelést szabályozó törvény az adatkezelésre vonatkozó adminisztratív rendszabályok mellett például a képzést és a továbbképzést egyedül a Nemzeti Biztonsági Felügyelet feladatainál említi, részletesebb követelmények nélkül [1.]. Ugyanez tapasztalható a minősített NATO, EU és egyéb külföldi adatkezelést szabályozó 2010. március 31-ig érvényes kormányrendelet esetében is.
Emiatt célszerűnek látszik a személyi biztonság kérdéseinek pontosabb vizsgálata és meghatározása. Az életciklus szerinti megközelítés már megjelenik a nemzeti szabványokban [4], a jelenleg érvényes nemzeti ajánlás is ezt a szemléletet tükrözi [6], illetve az informatikai szolgáltatások szabályozása területén is megfigyelhető [7]. Az említett források feldolgozása az információvédelmi szakemberek munkáját támogathatja, ezzel összefüggésben Kassai Károly Hadtudományi Szemlében megjelent cikke [8] jó példa a szabványok, a civil ajánlások alkalmazhatóságának vizsgálatára.

A 90/2010. (III. 26.) Korm. rendelet előírja, [2] hogy a minősített adatot kezelő szervezetnek el kell készítenie a biztonsági szabályzatát, amelyben leírja a minősített adatok védelmének érdekében felállított szervezet felépítését, működését, a személyi fizikai adminisztratív és elektronikai védelem területén foganatosított védelmi intézkedéseket és a veszélyhelyzeti tervet. Az alábbiakban a kormányrendeletben előírtakra figyelemmel, biztonsági szabályzat ajánlásban célszerű összefoglalni a kormányrendeletekben tükröződő követelményrendszert.
A komplex információbiztonsági elveket szem előtt tartva, fontos kiemelni, hogy az elektronikai biztonsági követelményrendszer – és az ezzel összefüggő szabályzat kialakítása – a biztonsági szabályzaton túl mutató (szabályozási szempontból, a törvény erejéből fakadóan követő) önálló szabályozási ciklusban nyilvánul meg. Ebből eredően ugyan nem szükséges az elektronikus biztonságot a szervezet biztonsági szabályzatában szabályozni, viszont az információs társadalmi fejlődés jelen szakaszában, valós kockázatot jelent ezen a területen a szabályozás hiánya.

BIZTONSÁGI SZABÁLYZAT

(ajánlás)

a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján minősített és a nemzeti minősített adatok védelmére

I. fejezet
ÁLTALÁNOS SZABÁLYOK

Jelen Szabályzat (ajánlás) a minősített adat védelméről szóló 2009. évi CLV. törvényben (a továbbiakban: (Mavtv.) valamint Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendeletben (a továbbiakban: Rendelet) a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V.6) Korm. rendeletben és az iparbiztonsági ellenőrzés és a telephely biztonsági

tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendeletben foglaltak alapján meghatározza:

a) azon kezelési eljárások és módszerek összességét, amelyek kizárják a nemzeti és a külföldi minősített adatok illetéktelen személyek által történő megismerését;

b) nemzeti és a külföldi minősített adathordozók (iratok) készítésének, nyilvántartásának, továbbításának és irattári kezelésének szabályait.

Az alkalmazott biztonsági intézkedések:

- kiterjednek a minősített adatokhoz hozzáférő személyekre, a minősített adathordozókra, a minősített adatoknak helyet adó helyiségekre és berendezésekre;
- kiszűrik azokat a személyeket, akiknek az alkalmazása veszélyezteti a minősített adatok és az azokat tartalmazó adathordozók, berendezések biztonságát;
- megakadályozzák, hogy a minősített adatokhoz, adathordozókhoz és berendezésekhez, illetéktelen személyek hozzáférhessenek;
- a minősített adatok elosztása során a „szükséges ismeret" elvét követik;
- biztosítják a minősített adat integritását, (megakadályozzák a megrongálódást, illetéktelen módosítását, vagy illetéktelen törlését) és rendelkezésre állását (hozzáférést biztosít az arra jogosultak részére).

1. Alapelvek

Szükségesség és arányosság elve a közérdekű adat nyilvánosságához fűződő jogot minősítéssel korlátozni csak az e törvényben meghatározott feltételek fennállása esetén, a védelemhez szükséges minősítési szinttel és a feltétlenül szükséges ideig lehet. *Szükségesség és arányosság elve alapján a zavartalan információáramlás biztosítása érdekében törek*edni kell az indokolatlan szigorú minősítés elkerülésére.

Szükséges ismeret elve: minősített adatot csak az ismerhet meg, akinek az állami vagy közfeladata ellátásához feltétlenül szükséges.

Bizalmasság elve: minősített adat illetéktelen személy számára nem válhat hozzáférhetővé vagy megismerhetővé.

Sérthetetlenség elve: a minősített adatot kizárólag az arra jogosult személy módosíthatja vagy semmisítheti meg.

Rendelkezésre állás elve: annak biztosítása, hogy a minősített adat az arra jogosult személy számára szükség szerint elérhető és felhasználható legyen.

2. A Szabályzat hatálya

2.1. Itt kell megfogalmazni, hogy mely hivatali szervezeti egységekre terjed ki a biztonsági szabályzat hatálya.

3. Értelmező rendelkezések [1] 3.§

2.2. **NATO, illetve NYEU Központi Nyilvántartó:** a Honvédelmi Minisztérium információ- és dokumentumvédelemmel foglalkozó szervének a NATO, illetve a NYEU minősített információk országos szinten történő fogadására, elosztására és kezelésére kijelölt szervezeti egysége;

2.3. **EU Központi Nyilvántartó:** a Külügyminisztériumnak az EU minősített adatok országos szinten történő fogadására, elosztására és kezelésére kijelölt szervezeti egysége;

2.4. **Nemzeti minősített adat:** a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést a Mavtv-ben, valamint a törvény felhatalmazása alapján kiadott,

jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele, a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti, vagy veszélyezteti és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza;

2.5. **Külföldi minősített adat:** az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza.

2.6. **Nyilvántartó:** a minősített adatot kezelő szervhez érkező vagy ott keletkező, külföldi és nemzeti minősített adatok nyilvántartásával kapcsolatos feladatok végrehajtására feljogosított szervezet;

2.7. **Kezelő pont:** a Nyilvántartó felügyelete alatt működő, a nemzeti minősített adatok nyilvántartásával kapcsolatos feladatok végrehajtására létrehozott szervezet;

2.8. **Érvényességi idő:** az az év, hó, nap, szükség esetén óra, perc szerint feltüntetett időpont, ameddig a nemzeti minősített adat nyilvánosságra hozatalát, illetve az arra feljogosítotton kívüli minden megismerhetőségét a minősítő korlátozza;

2.9. **Minősítő:** feladat- és hatáskörében minősítésre jogosult személy;

2.10. **Minősített adatot kezelő szerv:** állami vagy közfeladat ellátása érdekében minősített adat kezelését végző szerv, szervezet vagy szervezeti egység, továbbá a gazdálkodó szervezet.

2.11. **Biztonsági vezető:** a minősített adatok védelmével kapcsolatos feladatok végrehajtását és koordinálását végző, a minősített adatot kezelő szerv vezetője által – a Nemzeti Biztonsági Felügyelet elnökének egyetértésével - kinevezett személy;

2.12. **Titkos ügykezelő:** a nyilvántartó és a kezelő pont iratkezelője;

2.13. **Közreműködő:** az a természetes személy, aki az állami vagy közfeladatot ellátó szerv feladat- és hatáskörébe tartozó ügyben segítséget nyújt, és ehhez minősített adat felhasználása is szükséges.

2.14. **Felhasználó:** az a személy, akinek állami vagy közfeladat végrehajtása céljából a felhasználói engedély kiadására jogosult vezető a minősített adatra vonatkozóan a felhasználói engedélyben rendelkezési jogosultságokat biztosít;

2.15. **Felhasználás:** állami vagy közfeladat végrehajtása érdekében a felhasználói engedély kiadására jogosult vezető által, a felhasználói engedélyben meghatározott, a minősített adatra vonatkozó rendelkezési jogosultságok gyakorlása.

2.16. **Felhasználói engedély:** állami vagy közfeladat végrehajtása érdekében a minősítő, illetve a felhasználói engedély kiadására jogosult vezető által, a minősített adat felhasználására jogosult személy részére írásban adott felhatalmazás, a minősített adattal kapcsolatos egyes rendelkezési jogosultságok meghatározásával.

2.17. **Megismerési engedély:** a minősítő által a jogosult személyazonosító adatainak feltüntetésével, a nemzeti minősített adattal kapcsolatos rendelkezési jogosultságok megjelölésével, a nemzeti minősített adat megismerésére írásban adott felhatalmazás. **Titoktartási nyilatkozat:** a minősített adatot felhasználó vagy megismerő személy nyilatkozata arról, hogy a minősített adat védelmére vonatkozó szabályokat megismerte, és az őt terhelő titoktartási kötelezettséget tudomásul vette.

2.18. **Személyi biztonsági tanúsítvány:** az a tanúsítvány, amely érvényességi idejének lejártáig meghatározza, hogy valamely természetes személy milyen legmagasabb minősítési szintű adat felhasználására kapott felhasználói engedélyt.

2.19. **Elektronikus adatkezelő rendszer:** minősített adat elektronikus, elektromagnetikus vagy optikai úton történő kezelésére alkalmas berendezés, módszer és eljárás együttese;
2.20. **Rendvédelmi szerv:** a rendőrség, a polgári védelem, a polgári nemzetbiztonsági szolgálatok, a büntetés-végrehajtási szervezet, a vám- és pénzügyőrség, valamint az állami és hivatásos önkormányzati tűzoltóság;

4. A külföldi minősítési szint és annak nemzetközi minősítési szintű megfelelője [1] / 2.sz. melléklet

4.1. A NATO által használt minősítési szint és annak nemzeti minősítési szintű megfelelője:
- „COSMIC TOP SECRET" - „Szigorúan titkos!";
- „NATO SECRET" - „Titkos!";
- „NATO CONFIDENTIAL" - „Bizalmas!";
- „NATO RESTRICTED" - „Korlátozott terjesztésű!".

4.2. A NYEU által használt minősítési szint és annak nemzeti minősítési szintű megfelelője:
- „FOCAL TOP SECRET" - „Szigorúan titkos!";
- „WEU SECRET" - „Titkos!";
- „WEU CONFIDENTIAL" - „Bizalmas!";
- „WEU RESTRICTED" - „Korlátozott terjesztésű!".

4.3. Az Európai Unió Tanácsa által alkalmazott minősítési szint és annak nemzeti minősítési szintű megfelelője:
- „TRES SECRET UE/EU TOP SECRET" - „Szigorúan titkos!";
- „SECRET UE" - „Titkos!";
- „CONFIDENTIEL UE" - „Bizalmas!";
- „RESTREINT UE" - „Korlátozott terjesztésű!".

4.4. Az Európai Bizottság által alkalmazott minősítési szint és annak nemzeti minősítési szintű megfelelője:
- „TRES SECRET UE/EU TOP SECRET" - „Szigorúan titkos!";
- „SECRET UE" - „Titkos!";
- „CONFIDENTIEL UE" - „Bizalmas!";
- „RESTREINT UE" - „Korlátozott terjesztésű!".

4.5. Az EURATOM által alkalmazott minősítési szint és annak nemzeti minősítési szintű megfelelője:
- „EURA-TOP SECRET" - „Szigorúan titkos!";
- „EURA-SECRET" - „Titkos!";
- „EURA-CONFIDENTIAL" - „Bizalmas!";
- „EURA-RESTRICTED" - „Korlátozott terjesztésű!".

4.6. Az EUROPOL által alkalmazott minősítési szint és annak nemzeti minősítési szintű megfelelője:
- „EUROPOL TOP SECRET" - „Szigorúan titkos!";
- „EUROPOL SECRET" - „Titkos!";
- „EUROPOL CONFIDENTIAL" - „Bizalmas!";
- „EUROPOL RESTRICTED" - „Korlátozott terjesztésű!".

4.7. AZ EUROJUST által alkalmazott minősítési szint és annak nemzeti minősítési szintű megfelelője:

- „EUROJUST TOP SECRET” - „Szigorúan titkos!”;
- „EUROJUST SECRET” - „Titkos!”;
- „EUROJUST CONFIDENTIAL” - „Bizalmas!”;
- „EUROJUST RESTRICTED” - „Korlátozott terjesztésű!”.

II. fejezet
A BIZTONSÁGI SZERVEZET

5. A minősített adatot kezelő szerv vezetőjének jogköre

5.1. Meghatározza a személyi, fizikai és adminisztratív biztonsági követelményeket, a minősítéssel a minősített adat felhasználásával, megismerésével kapcsolatos jogokat és kötelezettségeket.
5.2. Megállapítja a minősített adat biztonságának megsértése esetén szükséges eljárás, valamint a minősített adatok veszélyhelyzetben történő védelmi intézkedéseinek rendjét.
5.3. Kialakítja a minősített adat védelmének feltételeit.
5.4. Kijelöli az elektronikus biztonságért felelős személyek körét.
5.5. Kiadja az elektronikus rendszer biztonsági dokumentációit.
5.6. Megállapítja rejtjeltevékenység szervezeti rendjét, biztosítja a rejtjeltevékenység végrehajtásához szükséges személyi, tárgyi és biztonsági feltételeket és kiadja a rejtjelszabályzatot.
5.7. Kijelöli a rejtjeltevékenység biztonságáért felelős személyeket.
5.8. Kiadja a rejtjeltevékenységére vonatkozó rejtjel-hozzáférési engedélyeket.
5.9. Kijelöli a felhasználói engedély kiadására jogosult vezetőket.
5.10. A személyi biztonsági tanúsítvány kiadása érdekében kezdeményezi a nemzetbiztonsági ellenőrzések lefolytatását.

6. Helyi biztonsági felügyelet

6.1. A szervezet minősített adatok védelmének érdekében helyi biztonsági felügyeletet működtet.
6.2. A helyi biztonsági felügyelet ellátja a személyi, fizikai, adminisztratív, dokumentum, elektronikai és egyéb biztonsági szabályok alkalmazásának felügyeletét.

7. A biztonsági vezető

7.1. A Biztonsági vezetőt a szervezet vezetője nevezi ki a Nemzeti Biztonsági Felügyelet (a továbbiakban: NBF) elnökének egyetértésével.
7.2. A biztonsági vezető a minősített adatot kezelő szervezet vezetőjének átruházott hatáskörében eljárva – az Mavtv. irányelvei alapján – utasítási joggal gyakorolja a szervezet vezetőjének minősített adat védelmére vonatkozó jogosítványait.
7.3. Ellátja a Rendelet és a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályiról szóló 161/2010. (V.6.) Korm. rendeletben meghatározott szabályok alkalmazásának felügyeletét. Ennek keretében gondoskodik a nemzeti és a külföldi minősítéssel és jelöléssel ellátott adatok védelme érdekében meghatározott feladatok végrehajtásáról.

7.4. **Biztonsági vezető feladatai**

- gondoskodik a hivatali szervezeti egységnél a minősített adatok védelmével kapcsolatos feladatok végrehajtásáról és koordinálásáról;
- ellenőrzi a minősített adat védelmére vonatkozó személyi, fizikai, adminisztratív és elektronikus biztonsági rendelkezések megtartását,
- intézkedik a minősített iratforgalmi statisztikák minősítési szintenkénti bontásban történő elkészítéséről;
- intézkedik a nemzeti minősített adatra érvényes személyi biztonsági tanúsítványok kiadásáról, kezeléséről és tárolásáról;
- kezdeményezi a Nemzeti Biztonsági Felügyeletnél a külföldi minősített adatra érvényes személyi biztonsági tanúsítvány kiadását a NATO, NYEU és az EU minősített adatokhoz hozzáférő felhasználók és közreműködők részére;
- felügyeli a titkos ügykezelők tevékenységét;
- elkészíti a titkos ügykezelőre meghatározott tananyagot, vizsgakövetelményt, meghatározza az oktatás szervezeti kereteinek és a vizsgáztatás eljárási rendjét,
- gondoskodik a felhasználói engedély és a titoktartási nyilatkozat kiadásáról, kezeléséről, valamint tárolásáról;
- elkészíti a biztonsági szabályzatot, ellenőrzi az abban foglaltak betartását;
- intézkedik a biztonsági területre telepített biztonságtechnikai eszközöknek és rendszereknek a gyártó előírása szerinti gyakorisággal, de legalább évente egy alkalommal történő karbantartására;
- engedélyezi a személyi biztonsági tanúsítvánnyal rendelkező látogatók azonosító kártya viselése melletti önálló, kíséret nélküli mozgását a biztonsági területen, amennyiben a biztonsági területre érkező látogató biztonsági vezetője írásban igazolja, hogy a látogató személyi biztonsági tanúsítvánnyal rendelkezik;
- kezeli a biztonsági területen használt kódok megváltoztatásának tényét és időpontját rögzítő nyilvántartást;
- ellátja a Nyilvántartó(k) és Kezelő pont(ok) szakmai felügyeletét;
- a minősített adat biztonságának megsértése esetén intézkedik a minősített adat biztonságának megsértése kapcsán felmerülő kár felméréséről és enyhítéséről, valamint – ha ez lehetséges – a jogszerű állapot helyreállításáról;
- tárolja a Nyilvántartók és a Kezelő pontok (irodák, irodabútorok) tartalék kulcsait;
- rendszeresen részt vesz az NBF és a központi nyilvántartók által szervezett továbbképzéseken;
- jelen van a szervezeti egységnél végrehajtott biztonsági ellenőrzéseken;
- vezeti a jogszabályban meghatározott nyilvántartásokat;
- irányítja a helyi biztonsági felügyelet szakmai tevékenységét;
- szakmailag irányítja rendszeradminisztrátor tevékenységét;
- kezdeményezi az elektronikus biztonsághoz, és a rejtjeltevékenységhez előírt engedélyek beszerzését, gondoskodik azok nyilvántartásáról, gondoskodik a rendszerbiztonsági dokumentumok elkészítéséről;
- kivizsgáltatja a rendszerbiztonsági eseményeket;
- kapcsolatot tart a Nemzeti Hálózatbiztonsági Központtal;
- ellenőrzi az elektronikus biztonsági előírások betartását;
- irányítja a rejtjelfelügyelet tevékenységét.

8. Központi rejtjelfelügyelet vezető

8.1. A rejtjelfelügyelet vezetője irányítja a minősített adatokat kezelő szervezet rejtjeltevékenységét.

8.2. A rejtjelfelügyelet rejtjelszabályzatban állapítja meg a minősített adatot kezelő szervezet rejtjeltevékenységének szervezeti rendjét, szabályait, feladat és hatáskörét.
8.3. A rejtjel felügyelet hatáskörét, szervezeti és működési rendjét, feladatait valamint a szervezet rejtjel anyagaira vonatkozó biztonsági követelmények szabályozására a rejtjeltevékenységet végző szervezet vezetője, rejtjelszabályzatot ad ki.

9. Rejtjelző

9.1. A rejtjelző eszközöket a megfelelő szintű, az adott rejtjelző eszközre érvényes rejtjel-hozzáférési engedéllyel rendelkező rejtjelző üzemelteti.
9.2. A rejtjelzők feladatait a minősített adatokat kezelő szervezet vezetője rejtjelszabályzat rögzíti.

10. A titkos ügykezelők

10.1. Titkos ügykezelő feladatai.

11. Rendszerbiztonsági felügyelő

11.1. Rendszerbiztonsági felügyelő feladatai.

12. Személyi és fizikai biztonsági felügyeleti munkatárs

A személyi és fizikai biztonsági szakreferens a helyi biztonsági felügyelet állományába tartozó személy, akinek szakmai tevékenységét a biztonsági vezető közvetlenül irányítja.
12.1. A személyi és fizikai biztonsági szakreferens feladatai .

13. Rendszeradminisztrátor

13.1. A minősített adatok elektronikus kezelésére alkalmas rendszer üzemeltetését a rendszeradminisztrátor végzi.
13.2. A rendszeradminisztrátor feladatai.

III. fejezet
SZEMÉLYI BIZTONSÁG

14. Nemzeti és külföldi minősített adat felhasználása, megismerése és a rendelkezési jogosultság meghatározása.

IV. fejezet
FIZIKAI BIZTONSÁG

15. A fizikai biztonsági követelmények érvényesülése.

16. Fizikai biztonsági védelmi intézkedések.

17. A kulcsok kezelése.

VI. fejezet
ELEKTRONIKUS BIZTONSÁG

18. A minősített adatok elektronikus rendszeren történő felhasználásának és tárolásának (kezelésének) szabályai.

VII. fejezet
ADMINISZTRATÍV BIZTONSÁG

19. A minősítési eljárás és a minősítés szabályai.

20. A minősített adatot tartalmazó adathordozó nyilvántartásba vétele.

21. A más szervtől érkezett minősített küldemény átvétele.

22. A küldemény felbontása.

23. A minősített adathordozó továbbítására vonatkozó rendelkezések.

24. A minősítés felülvizsgálata, felül bírálata.

25. A minősített adat átadása közreműködő részére.

26. Minősített adathordozó sokszorosítása, fordítása, kivonatolása .

27. Minősített adathordozók átadása megbízás megszűnése esetén.

28. A minősített adathordozó megsemmisítése.

29. A titoktartási kötelezettség alóli felmentés.

VIII. fejezet
ELLENŐRZÉS

30. Az ellenőrzés

30.1. A minősített adatok védelmére vonatkozó szabályok megtartásának ellenőrzésére jogosultak:
a) a minősített adatok kezelésére jogosult szervezet állományából:
- a minősített adatot kezelő szervezet vezetője;
- a biztonsági vezető;
- a minősített adatot kezelő szervezet vezetője által írásban felhatalmazott személy;

b) a jogszabályban erre feljogosított más szervezet.

30.2. Az ellenőrzésről jegyzőkönyvet kell készíteni, amelyet az ellenőrzött személynek is alá kell írnia. Az ellenőrzött személy kérésére az ellenőrzéssel kapcsolatos megállapításait a jegyzőkönyvben rögzíteni kell.

30.3. Az ellenőrzés során megállapított hiányosságokról haladéktalanul írásban tájékoztatni kell a minősített adatok kezelésére jogosult szervezet vezetőjét, aki soron kívül intézkedik a feltárt szabálytalanságok megszüntetéséről, a felelősség megállapításáról.

30.4. Évente, január 02. és február 20. között e feladatra kijelölt bizottságnak ellenőrizni kell a minősített adathordozók meglétét, valamint az biztonsági szabályainak betartását. Az ellenőrzés eredményét jegyzőkönyvben kell rögzíteni, azt 10 évig meg kell őrizni.

30.5. A tikos ügykezelők és felhasználók a kezelésükben lévő minősített adathordozókat negyedévente egyszer kötelesek tételesen ellenőrizni és ennek tényét dokumentálni. Adathordozó esetleges hiányának észlelése esetén a biztonsági vezető felé jelentést kell tenni.

30.6. A tikos ügykezelők és a felhasználók, tételes ellenőrzést kötelesek végrehajtani az 50 napot meghaladó távollét esetén is a távolét (szabadság stb.) megkezdése előtt.

30.7. Az NBF elnöke, a biztonsági vezető valamint a NATO, EU, NYEU Központi Nyilvántartó vezetője – ha súlyos szabálytalanságot vagy működési zavart észlel – soron kívül is bármikor elrendelhet tételes bizottsági ellenőrzést.

IX. fejezet
A MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE ESETÉN SZÜKSÉGES ELJÁRÁSOK, A MINŐSÍTETT ADATOK VESZÉLYHELYZETBEN TÖRTÉNŐ VÉDELME

31. Veszélyhelyzeti terv

A „Veszélyhelyzeti Terv”-ben meghatározott szabályok, feladatok és tevékenységek, alkalmazására akkor kerül sor, ha fennáll annak a veszélye, hogy a nemzeti és külföldi minősített adat illetéktelen kezekbe kerül vagy megsemmisül.

A minősített nemzeti és külföldi minősített adat biztonságának bármely módon történő megsérülését a biztonsági vezető haladéktalanul köteles dokumentálni és jelenteni az NBF-nek.

31.1. A minősített információ biztonságának megsértése esetén

32. A nemzeti és külföldi minősített adathordozóhoz való hozzáférésre kijelölt személy - különösen a titkos ügykezelő - igazolatlan távolléte esetén szükséges intézkedések

33. Az elektronikus védelmi berendezés indokolt és indokolatlan működése esetén követendő eljárás

33.2. <u>Elektronikus rendszer indokolt működésbe lépése esetén:</u>
a) A reagáló erő köteles :

33.3. Elektronikus védelmi berendezés <u>Indokolatlan működés esetén</u>
a) A reagáló erő köteles :

b) A riasztás okának kiderítése után vissza kell állítani az eredeti helyzetet.

34. A biztonsági kulcsok és tartalék példányaik, valamint a kódok lezárt borítékjai kezelésére vonatkozó szabályok.

35. Tűz, elemi csapás bekövetkezése esetén szükséges intézkedések.

35.1. Eljárásrend munkaidő alatt keletkező tűz esetén:
35.2. Eljárásrend munkaidőn kívül keletkezett tűz esetén:
35.3. Eljárásrend munkaidőben történt vízvezeték törése esetén:
35.4. Eljárásrend munkaidőn kívül történt vízvezeték törése esetén:

36. Eljárás természeti katasztrófa esetén

37. Eljárás szükségállapot esetén

37.1. Az adminisztratív zóna evakuálásának rendje:

38. Eljárás az iratkezelés szabálytalanságából adódó sérelem esetén

39. További biztonsági intézkedések

X. fejezet
ZÁRÓ RENDELKEZÉSEK

ÖSSZEFOGLALÁS

Irányadó szakemberek egyetértenek abban, hogy a minősített adatok kezelésével összefüggő szabályozás újragondolása időszerű volt. Különösen időszerűvé tették ezt az Európai Unió által megfogalmazott direktívák és az Uniós soros elnökségi feladatok is. A szabályozásban jól érzékelhetőek a komplex információvédelmi alapelvek és a komplex védelmi intézkedések alkalmazásának igénye.
A személyi, adminisztratív és a fizikai biztonsági követelményrendszer egyértelműen megfogalmazott, az akkreditációs folyamatba jól beilleszkedő, számon kérhető pontrendszeren alapuló alrendszereket alkotnak. Az viszont tapasztalati tény, hogy a közigazgatás nincs felkészülve a fizikai biztonsági követelmények teljesítésére, annak ellenére sem, hogy a szabályozás haladékot ad a szervezetek számára a megvalósítást illetően.
Az elektronikus védelem területén viszont irányadó szakemberek szerint is további egységes és világos követelményrendszer megfogalmazása szükséges, különösen a minősített adatok elektronikus rendszereken történő kezelésével és továbbításával összefüggésben.
Ezt különösen fontos kiemelni, hiszen napjainkban szinte minden minősített adat, elektronikus adathordozón kerül előállításra, tárolásra, feldolgozásra és többnyire aminősített adatok elektronikus továbbításával összefüggésben fogalmazódnak meg a felhasználói igények. Ugyanakkor a közigazgatás nem tudja értelmezni – és nem is érti – az elektronikus védelmi intézkedések kialakításának szükségességét és rendszerint a túlzott anyagi erőforrásokra (illetve annak hiányára) hivatkozva vonakodik teljesíteni az ezzel összefüggő beruházásokat.

FELHASZÁLT IRODALOM

[1] A minősített adat védelméről szóló 2009 évi CLV. törvény

[2] A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010.(III.26.) Korm. rendelet. (58.§ (1),(2))

[3] A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Korm. rendelet. 49§-51§

[4] MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények; A mellék-let, A 8.1- A 8.3. p.

[5] MSZ ISO/IEC 17799 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002), 8.1 – 8-3. p.

[6] Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszer (MIBIK), Informatikai Biz-tonsági Követelmények v 1.1. 2008, p. 76-87.

[7] ISO/IEC 20000-1 Information technology – Service management - Part 1: Specification; 3.3. p. és 6.6. p.

[8] Kassai Károly Az elektronikus adatkezelés során szükséges személyi biztonság kérdései.(Hadtudományi Szemle 3. évfolyam 3. szám 2010. 1. oldal)

[9] A Nemzeti Biztonsági Felügyelet elnökének (*NBF bemutatása biztonsági vezetőknek.ppt 2010.11.12)* előadása.

[10] A telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendelet.

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Lipics László
laszlo_lipics@yahoo.de

AZ INFORMÁCIÓS RENDSZEREK SZEREPE AZ INTEGRÁLT HATÁRBIZTONSÁGI RENDSZERBEN

Absztrakt

A szerző a cikkben három információs rendszert mutat be. Egy ezek közül működik, egy rendszerbe állítása folyamatban van, míg az utolsó csak tervezési szakaszban van. Ez utóbbival (határregisztrációs rendszer) kapcsolatban leírja a magyar rendszer működését, melyet a jövőben megvalósuló közös rendszer követendő példájának talál.
Mindhárom rendszerrel kapcsolatban leírja azok magyarországi helyzetét, feltárja a problémákat és tesz néhány javaslatot is.

Three information systems are demonstrated in this article. One of these is working, one is putting into a system and the last is only being planned. The letter one (the border registration system) is presented through the Hungarian system, which could be the example for the European Union's common system in the next future.
In connection with all three systems the problems the Hungarian situation is described and are digested, moreover some suggestions are nominated.

Kulcsszavak: fejlesztés, Vízuminformációs Rendszer, Eurodac, határregisztrációs rendszer, idegenrendészet ~ development, Visa Information System (VIS), Eurodac, border registration system, foreign-order

BEVEZETÉS

Jelen írás fő célja az Európai Unió integrált határbiztonsági rendszerével kapcsolatba hozható, azon információs rendszerek bemutatása, amelyek ma még kísérleti, fejlesztési szakaszban vannak, valamint a várhatóan megvalósuló, még csak ötletek szintjén lévő rendszereket.

A bővülő Európai Unióban nemcsak a határellenőrzések végrehajtását, hanem a kiegyenlítő intézkedések közé tartozó mélységi migrációs (idegenrendészeti) ellenőrzések véghezvitelét is segítik e rendszerek. Ehhez a szerző be kívánja mutatni, hogyan alkalmazhatóak, illetve hogyan lehetnének hasznosíthatóak e területen is a rendszerek. A

szerző hipotézise szerint néhány dologban a határellenőrzés terén továbbra is élen jár Magyarország.

A cikk csak a rendvédelmi célból alkalmazható információs rendszerekkel foglalkik, a bűnügyi területen létrehozott hálózati alkalmazásokkal, valamint a működő Schengeni Információs Rendszerre – melyet a szerző egy korábbi cikkében [1] az integrált határbiztonsági rendszerrel együtt részletesen ismertetett – nem tér ki.

1. VÍZUMINFORMÁCIÓS RENDSZER

A Tanács által elfogadott iránymutatások alapján 2002. június 21-22-i sevillai ülésén az Európai Tanács felvetette a vízumadatok közös azonosítási rendszerének létrehozását. Egy megvalósíthatósági tanulmány elkészítésére kérte fel a Bizottságot. 2003. június 5-6-án a Tanács elfogadta a bemutatott megvalósíthatósági tanulmányt, mely alapján továbbra is szükségesnek tartotta a VIS létrehozását és megerősítette annak céljait, egyben felkérte a Bizottságot a VIS kifejlesztése érdekében a tagállamokkal együttműködésben végzett előkészítő munkája folytatására. A thessaloniki ülésén az Európai Tanács már a lehető legkorábbi a VIS fejlesztést sürgette, pontos tervet kért a kifejlesztésre, a megvalósításra és az üzembe állításra, valamint a szükséges pénzügyi eszközök bevonását lehetővé tevő megfelelő jogalapra vonatkozó irányvonalakat állított fel. Végül a Tanács 2004. június 8-án döntött Vízuminformációs Rendszer létrehozásáról.[2]

Létrejön a vízumadatok tagállamok közötti cseréjét kezelő rendszer, a továbbiakban Vízuminformációs Rendszer (VIS), amely az engedéllyel rendelkező nemzeti hatóságok számára lehetővé teszi a vízumadatok bevitelét és frissítését, valamint az adatok elektronikus úton való megtekintését.

A megvalósításhoz az alábbi feladatokat tartották szükségesnek végrehajtani:

a) a rendszer fizikai architektúrájának megtervezése, ideértve a kommunikációs hálózatot is;

b) azok a technikai szempontok, amelyek a személyes adatok védelmével kapcsolatos vonatkozással bírnak;

c) azok a technikai szempontok, amelyek komoly pénzügyi hatással bírnak a tagállamok költségvetésére, vagy komoly technikai hatással bírnak a tagállamok nemzeti rendszerére;

d) a biztonsági követelmények kidolgozása, ideértve a biometrikus jellemzőket is.

A SIS rendszerrel való párhuzamosságot már ekkor felfedezték, hiszen a Bizottság figyelmébe ajánlották, hogy segítségükre lehet a SIS II. kiépítésére hivatott bizottság is.

A VIS felépítése a SIS rendszerhez hasonló, azaz van egy központi szerver (CS-VIS) és egy interfész mindegyik tagállamban, a nemzeti szerver (NI-VIS), a szervereket pedig egy hálózat köti össze. A központi szerverek ugyanúgy Strasbourgban és Sankt Johann im Pongauban (tartalék) van, ahogy a SIS-nél megismertük.

A létrehozásról szóló döntés követően négy évvel újabb rendelet [3] megalkotása vált szükségessé, a VIS céljának, működőképességének és feladatainak meghatározása és a tagállamok közötti, a vízumadatok cseréjére vonatkozó feltételek és eljárások megállapítása érdekében, továbbá hogy megkönnyítsék a vízumkérelmek elbírálását és a kapcsolódó határozatokat.

A VIS célja, hogy a kérelmekkel és az ezekhez kapcsolódó határozatokkal kapcsolatos adatok tagállamok közötti cseréjének megkönnyítése révén javítsa a közös vízumpolitika

végrehajtását, a konzuli együttműködést és a központi vízumhatóságok közötti konzultációt az alábbiak érdekében:[1]

a) a vízumkérelmezési eljárás megkönnyítése;

b) annak megelőzése, hogy a kérelem elbírálásáért felelős tagállam meghatározására vonatkozó kritériumok kikerülhetők legyenek (azaz megakadályozza a "vízum shoppingot");

c) a csalás elleni küzdelem megkönnyítése;

d) a külső határátkelőhelyeken és a tagállamok területén belüli ellenőrzések megkönnyítése;

e) segítségnyújtás az olyan személyek azonosításában, akik esetleg nem, vagy már nem teljesítik a tagállamok területére történő beutazásra, az ott-tartózkodásra vagy letelepedésre vonatkozó feltételeket;

f) egy harmadik ország állampolgára által a tagállamok egyikében benyújtott menedékjog iránti kérelem megvizsgálásáért felelős tagállam meghatározásának megkönnyítése;

g) hozzájárulás a bármely tagállam belső biztonságát fenyegető veszélyek megelőzéséhez.

Amint az a felsorolásban az általam kiemelt szövegből kitűnik a VIS segíti a határellenőrzést végrehajtó szervek, a mélységi migrációs ellenőrzést végzők munkáját, valamint a tagállamok területen okmány nélkül tartózkodó személyek azonosítását.

A VIS-ben rögzíthető adatok:

1. technikai jellegű adatok (a kérelem száma; státusinformáció, amely jelöli a vízum kérelmezésének tényét; a hatóságot megnevezése, amelyhez a kérelmet benyújtották; a kérelem benyújtás helye és időpontja; a kérelmezett vízum típusa)
2. személyes és biometrikus adatok:
   - vezetéknév, születéskori vezetéknév, korábbi vezetéknév (nevek) és utónév (nevek); nem; születési dátum, hely és ország;
   - jelenlegi állampolgárság és születéskori állampolgárság;
   - az úti okmány típusa és száma, a kiállító hatóság, valamint a kiállítás és a lejárat időpontja;
   - lakóhely;
   - jelenlegi foglalkozás és munkahely; tanulók esetében az iskola neve, valamint kiskorúak esetén a kérelmező szüleinek vezetékneve és utóneve(i);
   - fénykép;
   - ujjlenyomat.
3. beutazáshoz kapcsolódó adatok:
   - a meghívólevelet kiállító személy adatai;
   - fő úti cél és a tartózkodás tervezett időtartama;
   - az utazás célja;
   - az érkezés és a visszaindulás tervezett időpontja;
   - az első beutazás tervezett határszakasza vagy átutazási útvonal.

A fentieken kívül pozitív elbírálás esetén a technikai jellegű adatok kiegészülnek a vízum kiállításáról szóló státusinformációval; a vízumot kiállító hatóság megnevezésével; a vízum kiadásáról szóló döntés meghozatalának helyével és idejével; a vízum típusával és a vízumbélyeg számával, esetleg azzal, hogy a vízumot külön lapon adták ki. A beutazáshoz kapcsolódó adatok kibővülnek annak a területnek a megnevezésével ahová a

[1] VIS-rendelet 2. cikk alapján – kiemelések a szerzőtől

vízumbirtokosnak joga van utazni; a vízum érvényességi idejének kezdetével és lejáratával; a vízum által megengedett belépések számával és az engedélyezett tartózkodási idővel.

Amennyiben a kérelem elbírálása megszűnik, elutasítják, esetleg a vízumot törölik vagy visszavonják, vagy érvényességi idejét lerövidítik, hosszabbítják, újabb technikai jellegű adatokkal bővül a rendszerben tárolt információk köre.

A rendszer képes ugyanakkor arra is, hogy egy kérelmező több kérelmét összecsatolja, vagy az együtt utazók kérelmeit kapcsolja.

A rendszerből való lekérdezés joga nemcsak a vízumkiállító hatóságokat illeti meg, hanem a rendvédelmi szerveket is. A VIS-rendelet minden egyéb szabályozási kérdését megelőzve kiemeli a terrorcselekmények és más súlyos bűncselekmények megelőzése, felderítése és kivizsgálása céljából történő adatfelhasználást.

A szabályozási részt követően első körben a külső határátkelőhelyeken történő ellenőrzéssel kapcsolatban biztosít jogosultságot a rendelet, mely szerint elsősorban a vízumbélyeg száma alapján a vízumbirtokos ujjlenyomatának ellenőrzésével együtt történő kereséshez férnek hozzá a rendszerben tárolt adatokhoz. Ez alól két technikai kivétel van: az első három évben automatikusan lehet csak vízumszám alapján keresni (ujjnyomat-leolvasó berendezések beszerzése), illetve amennyiben a vízumbirtokos ujjlenyomata alkalmatlan az azonosításra. A rendelet ugyanakkor megengedi kizárólag ujjlenyomat alapján való keresést a rendszerben, amennyiben annak célja a személyazonosság megállapítása akár a határátkelőhelyeken, akár a mélységben történik a személy ellenőrzése.

A hatóságok a rendszerből a státuszinformációkhoz, a személyes adatok köréhez és a fényképhez, illetve a korábbi csatolt vízumokhoz, a vízumokkal történt egyéb információkhoz férhetnek hozzá.

Ugyanehhez az adatokhoz férhetnek hozzá a beutazásra, az ott-tartózkodásra és a letelepedésre vonatkozó feltételek teljesülését ellenőrző illetékes hatóságok a térségen belül végrehajtott ellenőrzéseik során, amennyiben ellenőrzésük célja a vízumbirtokos személyazonosságának és/vagy a vízum hitelességének és/vagy a tagállamok területére történő beutazásra, tartózkodásra és letelepedésre vonatkozó feltételek teljesülésének megállapítása.

Mivel a VIS céljai közt szerepel a menedékjoggal kapcsolatos hatáskörök megállapításának elősegítése, így az illetékes menekültügyi hatóságok a menedékjogot kérő ujjlenyomatával történő kereséssel férnek hozzá az adatokhoz.

A VIS-rendelet felhatalmazása alapján a Bizottság meghatározta azon régiókat, ahol el kell kezdeni az adatok gyűjtését, rendszerbe való feldolgozását. [4] Észak-Afrika az első régió, ahol a vízumkérelmek tekintetében a vízumadatok gyűjtését és a VIS-be történő továbbítását meg kell kezdeni, azaz Algéria, Egyiptom, Líbia, Mauritánia, Marokkó és Tunézia.

A Közel-Kelet (Izrael, Jordánia, Libanon és Szíria) lesz a második, míg a Perzsa-öböl térsége (Afganisztán, Bahrein, Irán, Irak, Kuvait, Omán, Katar, Szaúd-Arábia, Egyesült Arab Emírségek és Jemen) a harmadik régió. A schengeni határátkelőhelyeket különálló régióként célozta meg a Bizottság, hiszen a külső határokon benyújtott vízumkérelmek miatt célszerűnek látszik.

A következő lépés a VIS tekintetében a műveletek indítása, azaz a rendszer élesítése lesz. Ez akkor következhet be, amikor a meghatározott intézkedéseket megtették, befejeződött a VIS átfogó vizsgálata, az első régió valamennyi kérelmét a VIS-en keresztül dolgozták fel. Ezek alapján bizakodhatunk, hogy ez a SIS II-höz képest működő rendszerré válhat a közeljövőben. Ugyanakkor kétséges, hogy hosszú távon szükség van-e rá. Ugyanis az Európai Unió vízumpolitikája egyre inkább a liberalizáció irányába mutat. Nemrégiben például a Nyugat-Balkáni országok körében kezdődött a vízummentesség kialakítása, melynek első

köréből kimaradt országok is csatlakozhatnak ezen zónához. [5] Lefordítva a szituációt: minél szélesebb körben alkalmazza az EU a vízummentességet, annál kevésbé éri meg fejleszteni ezt a rendszert.

A rendszerhez való hozzáférés széles körben biztosított a rendvédelmi szervek számára, legyen szó terrorizmusról, bűnözésről vagy „csak" illegális migrációról. [6] Bár a tavalyi kormányhatározat hiányolta, hogy Magyarországon még nem történtek meg a vízuminformációs rendszerrel kapcsolatos szabályozások, a VIS implementálása, [7] ezt a fogyatékosságot a kormány[2] és az illetékes miniszter[3] az idei évben pótolta. Például a Bevándorlási és Állampolgársági Hivatal (BÁH) ki lett jelölve központi vízumhatóságnak és az ehhez kapcsolódó, a VIS rendeletben foglalt feladatokra.[4]

A Vízuminformációs Rendszerhez hozzáféréssel rendelkező idegenrendészeti hatóságok a Bevándorlási és Állampolgársági Hivatal, a Rendőrség, a vízumkiadó hatóságok. A mélységi migrációs ellenőrzések tekintetében Bevándorlási és Állampolgársági Hivatal, a Rendőrség, valamint a BÁH regionális igazgatóságainak van joga hozzáférni az adatokhoz.

Jelenleg még a VIS Magyarországon nem üzemel[5], de a külső határokon már kiépítése megkezdődött és próbaüzeme megkezdődött. A vízumkiadáshoz szükséges rendszerként még a magyar üzemel, mely a VIS-hez képest kevesebb információt tartalmaz. Az ország területen végrehajtott idegenrendészeti ellenőrzésekhez a mobil ujjlenyomat-olvasók még nem kerültek beszerzésre.

Ez azért nem jelent komoly hátrányt, mert csak tavaly év végén határozták meg, hogy VIS-nek milyen ujjlenyomatokat kell tartalmazni és milyen lenyomatokon keresztül lehet ellenőrizni. [8] A Központi Vízuminformációs Rendszerbe kizárólag 500 (+/- 1%) képpont inchenként (dpi) névleges felbontású és 256 fényességi szintű („grey level") tízujjas sík ujjlenyomatképeket lehet bevinni. Az ellenőrzésekhez 1, 2, 4 vagy tízujjas beolvasás lehetséges. Ez utóbbit kizárólag azonosítási célból lehet használni.

Véleményem szerint a jogalkotó azon felismerése, hogy az Alkotmányvédelmi Hivatal[6] munkatársainak is hozzáférést kellene biztosítani a vízuminformációs rendszerhez - hiszen több olyan jellegű feladatot szab a rá vonatkozó törvény [9], melyhez szükség lehet a VIS használatára, például külföldiek szűrése a letelepedéshez, menekültkérelemhez, de terrorcselekmények felderítését is végzi[7] - helyes. Ennek érdekében módosítják [10] a nemzetbiztonsági szolgálatokról szóló törvényt is, a VIS-rendelet teljeskörű hatálybaléptetéséhez kapcsolódóan.

A bemutatott Vízuminformációs Rendszer kiépítése és kipróbálása folyamatban van. Az első régióban megkezdték használatát, az adatok értékelése, majd további régiókban történő kipróbálás hamarosan elindulhat.

---

[2] Egyes migrációs tárgyú kormányrendeleteknek a Vízuminformációs Rendszer alkalmazásával, valamint a Vízumkódex hatálybalépésével összefüggő jogharmonizációs célú módosításáról szóló 96/2010. (III. 31.) Kormányrendelet

[3] Egyes migrációs tárgyú miniszteri rendeleteknek a Vízuminformációs Rendszer alkalmazásával, valamint a Vízumkódex hatálybalépésével összefüggő jogharmonizációs célú módosításáról szóló 12/2010. (IV. 2.) IRM rendelet

[4] A harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló 2007. évi II. törvény végrehajtásáról 114/2007. (V. 24.) Kormányrendelet 21. § (1) bekezdés

[5] Az Országos Rendőr-főkapitányság Határrendészeti Főosztály tájékoztatása szerint az üzembe helyezés 2011. tavaszán várható, hozzáférés első körben csak a külső határátkelőhelyen lesz a BÁH-on kívül.

[6] 2010. június elsejétől, korábbi neve: Nemzetbiztonsági Hivatal; az új megnevezés törvényi alapja: A Magyar Köztársaság minisztériumainak felsorolásáról szóló 2010. évi XLII. törvény 3. § (5) bekezdés

[7] Nbtv. 5. §

Magyarországon a rendszer működéséhez szükséges eszközök beszerzése, a rendszer kiépítése folyamatban van. A magyar vízumkiadó rendszer hálózatán a rendszer működőképes lehet. A VIS-el kapcsolatos oktatások 2011. tavaszára vannak tervezve - az ORFK Határrendészeti Főosztályának tájékoztatása alapján.

Amennyiben kialakul az Európai Unió egységes vízumnyilvántartó rendszere, megkönnyíti a harmadik országbeli személyek személyazonosítását, területen való jogszerű tartózkodásának ellenőrzését, rendészeti szempontból ezek a legfontosabbak. A biztonság szempontjánól talán ennél is fontosabb, hogy a külképviseleteken a vízum kiadása előtt a személy, illetve az általa benyújtott kérelem valóságtartalma könnyebben ellenőrizhetővé válik. Magyarország tekintetében szintén a biztonság erősítését szolgálja, hogy az Alkotmányvédelmi Hivatalt is feljogosítja a jogszabály az adatokhoz való hozzáféréshez.

2. EURODAC/AFIS[8]

A tagállamok 1990. június 15-én Dublinban megkötötték az Európai Közösségek tagállamainak egyikében benyújtott menedékjog iránti kérelem megvizsgálására illetékes állam meghatározásáról szóló egyezményt (a továbbiakban: a dublini egyezmény)[9].

A dublini egyezmény alapján a párhuzamos eljárások kiküszöbölése érdekében meg kell állapítani a menedékjogot kérelmező személyek és a Közösség külső határainak jogellenes átlépése miatt letartóztatott személyek azonosságát. A Tanács és a Bizottság úgy találta, hogy erre a legmegfelelőbb eszköz az ujjlenyomat azonosítás. Ezért az egyezmény aláírása után 10 évvel kialakították az Eurodac rendszert. [11]

Az Eurodac egy olyan, ujjlenyomatokat tároló európai adatbázis, amely kizárólag a menedékjogi kérelmet benyújtók azonosítására szolgál. Minden 14 éven felüli személytől, aki az Európai Unióban vagy azon kívül menedékkérelmet nyújt be, az eljárás részeként rutinszerűen ujjlenyomatot vesznek.

Az Eurodac rendszer elemei a rendelet szerint a központi egység, a számítógépes központi adatbázis és adatátviteli eszközök, de valójában itt is létezik nemzeti egység.

Az egyes tagállamok haladéktalanul ujjlenyomatot vesznek minden, a 14. életévét betöltött menedékjogot kérelmező személytől, és a kérelmező személyes adataival haladéktalanul továbbítják a központi egység számára.

A központi adatbázis nyilvántartás adattartalma:

a) a származási hely szerinti tagállam, a menedékjog iránti kérelem benyújtásának helye és időpontja;
b) az ujjlenyomatadatok;
c) az érintett személy neme;
d) a származási hely szerinti tagállam által használt referenciaszám;
e) az ujjlenyomatvétel dátuma;
f) az adatok a központi egységhez történő továbbításának dátuma;
g) az adatok a központi adatbázisba történő bevitelének dátuma;
h) a továbbított adatok címzettjének/címzettjeinek adatai és a továbbítás dátuma(i).

A felvitt adatokat legfeljebb 10 évig tárolja a központi egység. A kérelmet be nem nyújtó, de külső határon elfogott olyan illegális migránsoktól, akik nem kerülnek azonnal toloncolásra származó, személyazonosítást szolgáló ujjlenyomatokat pedig legfeljebb kettő évig tárolja.

[8] Automated Fingerprint Identification System

[9] Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities - Dublin Convention In: Az Európai Unió Hivatalos lapja HL C 254., 1997.8.19., 1—12. o.

Amikor valaki menedékjog iránti kérelmet nyújt be, a fenti adatok és közte az ujjlenyomat a központi egységhez kerülnek továbbításra, ahol a rendszer automatikusan összehasonlítja azokat az adatbázisban szereplő többi ujjlenyomattal. A rendszer segít a hatóságoknak a szükséges iratok nélkül az EU területére lépő, illetve valamely másik tagállamban korábban már menedékkérelmet benyújtott személyek kiszűrésében. Találat esetén a rendszer azonnal értesítést küld, ha a beküldött ujjnyomatok megegyeznek ujjnyomat-azonosító rendszerben tárolt bármelyik mintával. Ilyen esetben az ujjlenyomatot beküldő országnak jogában áll abba az országba utasítani a kérelmezőt, ahol az belépett az Európai Unió területére vagy először folyamodott menedékjogért. (Ha nem kíván élni e jogával, saját maga köteles elbírálni a kérelmet, illetve a rendszerben nem szereplő ujjlenyomatokról szóló negatív választ is azonnal küldi a központi egység.)

Az egyes tagállamok jelölik ki azokat a hatóságokat, amelyek hozzáférhetnek a központi adatbázisban nyilvántartott adatokhoz. A tagállamok e hatóságok jegyzékét közlik a Bizottsággal.

A jogszabály végrehajtására egy másik rendeletet [12] is alkotott a Tanács, mely előírja, hogy az ujjnyomokat előírt formátumban (ld. 1. sz. melléklet) kell levenni és digitális formában kell tárolni. A központi egység az összehasonlítást a megkeresések beérkezésének sorrendjében végzi. A rendelet előírása alapján minden megkereséssel 24 órán belül foglalkozni kell, de az elektronikus úton továbbított adatok esetében a tagállam kérhet egy órán belül elvégzendő különösen sürgős összehasonlítást.

Magyarországon a nemzeti egység feladatait a menekültügyi eljárásokhoz kapcsolódóan a Bevándorlási és Állampolgársági Hivatal látja el,[10] egyéb esetekben Bűnügyi Szakértői és Kutatóintézet Daktiloszkópiai Szakértői Osztálya, mely egyben a magyar szakirányításért (megfelelő adatok rendszerbe juttatása, képzés stb.) is felelős.

A BÁH és a Rendőrség munkaállomásai a Belügyminisztérium hálózatán keresztül közvetlenül csatlakoznak a Központi Daktiloszkópiai Nyilvántartáshoz.

A rendszer megbízhatóan működik olvasható a Bizottság jelentésében [13]: az Eurodac központi egység a teljes idő 99,84 %-ában volt elérhető.

2008-ban két „téves találatot", vagyis a Csalás elleni Információs rendszer (AFIS) által végzett téves azonosítást jelentettek a Bizottságnak, bár a tagállamok nem kötelesek értesíteni a Bizottságot a téves találatokról. Ugyanakkor a rendszer továbbra is rendkívül pontosnak tekinthető, hiszen két év alatt a több mint 1,5 millió lekérdezésből és 300 000-et meghaladó találatból csupán háromszor fordult elő téves találat – állapítja meg a jelentés.

Az AFIS rendszerben a menekültkérelmet benyújtó személyek által megadott személyes adatok mellett a személyek ujjlenyomata is rögzíthető, illetve ellenőrizhető. Ezzel meg lehet akadályozni a menekültügyi eljárások multiplikálódását, továbbá a személyek azonosítását is. A terrorellenes intézkedések közt felvetődött azon ötlet is, hogy a gyanúsítható személyek ujjnyomatát ellenőrzik az Eurodac adatbázisban. Azonban adatvédelmi szempontból ez kifogásolható, mivel az adatok felhasználási köre a rendeletben e célból nem biztosított. [14]

[10] A menekültügy szervezeti rendszeréről szóló 52/2007. (XII. 11.) IRM rendelet 1. § (2) c)

3. HATÁRREGISZTRÁCIÓS RENDSZER

Az Európai Unió határellenőrzési politikájában új fejezetet nyithat a közös határregisztrációs rendszer[11], mely egy stratégia mérföldkő. A létező, országonként különböző rendszereket kellene összehangolni vagy egy közös újat létrehozni.

A határregisztrációs rendszer célja az, hogy a tagállamok illetékes hatóságai az ellenőrzött harmadik országbeli személy tartózkodásának jogszerűségét meg tudják állapítani. Egyrészt, hogy a külföldi az arra kijelölt helyen és időben lépte át a külső határt, másrészt az engedélyezett tartózkodási idejét nem lépte túl. A rendszerbe történő ellenőrzés lehetősége nemcsak a külső határokon szolgálatot teljesítő hivatalnokoknak, hanem a terület mélységében végrehajtott idegenrendészeti ellenőrzést véghezvivő tisztviselőknek engedélyezett lesz. A rendszer figyelmeztetést küldene a nemzeti hatóságok számára, amikor lejár egy egyén engedélyezett tartózkodási ideje az EU-ban, és nem rögzítették kilépési adatait. 2011-ben várható a jogalkotás [15] a határregisztrációs rendszerre vonatkozóan, mely megalapozná annak fejlesztési lehetőségeit.

A megvalósításhoz szükségesnek vélem az alábbiakat végrehajtani:

a) a rendszer fizikai architektúrájának megtervezése, beleértve a kommunikációs hálózatot is;
b) a már működő határregisztrációs rendszerek integrálása az új rendszerbe;
c) a rendszer adattartalmának és adatkezelési idő meghatározása;
d) az előzőhöz kapcsolódóan azok a technikai szempontok, amelyek a személyes adatok védelmével kapcsolatos vonatkozással bírnak;
e) azok a technikai szempontok, amelyek komoly pénzügyi hatással bírnak a tagállamok költségvetésére, vagy komoly technikai hatással bírnak a tagállamok nemzeti rendszerére;
f) a biztonsági követelmények kidolgozása.

Magyarországon 2000 óta működik, az Európai Unió által is mintaként szolgáló határregisztrációs rendszer. A rendszer BorderGuard (útlevél-ellenőrző) egysége automatikusan ellenőrzi az útlevelet (5-féle fény alatt vizsgálja, ellenőrzi az alapadatokat) a nemzeti és a nemzetközi körözési rendszerekben, riasztást ad, ha találatot észlel. Emellett regisztrálja az átlépést. A Rendszám Felismerő Modul (LPR) infravörös technológia alkalmazásával a határon átkelni szándékozó jármű rendszámát beolvassa, és szintén ellenőrzi a fenti helyeken.

A magyar határregisztrációs rendszer fejlesztése megtörtént, 2010. január 31. óta képes a harmadik országbeliek tartózkodási idejének számítására. Emiatt az első három napon öt magyar-ukrán átkelőhelyen 245 visszairányítás történt.[16] Összehasonlításul: 2009-ben ugyanitt mindössze 55 visszairányítás történt ezen okból.

Ugyanakkor a határregisztrációs rendszer megvalósítása során nem lehet figyelmen kívül hagyni az időközben megvalósult egyéb technikai fejlesztéseket sem. A határforgalom ellenőrzése egyre inkább az automatizálás felé halad. Elektronikus utazási engedély rendszer, regisztrált utazói státusz, valamint az arcképfelismerő rendszer fejlesztése van napirenden.

A regisztrált utazói státusz elméletileg azon határátlépésre jelentkező, harmadik országokból származó állampolgárokra vonatkozhatna, akik kis kockázatot jelentenek az Európai Unió biztonsága szempontjából. Ez egy önkéntes alapon működő előzetes ellenőrzési eljárás, melynek pozitív elbírálása esetén az azt igénylő személynek a határátkelőhelyeken

[11] A Stockholmi Program belépést, illetve kilépést nyilvántartó elektronikus rendszert említ - A Bizottság közleménye a Tanácsnak és az Európai Parlamentnek: A szabadság, a biztonság és a jog érvényesülésén alapuló térség a polgárok szolgálatában Brüsszel, 10.6.2009 COM(2009) 262 végleges 20.o.

nem kellene várakoznia, hanem a külön sávon, a felállítandó automata kapukon keresztül léphetné át az EU határát.

Az elektronikus utazási engedély rendszer a harmadik országok nem vízumköteles állampolgárai előzetes vizsgálata abban a tekintetben, hogy teljesíti-e a belépési feltételeket. Az ezzel élni kívánó az utazás megkezdése előtt elektronikus kérelmet nyújtana be, amely tartalmazná a személyazonosító, valamint az útlevélben szereplő és az utazásra vonatkozó adatokat, mely alapján eldöntenék azt, hogy a személy beléptethető-e az Európai Unióba.

Az arcképfelismerő rendszer fejlesztése az egyéb biometrikus (ujjnyomat, írisz) azonosítókat válthatná fel, illetve egészíthetné ki. A kamara által rögzített képet hasonlítaná össze az útlevélben elhelyezett fényképpel. Hátránya a rendszernek, hogy az útlevélben fellelhető hamisításokat nem tudja kiszűrni, csak a két kép összehasonlításra képes.

Az Európai Unió határregisztrációs rendszerének kifejlesztése az integrált határbiztonsági rendszer evolúciójában fontos lépés. A harmadik országok állampolgárai útlevelének kezelése mind ki-, mind befelé kötelező. Azonban a külső határokon átlépő személyek útlevelében a bélyegzőlenyomatok nem mindig olvashatóak, illetve néhány alkalommal a kezelést is elmulasztják az ott dolgozó határőrök. Emiatt az idegenrendészeti ellenőrzést végrehajtók a személyek tartózkodási idejének betartását nem minden alkalommal tudják végrehajtani. Ennek megoldása lehet az egységes határregisztrációs rendszer, melyben nemcsak a külső határok átlépésekor tudnának a határellenőrzési szervek beosztottai ellenőrizni, hanem a mélységi ellenőrzést végrehajtók is. Úgy gondolom továbbá, hogy a magyar példa a határregisztrációs rendszer alkalmazására, fejlesztésére megfelelő lehet az Európai Unió számára.

ÖSSZEFOGLALÁS

A cikkben egy működő, egy megvalósítás alatt lévő és egy ötlet szintjén lévő információs rendszert mutattam be.

Az Eurodac egy olyan, ujjlenyomatokat tároló európai adatbázis, amely kizárólag a menedékjogi kérelmet benyújtók azonosítására szolgál. A hozzá kapcsolódó működő, AFIS rendszerben a menekültkérelmet benyújtó személyek által megadott személyes adatok mellett a személyek ujjlenyomata is rögzíthető, illetve ellenőrizhető. Az AFIS egyben a csalások megelőzésére is szolgál, hiszen egyből visszajelez, amennyiben találatot észlel. A rendszer megbízhatóan működik, a központi egység a teljes idő 99,84 %-ában volt elérhető.

A menekültügyi eljárásokhoz kötődő ujjlenyomat-vételekkel, ellenőrzésekkel meg lehet akadályozni a menekültügyi eljárások multiplikálódását, továbbá a személyek azonosítását is.

A vízumadatok tagállamok közötti cseréjét kezelő rendszer, azaz a Vízuminformációs Rendszer (VIS), az engedéllyel rendelkező nemzeti hatóságok számára lehetővé teszi a vízumadatok bevitelét és frissítését, valamint az adatok elektronikus úton való megtekintését.

A VIS a rá vonatkozó jogforrásban deklaráltan segíti a határellenőrzést végrehajtó szervek, a mélységi migrációs ellenőrzést végzők munkáját, valamint a tagállamok területen okmány nélkül tartózkodó személyek azonosítását.

A Vízuminformációs Rendszer kiépítése és kipróbálása folyamatban van. Az első régióban megkezdték használatát, az adatok értékelése, majd további régiókban történő kipróbálás hamarosan elindulhat.

Amennyiben az egységes vízumnyilvántartó rendszere teljes mértékben üzemképes lesz, az megkönnyíti a harmadik országbeli személyek személyazonosítását, területen való jogszerű tartózkodásának ellenőrzését, rendészeti szempontból ezek a legfontosabbak. A biztonság

szempontjából talán ennél is fontosabb, hogy a külképviseleteken a vízum kiadása előtt a személy, illetve az általa benyújtott kérelem valóságtartalma könnyebben ellenőrizhetővé válik.

Az Európai Unió határregisztrációs rendszerének kifejlesztése az integrált határbiztonsági rendszer evolúciójában fontos lépés, azonban önmagában nem értelmezhető, csak az ismertetett egyéb automatizálásokra irányuló fejlesztések függvényében. Az egységes határregisztrációs rendszer előnye abban rejlene, ha nemcsak a külső határok átlépésekor tudnának a határellenőrzési szervek beosztottai ellenőrizni, hanem a mélységi ellenőrzést végrehajtók is. A cikkben javaslatot tettem egyúttal a határregisztrációs rendszer megvalósításához szükséges lépésekre.

Mindhárom információs rendszernél fontos annak biztosítása, hogy a rendszerek operatív irányítása hatékonyan biztosítja a folyamatos működést és a megszakításmentes (24/7) szolgáltatást, az adatintegritást és –biztonságot. Lényeges továbbá, hogy az irányítást olyan szerv végezze, amely képes az egyes rendszerek felhasználói által elvárt szolgáltatási minőséget nyújtani. Ennek létrehozására már született döntés: a Schengeni Információs Rendszer kibővített adattartalommal rendelkező második verziója (SIS II) és a VIS rendszerek központja Észtországban lesz. Véleményem szerint ide lehetne költöztetni a másik két, a cikkemben említett rendszer központját is.

Továbbá szükséges lenne már a Hágai programban megfogalmazott SIS, a VIS és az Eurodac átjárhatóságának elérése, illetve a vízumigénylés és határátlépés információk összekapcsolása. Ezek mind az előzőekben megfogalmazott véleményem szükségességét támasztják alá.

Magyarországon az Eurodac/AFIS rendszer működésének jogi szabályozása, működése rendben van.

A VIS alkalmazásához kapcsolódó jogi lépések megtörténtek, a rendszer kiépítése folyamatban van. Hiányosságként értékelem, hogy a mélységi ellenőrzések végrehajtásához jelen pillanatban még a rendszer használatához szükséges oktatások nincsenek tervben, nemhogy az eszközbeszerzések.

A határregisztrációs rendszer idei évi továbbfejlesztett változata, amely már a tartózkodási idő számítására is képes – megítélésem szerint – példaként szolgálhat az Európai Unió egységes rendszerének.

Felhasznált irodalom:

[1] Lipics László: A Schengeni Információs Rendszer szerepe az integrált határbiztonsági rendszerben Hadmérnök, 2010/3

[2] A Tanács Határozata (2004. június 8.) a Vízuminformációs Rendszer létrehozásáról (VIS) (2004/512/EK)

[3] Az Európai Parlament és a Tanács 767/2008/EK rendelete (2008. július 9.) a vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről (VIS-rendelet)

[4] A Bizottság Határozata (2009. november 30.) a vízuminformációs rendszer (VIS) működésének megkezdése tekintetében az első régiók meghatározásáról (2010/49/EK)

[5] Lipics László: A balkáni országok vízumkönnyítése 2010. 02. 25. Elérhető: http://www.biztonsagpolitika.hu/?id=16&aid=836&title=A_balk%C3%A1ni_orsz%C3%A1gok_v%C3%ADzumk%C3%B6nny%C3%ADt%C3%A9se

[6] Hegyaljai Mátyás: A vízuminformációs rendszer rendvédelmi célú használata In: Pécsi Határőr Tudományos Közlemények VII. 129-137. o. ISSN 1589-1674

[7] A Magyar Köztársaságnak a szabadság, biztonság és a jog érvényesülése térségében való együttműködésére vonatkozó 2009-2014 közötti kormányzati stratégiájáról szóló 1057/2009. (IV. 24.) Kormányhatározat

[8] A Bizottság Határozata (2009. október 9.) az ujjlenyomatok felbontásával, valamint biometrikus azonosításra, illetve a vízuminformációs rendszerben történő ellenőrzésre való felhasználásukkal kapcsolatos előírások megállapításáról (2009/756/EK)

[9] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (Nbtv.)

[10] Egyes rendészeti és migrációs tárgyú törvények módosításáról, valamint egyes törvényeknek a Vízuminformációs Rendszer bevezetésével összefüggő jogharmonizációs célú módosításáról szóló 2010. évi XL. törvény

[11] A Tanács 2725/2000/EK rendelete (2000. december 11.) a dublini egyezmény hatékony alkalmazása érdekében az ujjlenyomatok összehasonlítására irányuló „Eurodac" létrehozásáról

[12] A Tanács 407/2002/EK rendelete (2002. február 28.) a Dublini Egyezmény hatékony alkalmazása érdekében az ujjlenyomatok összehasonlítására irányuló „Eurodac" létrehozásáról szóló 2725/2000/EK rendelet végrehajtására vonatkozó egyes szabályok megállapításáról

[13] A Bizottság jelentése az Európai Parlamentnek és a Tanácsnak: Éves jelentés a Tanácsnak és az Európai Parlamentnek az EURODAC központi egység 2008. évi tevékenységéről Brüsszel, 2009.09.25. COM(2009) 494 végleges

[14] Az Eurodac-ot bírálta Peter Hustinx 2009.10.09. Forrás: http://www.sg.hu/cikkek/70256/az_eurodac_ot_biralta_peter_hustinx Letöltés ideje: 2010. június 30.

[15] Öt éven belül létrehoznák a biztonság egységes térségét Forrás: http://www.bruxinfo.hu/index.php?lap=dokument/dokument&dok_id=26865 Letöltés ideje: 2010. június 20.

[16] Lejárt a 90 nap: visszairányítások a magyar-ukrán határállomásokon Forrás: http://hvg.hu/itthon/20100204_magyar_ukran_hatar_visszairanyitas_blokad?s=24h Letöltés ideje: 2010. június 20.

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Lipics László
laszlo_lipics@yahoo.de

ROBOTJÁRMŰVEK ALKALMAZHATÓSÁGI LEHETŐSÉGEI AZ INTEGRÁLT HATÁRBIZTONSÁGI RENDSZER MŰKÖDÉSÉBEN

„We said why not get a jump start on the initiative"
Michael Wimberly[1]

Absztrakt

A cikkben bemutatásra kerülnek az Európai Unióba irányuló migráció kezelését szolgáló integrált határbiztonsági rendszerben jelenleg rendelkezésre álló eszközök, valamint az automatizálásban látható fejlesztések. Komplex megközelítéssel leírja a szerző a robotok alkalmazhatóságát, valamint a vízi, légi és szárazföldi távirányítású járművek közül bemutat néhányat, melyek alkalmazhatóak lennének határellenőrzési feladatra. Végezetül Magyarországon kevésbé ismert Talos rendszer fejlesztését mutatja be és megállapítja, hogy (megfelelő feltételek fennállása esetén) elgondolása helyes, azaz a robotjárművek alkalmazhatóak az integrált határbiztonsági rendszerben.

In the article the available tools and the developments of integrated border management are demonstrated, which put off the illegal migration to the European Union. With complex approach the author wrote about automaton practice, moreover any remote controlled boat, airplane and vehicle are introduced, which could be put in for border control. At last the Talos system developing is demonstrated and the writer appointed his idea is right (if some conditions exist), the robots can be applied in the integrated border system.

***Kulcsszavak**: integrált határbiztonsági rendszer, Talos, illegális migráció, robotjármű ~ integrated border managment, Talos, illegal migration, unmanned vehicle*

[1] Az idézet fordítása: „Azt mondtuk, miért ne ugorhatnánk egyet és próbálhatnánk ki?"
Frank Tiboni: Border Patrol to deploy unmanned aerial vehicles USA Today 17/5/2004 Forrás: http://www.usatoday.com/tech/news/techpolicy/2004-05-17-border-uav_x.htm Letöltés ideje: 2010. november 5.

BEVEZETÉS

A Magyar Köztársaság 2007. december 21. óta teljes jogú schengeni tagállam. Ez azt jelenti, hogy a szomszédos, szintén teljes jogú schengeni tagállamokkal (Szlovákia, Ausztria, Szlovénia) közös határokon megszűnt a határátlépésre irányuló határellenőrzés. Bárhol, bármikor átléphető az államhatár. Ugyanakkor keleti és déli határaink (Ukrajna, Románia, Szerbia, Horvátország) schengeni külső határokká váltak, mely azt jelenti, hogy Magyarország felel a Schengeni térség szárazföldi határai 15 %-nak megbízható ellenőrzéséért.

Emellett 2008. január elsejétől a Rendőrség feladata a határellenőrzés, mivel a Határőrség megszűnt. Ez azzal is együtt járt, hogy a határellenőrzési szakterületen dolgozók létszáma lecsökkent. Ez a folyamat nem állt meg, jelenleg is tart.

Feltevésem szerint a kieső állomány kompenzálására, a határellenőrzés minőségi szintjének megtartására és javítására a technikai fejlesztés az egyik megfelelő válasz. Ennek egy része lehet a robotjárművek alkalmazása.

1. A KIHÍVÁS

Az Európai Unió és benne Magyarország napjaink egyik legnagyobb kihívása az illegális migráció. Ezt a Nemzeti Biztonsági Stratégia [1] is megerősíti. Ugyanakkor az egyre növekvő migrációs nyomás koncentrálódik a schengeni külső határokon. Magyarország tekintetében ez a magyar-szerb és a magyar-ukrán államhatárt, míg az Európai Unió tekintetében ez a déli, elsősorban tengeri határokat jelenti. A Határőrség Rendőrségbe történt integrációjával nemcsak a határellenőrzési feladat, hanem a megmaradt személyi állomány is átkerült, azonban nem mindenki határrendészeti feladatra alkalmazva. Ez a létszám az átszervezések következtében folyamatosan csökken. Az évente bekövetkezett illegális migrációhoz kapcsolódó cselekmények és a határrendészeti szakterületen dolgozók létszámának összehasonlítása az alábbi táblázatban látható.

Évek:	2007	2008	2009
Illegális migráció (fő)	8948	7567	9888
Határrendészek (fő)	6200	5396	4933

1. táblázat.
Bekövetkezett illegális migrációhoz kapcsolódó cselekmények és a határrendészeti szakterületen dolgozók létszáma évente[2]

A csökkenő létszám és a növekvő jogsértő cselekmények okozta kihívásra kell keresnünk a választ. A megoldásra többféle lehetőség mutatkozik. Egyrészt adódik az együttműködés kérdésköre, mely minden szinten létezik. Egyrészt szervezeten belüli (jelen esetben a bevetési szakterülettel a legjellemzőbb), másrészt a szervezetek közti (például a vám- és pénzügyőrséggel), mely jogszabályban [2] is szabályozva van. Ezen kívül egyre több szomszédos országgal, azok határrendészeti szerveivel nemzetközi együttműködés is létezik. Az előbb ismertetett hármas együttműködés az integrált határbiztonsági rendszer – melynek ismertetése korábbi cikkben [3] olvasható - egyik alapelve.

Másik lehetőségként számolni lehet a feladatok átadásával vagy kiszervezésével. Az elsőre már 2010 augusztusában hallhattunk hangokat, mely szerint a Vám- és Pénzügyőrség átvenné

[2] Adatok forrása: ORFK Rendészeti Főigazgatóság Elemző-értékelő osztály Határrendészeti helyzetképek és dr. Demeter Tamás r. őrnagy: A határrendészeti szolgálati ág jelenlegi helyzete című előadása 2009. november

a Rendőrségtől a határrendészeti feladatokat. [4] A feladatok kiszervezése, azaz civil, profitorientált szervezeteknek rendészeti feladatok kiadása lehetne egy másik lehetőség. Amennyiben hazánkon túlra kitekintünk, láthatjuk, hogy az Egyesült Államokban erre már volt példa. A CIA megbízásából a Blackwater (ma Xe Company) cég az iraki háborúban egyes feladatokat ellátott. Határrendészetben pedig Szaúd-Arábiában bízták meg tavaly az EADS céget a határvédelmi rendszer kiépítésével [5], melyet elkészülte után, 2014-től valószínűleg működtetni is fog. Azonban a szabályozási alrendszert vizsgálva meg kell állapítanunk, hogy erre ma Magyarországon nincs lehetőség.

Az utolsó – talán legegyszerűbben járható út – az automatizálás, robotika. Az Európai Unió legújabb a bel- és igazságügyi együttműködésre vonatkozó stratégiai terve a Stockholmi Program, melynek határrendészeti vonatkozásaival már foglalkoztam. [6] Az Európai Tanács által elfogadott végleges szöveg alapján a folyamatban lévő fejlesztéseket, kísérleti projektek folytatását bátorítja.

2. MEGLÉVŐ ESZKÖZÖK

Az Európai Unió határőrizeti szerveinek (rendőrség, csendőrség, határőrség, vámőrség és parti őrség) a határokon átlépő illegális migráció megakadályozására sokféle technikai eszköz áll rendelkezésre. A különféle határszakaszokon, azaz a szárazföldi és a vízi határok ellenőrzésére természetes a különféle járőrautók megléte (terepjárók és csapatszállító járművek), valamint vízi járművek (motorcsónakok, mocsárjárók). Néhány helyen a természeti viszonyok miatt quadokat és hójárókat is rendszeresítettek. A technikai eszközök nagy része a vizuális figyelést segíti elő (távcső, stabil (telepített) és mobil hőkamerák, infratávcsövek, éjjellátó eszközök), de a zöldhatárra lépés- és mozgásérzékelő rendszert is lehet telepíteni. A határ mentén történő eseményeket levegőből is lehetőség van figyelni, néhány helyen helikoptert és repülőgépet is alkalmaznak. Az eszközök másik nagyobb csoportját a határátkelőhelyeken vetik be (röntgenkapu, szívdobbanás érzékelő, CO-mérő, sugárzásfigyelő, rendszámfelismerő, okmányleolvasó, arcképfelismerő rendszer) az illegális migráció és jogtalan áruk felderítése ellen. Az eszközök közé sorolom a meglévő és fejlesztés alatt álló számítógépes informatikai rendszereket (Schengeni Információs Rendszer, Vízuminformációs Rendszer, Határforgalom-ellenőrzési Regisztrációs Rendszer és az idegenrendészetben segítséget nyújtó ujjnyom-olvasó rendszer (AFIS)).

A technikai eszközök nemcsak rendkívül sokfélék, azok fejlettsége is eltérő. Értem ezalatt azt, hogy a később csatlakozott országok eszközei újabb generációkból származnak, ezáltal jobban elősegíthetik a munkát. Másik megközelítésben az országok eleve különféleképp gondolják fontosnak a határellenőrzést, ennek megfelelően költségvetésükben különböző mértékű támogatást biztosítanak a szerveknek, így a jobban támogatottak könnyebben vásárolnak új, modernebb eszközöket. A saját, honi költségvetésen túl az Európai Unió alapjain keresztül (például Külső Határok Alap) az illegális migrációval érintettség függvényében biztosít anyagi forrásokat a határellenőrzésre.

Nem lehet elhanyagolni a varsói székhelyű, Frontex elnevezésű határőr ügynökség szerepét sem, mely összehangolja és támogatja a tagállamoknak az EU közös határának igazgatásával (ellenőrzésével) kapcsolatos különböző intézkedéseit. Az ügynökség 2005-ben jött létre [7] és a feladatai közt szerepel egy nyilvántartás felfektetése és vezetése is, mely tartalmazza a tagállamok határőrizeti eszközeinek felsorolását (CREATE).

Amennyiben egy tagállamnak az illegális migráció hirtelen, nagy mértékű emelkedése miatt szüksége van korlátozott időtartamra szóló gyors, operatív segítségnyújtásra, akkor a Frontex ügynökségnél igényelheti a gyorsreagálású határvédelmi csapatok (RABIT) [8] bevetését, melyek saját technikai eszközeiket is hozzák. A gyorsreagálású határvédelmi

csapatok gyakorlatilag egy nemzetközi erőkből álló virtuális szervezet, amelynek tagjai a schengeni tagállamok speciálisan felkészített határőrei.

És éppen itt merül fel az egyik probléma. Előfordul, hogy a tagállamok ugyanazt a feladatot, célt szolgáló eszközt más-más gyártótól, így más képességekkel rendelik meg. A jövőben - úgy gondolom – az egységesítés felé kell haladni. Jó példa erre a terepjáró járőrgépkocsi, mely típusában (Nissan Pathfinder) több ország különböző hatóságainál is szolgálatot teljesít. A közös műveletek során lehet ez előnyös, amikor esetleg egy-egy eszközt hirtelen másnak kell használnia, vagy meghibásodásra számítva tartalék alkatrészt könnyebb raktározni.

3. JELENLEGI FEJLESZTÉSEK AZ AUTOMATIZÁLÁSBAN

Az automatizálás a határforgalomban jelentkezik elsősorban. A regisztrált utazói státusz elméletileg azon határátlépésre jelentkező, harmadik országokból származó állampolgárokra vonatkozhatna, akik kis kockázatot jelentenek az Európai Unió biztonsága szempontjából. Ez egy önkéntes alapon működő előzetes ellenőrzési eljárás, melynek pozitív elbírálása esetén az azt igénylő személynek a határátkelőhelyeken nem kellene várakoznia, hanem a külön sávon, a felállítandó automata kapukon keresztül léphetné át az EU határát. Az, hogy a regisztrált utazói státuszú személyek elektronikus kártyát kapnának, vagy az útlevelük azonosító rendszerén keresztül nyitnák a sorompót nem eldöntött. A rendszerek fejlesztéséhez szükség volt a biometrikus azonosítók rögzítése lehetőségének megalkotására. A mai modern útlevelek chipjei képesek ezeket az elsődleges azonosítókon (fénykép, személyes adatok, útlevél-adatok) túl akár az ujjnyomatot vagy az írisz-kódot tartalmazni. A regisztrált utazókhoz kapcsolódó pilot projectek folyamatban vannak. Többek között a frankfurti repülőtéren lehetősége van az Európai Gazdasági Térség országai állampolgárainak külső határon történő átlépéskor automata határellenőrzésen átesniük. Ehhez regisztráltatniuk kell magukat, melyhez a személyes adatokon kívül útlevelük bemutatása kell, valamint írisz-képet készítenek szemükről. A regisztrált utasok útlevelük gépbe helyezése és írisz-kódjuk ellenőrzése után átléphetik a határt.

Határátlépéseit rögzítő rendszer létrehozása szintén egy stratégia cél. A létező, országonként különböző rendszereket kellene összehangolni vagy egy közös újat létrehozni. A határregisztrációs rendszer célja az, hogy a tagállamok illetékes hatóságai az ellenőrzött harmadik országbeli személy tartózkodásának jogszerűségét meg tudják állapítani. Egyrészt, hogy a külföldi az arra kijelölt helyen és időben lépte át a külső határt, másrészt az engedélyezett tartózkodási idejét nem lépte túl. A rendszerbe történő ellenőrzés lehetősége nemcsak a külső határokon szolgálatot teljesítő hivatalnokoknak, hanem a terület mélységében végrehajtott idegenrendészeti ellenőrzést véghezvivő tisztviselőknek engedélyezett lesz. A rendszer figyelmeztetést küldene a nemzeti hatóságok számára, amikor lejár egy egyén engedélyezett tartózkodási ideje az EU-ban, és nem rögzítették kilépési adatait. 2011-ben várható a jogalkotás [9] a határregisztrációs rendszerre vonatkozóan, mely megalapozná annak fejlesztési lehetőségeit.

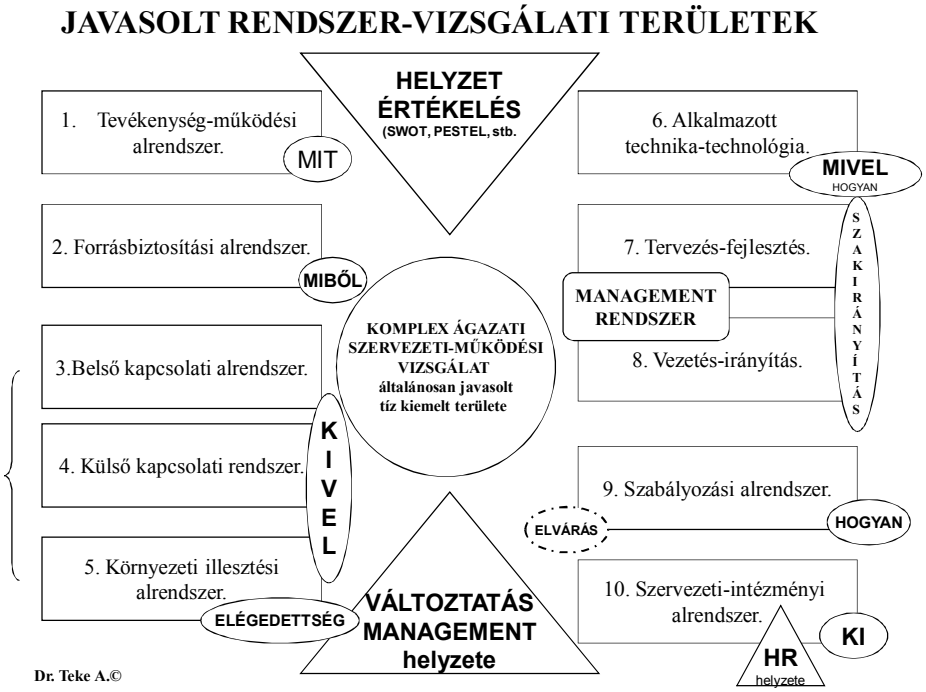
Az elektronikus utazási engedély rendszer pedig nem más, mint a harmadik országok nem vízumköteles állampolgárai előzetes vizsgálata abban a tekintetben, hogy teljesíti-e a belépési feltételeket. Az ezzel élni kívánó az utazás megkezdése előtt elektronikus kérelmet nyújtana be, amely tartalmazná a személyazonosító, valamint az útlevélben szereplő és az utazásra vonatkozó adatokat, mely alapján eldöntenék azt, hogy a személy beléptethető-e az Európai Unióba. Ezáltal a valódi határátlépéskor az elektronikus utazási engedély birtokában a személy gyorsabban ellenőrizhető. Ez a lehetőség csak a nem vízumköteles államok polgárainak lenne elérhető. A rendszer véleményem szerint nagymértékben hasonlítana az Amerikai Egyesült Államok Utazási Engedélyt Jóváhagyó Elektronikus Rendszerére

(ESTA).[10] Ezt azon országok állampolgárainak biztosítják, melyek részt vesznek az ún. Vízummentességi Programban (Visa Waiver Program), azaz nincs szükségük vízumra, ha üzleti vagy magáncélból utaznak az USA-ba 90 napnál nem hosszabb időtartamra.

4. LEHETŐSÉGEK A ROBOTJÁRMŰVEK ALKALMAZÁSÁRA

A választási lehetőségek közül ez a - jelenleg még - legjáratlanabb út, azonban talán az automatizálás mellett a leglogikusabb.

Természetesen mielőtt belevágnánk a robotok rendszerbe állítására előtte sok teendőt el kell végeznünk. Először egy komplett rendszervizsgálatot szükséges végrehajtani.



1. ábra. Rendszer-vizsgálati területek [3]

Magyarországon az integrált határbiztonsági rendszer működtetésének fő felelőse a rendőrség, ennek megfelelően azt, míg az Európai Unió tekintetében az egyes országok határellenőrzési feladatot ellátó szerveit, továbbá a Frontex ügynökséget is vizsgálni kellene. A cikk keretei ezt nem teszik lehetővé, ezért csak néhány dolgot emelek ki a magyar helyzettel kapcsolatban.

Abból indultam ki, hogy a határellenőrzési feladatot kik hajtják végre és megállapítottam, hogy a rendelkezésre álló létszám egyre kevesebb. Ez a szervezeti-intézményi alrendszerben található. Ehhez szorosan kapcsolódik az együttműködés kérdése, azaz kiket lehet bevonni a feladat végrehajtásába a rendőrségen belül (belső kapcsolati alrendszer), a más szervezetek közül (külső kapcsolati alrendszer), és tevékenységünk hogyan illeszkedik a környezetébe. Itt vizsgálni kellene azt is, hogy a környezet mennyire elégedett a tevékenységünkkel.

A jelenlegi működéshez a költségvetés biztosítja az alapvető forrásokat, melyen kívül a már említett EU-s forrás is rendelkezésre áll. Ez utóbbi az eszközök beszerzéséhez segítséget nyújt, azonban a működtetéshez szükséges forrásokra csak a honi lehetőségekkel lehetne számolni, azonban ezek nincsenek minden esetben biztosítva. A fejlesztések ötletszerűek, rendszertelenek. Az alkalmazott technikai eszközök és technológiák megkönnyítik a feladat-

[3] Az ábrát Dr. Teke András készítette és bocsátotta rendelkezésemre 2010. június 24-én Pécsett tartott előadásából. Az írott előadásanyag elérhető: Pécsi Határőr Tudományos Közlemények XI., Pécs, 2010.

végrehajtást és létszámot spórolnak, erről egy cikkben olvashatunk. [11] A szabályozási alrendszert vizsgálva azonban meg kell állapítanunk, hogy a robotjárművek ilyen célú alkalmazására nincs szabályozás. A rendőrség rendelkezik egy TeleMax típusú robotjárművel, mely a fő rendeltetésének, azaz a robbanóanyag felkutatásának és megsemmisítésének a nemzetközi repülőtereken, az utasbiztonság növelése érdekében került beszerzésre, nem kis részben Külső Határok Alap támogatásával, azonban másra történő alkalmazása jelenleg nincs. Pedig a rajta lévő többfunkciós karon a kamera elhelyezésével szabad szemmel nem vagy nehezen elérhető helyek átvizsgálása történhetne. Az integrált határbiztonsági rendszer működésének rendszerszemléletű elemzése bővebben egy másik folyóiratban megtörtént. [12]

Összefoglalva kiindulási alapom megismételve, véleményem szerint úgy, ahogy az a hőkamerák rendszerbeállításakor történt (ld. Papp et al. 2010. [11]) a robotjárművek alkalmazása is csökkentheti az emberi erőforrás szükségességét.

Amennyiben ez alapján úgy döntöttünk, hogy szükséges, vagy munkánk elősegíti a robotjárművek alkalmazása, meg kell határoznunk, mire van szükségünk? Magyarország tekintetében kizárható a vízi vagy víz alatti ember nélküli jármű, mivel az illegális migráció fő irányai és a határvizeink tulajdonságai szükségtelenné teszik, ugyanakkor uniós szinten a leginkább migrációval sújtott déli tengereken alkalmazhatóak lennének. A légi járművek közül milyen kategóriásat válasszunk, vagy gondolkozzunk helikopterben? A szárazföldi jármű kerekes vagy lánctalpas legyen, számít-e a teherbírása? Egyáltalán mennyi eszközt vásároljunk? Azaz fontos a pontos típuskövetelmények meghatározása. Ezek mellett nem szabad elfelejteni az előbbi rendszervizsgálati elveknek megfelelően mire és hol alkalmazzuk, valamint azt hogyan alkalmazzuk? Nem utolsó sorban figyelembe kell venni a határőrizeti alapelveket. [13] Véleményem szerint az ilyen eszközök rendszerbe állításával a meglepetésszerűség növelhető, míg az aktivitás inkább az alkalmazó kezelőszemélyzet munkájától, illetve a vezetők hozzáállásától függ. El kell gondolkodni továbbá azon is, hogy egy-egy kifejezetten nagy értékű eszköz beszerzése történjen-e EU-s szinten, mondjuk úgy, hogy a Frontex gépparkjába kerülne esetleg többnemzeti együttműködéssel?

A robotjárművek alkalmazásával a határellenőrzés minőségét lehet növelni, a személyi állomány létszámát lehet csökkenteni, a feleslegessé váló erőket átcsoportosítani, vagy a hiányzó létszámot pótolni. Csekély hátránya e körben az, hogy a robotok irányításhoz szükséges létszám egy időre kiesik, a kiképzés miatt. Ugyanakkor a robotoknak – hasonlóan más technikai eszközökhöz - van egy olyan jó tulajdonsága, hogy megbízhatóak és egyenletes színvonalon tudják teljesítményüket leadni. Továbbá kevésbé érzékenyek a körülmények változására (pl. időjárás) és olyan szituációkban is alkalmazhatóak, mely az emberek számára kényelmetlen (pl. vasúti szerelvények átkutatása). A jelenleg határrendészeti feladatokat ellátó rendőrségen az állomány életkora rendkívül alacsony: 32,2 év [14], mely előnyös abból a szempontból, hogy a technikai eszközök alkalmazását, így a robotjárművek irányítását könnyen elsajátítják.

Hátrányok között szerepel még néhány dolog. Problémát okozhat, ha a robotjármű üzemideje végéhez közelít, és akkor történik felderítés. Ez a kézi hőkamerával is előforduló jelenség, sajnos ilyen esetekben csak a tapasztalat és a szerencse segít az illegális migránsok elfogásában. Van néhány szárazföldi robot mely szenzorokkal rendelkezik, hogy ne ütközzön bele más tárgyakba, azonban fel kell készülni a kisebb-nagyobb balesetekre. A határ menti alkalmazásnak pedig van egy olyan hendikepje is, hogy a járművek véletlenül átléphetik az államhatárt, határrend-sértést okozva. Ez elsősorban a légi járművekkel történhet meg, hiszen a szárazföldön a határvonal viszonylag tisztán látható. Erre megoldás lehet bi- vagy multilaterális egyezmények kötése a szomszédos országokkal, esetleg úgy, ahogy az a határ-menti közös járőrözéssel történt. Ez ma már nemcsak az EU tagállami szomszédokkal, de külső határként funkcionáló horvát határszakaszon is így van [15], lényege, hogy a

szomszédos országok rendvédelmi szervei közös járőrszolgálatot működtetnek, a járőrpáros 1-1 tagja a két országból áll és az államhatár vonalától 10-10 km távolságban (határterületen) látja el feladatát. Ennek megfelelően a megkötendő egyezménynek alapja az lehetne, hogy elősegítse a két ország határellenőrzését. Esetleg olyan megoldás is lehetne, hogy a szomszéd ország járőre is figyelhetné a jármű kamerája által közvetített képet és irányíthatná a saját járőreit az eredményes elfogás érdekében.

A légi robotjárművek alkalmazásával kapcsolatban több megoldásra váró probléma is felmerül. Egyrészt az, hogy az államhatár menti korlátozott légtér (10 km mélységű sáv) használatára állandó engedélyt kellene kérni a Nemzeti Közlekedési Hatóság Légiközlekedési Igazgatóságától. [16] Másrészt a légtér azon részeiben, ahol UAV-ok többsége működhetnének az ilyen célú alkalmazás jelenleg nem engedélyezett. [17] Megoldás lehetne egy olyan jogszabály alkotása, mely a Magyar Honvédség és a Rendőrség, valamint a Katasztrófavédelem számára külön engedélyezné az UAV-ok alkalmazását.

Előnyök	Hátrányok
- személyi állomány kiváltása	- állomány kiképzése
- megbízhatóság	- robotrepülők alkalmazásának magassága (Wührl)
- könnyű irányítóhatság a fiataloknak	- balesetek
- kényelmetlen szituációkban is alkalmazható	- üzemidő végén történő felderítés
	- szabotázs

2. táblázat. A robotjárművek alkalmazásának előnyei és hátrányai

5. ALKALMAZHATÓ ROBOTOK

E fejezetben azt kívánom bemutatni, hogy a jelenleg különböző helyeken, különböző céllal alkalmazott robotok közül elsősorban melyek a könnyen elérhetők, melyekről vannak tapasztalatok és van-e alternatíva.

5.1. Vízi járművek

Úgy gondolom, hogy Magyarország tekintetében határellenőrzési feladatok ellátására felesleges ember nélküli vízi járműveket beszerezni. Azonban Európai Uniós szinten lehet rá gondolni, hiszen a legnagyobb fenyegetés a Frontex adatai alapján az elmúlt években a legtöbb illegális migráns tengeren érkezett a területre. A bevándorlók egy része Afrikából, míg egy másik része Afganisztánból és a Közel-Keletről érkezett. A második csoport ugyanakkor Törökországon keresztül utazva, a szárazföldi helyett az Égei-tengeri vízi utakat választja. Ez alapján állítom, hogy Görögország, Málta, Olaszország, Franciaország, Spanyolország eredményesen tudná alkalmazni az USV-ket.

Határőrizeti, pontosabban határvédelmi célból - kutatásom alapján - egyetlen hajótípust használnak a világon, ez pedig az izraeli Rafael Advanced Defense Systems Protector nevű hajója (ma már a BAE és a Lockhead Martin közreműködésével gyártják), mely Izraelen kívül Szingapúrban szolgál. A határvédelmi jelleg dominál, ennek megfelelően fegyverzettel (7,62 mm-es gépfegyver) is rendelkezik, a megfigyeléshez és felderítéshez szükséges optikai rendszereken (éjjel infravörös) kívül. Ez utóbbit fejlesztve lehetne kihasználni a jármű képességeit. A 9 méter hosszúságú felfújható, merevtestű járművet dízelmotorja akár 90 km/órás sebességgel tudja hajtani, azaz képes lenne a felderített, embercsempészek által hajó felderítésén kívül megfigyelni, követni azt.

5.2. Szárazföldi járművek

Hazánkban – nem utolsó sorban a jogi környezet miatt – a szárazföldi ember nélküli járműveket tudnánk a legkönnyebben adoptálni. Magyarországon jelenleg a Magyar Honvédségen kívül a Rendőrség is rendelkezik (TeleMax típusú) robottal, melyet 2009-ben szerzett be. [18] Az Egyesült Államokból származó TeleMax robotnak vizsgálatom szempontjából nagy előnye, hogy több kamerával rendelkezik és karjával akár néhány cm-es résbe is be tud nyúlni, képet közvetíteni, valamint 2,6 méteres magasságra felnyúlva.

A másik – ma még kevés helyen alkalmazott – ténylegesen őrködési funkcióra kitalált kisméretű szárazföldi robot OFRO, mely német gyártmányú és a 2006. évben rendezett labdarúgó világbajnokságon is alkalmazták. [19]



1. kép. OFRO robotjármű[4]

Az éjjellátó hőkamerával is felszerelt robotnak legnagyobb előnye a hosszú üzemidő és a relatív olcsósága.

OFRO		**TeleMax**
1,2 m	Magasság	max: 2,6 m
0,5 m	Szélesség	0,4 m
7,2 km/h	Sebesség	3,5(gumikerék)/4,7 km/h
50 kg	Tömeg	80 kg
12 óra	Üzemidő	2 óra
1 db, 360°-ban forgatható + hő	Kamera	5 db (hőkamera is)
kb. 50 000 €	Ára	kb. 300000 $ (Rendőrség: 97 millió Ft teherautóval)
GSM/WLAN	Irányítás	opt.kábel/rádió

3. táblázat. Az OFRO és a TeleMax robot tulajdonságainak összehasonlítása[5]

[4] Kép forrása: Robowach Technologies http://www.uvs-info.com/pdf/ugvspec/Robowatch_OFRO_en.pdf Letöltés ideje: 2010. november 10.

[5] Adatok forrása: 1. OFRO Robowach Technologies http://www.uvs-info.com/pdf/ugvspec/Robowatch_OFRO_en.pdf Letöltés ideje: 2010. november 10.
2. TeleMax: Kuchera Engineering http://www.kuchera.com/ke/products/robotics/telemax.pdf Letöltés ideje: 2010. november 5.

A szárazföldi robotok közt találhatunk nagyobb méretűt is. E körben az izraeli Elbit gyártmányát, az AvantGuard-ot emelem ki, hiszen ez a gyártó országában határőrizeti – védelmi funkciót lát el, azaz hasonló szakterületen kerül alkalmazása.



2. kép. AvantGuard UGV[6]

A gyalogsági lövedék és útszéli bomba ellen páncélozott és emiatt roppant súlyos, 1,3 tonnás gépjármű fegyverzettel is rendelkezik, egy 7,62 mm-es géppuskával. Amire a határellenőrzés során alkalmazhatnánk (azaz felderítés, figyelés, követés) ezen tulajdonságokra nincs szükségünk, annál inkább a kamerarendszerére és sebességére, hiszen a kisméretű robotoknál gyorsabban tud közlekedni. A 3800 cm3-es dízel motorja 100 LE teljesítményű, mellyel a lánctalpas változata 20 km/h sebességre képes. [20] A gumikerekes változatról nincs adat, ennél valamivel fürgébb mozgásra képes. A kétfős kezelőszemélyzet 10-12 járművet tud egyszerre irányítani, azonban ez csak abban az esetben igaz, ha determinált útvonalon járőröznek.

A szárazföldi távirányítású robotok alkalmazási lehetőségei sokrétűek. A rendelkezésre álló TeleMax a Ferihegyi Repülőtéren szolgál, azonban csak a rendeltetésének megfelelően alkalmazva, azaz a terrorcselekmények megakadályozása érdekében bombakutatás, megsemmisítés.

A kisméretű robotokat elsősorban határforgalmi kirendeltségeken, határátkelőhelyeken lehet kihasználni. Ennek fő oka az alacsony üzemidő és hatótáv. A TeleMax robotot közúti határátkelőhelyen gépjárművek alvázának, autóbuszok csomagterének, egyes teherjárművek rakterének átvizsgálására lehetne alkalmazni. Különösen az alváz átvizsgálásánál célszerű, hiszen olyan kényelmetlenségtől, mint az alábújástól kímélheti meg az embereket, hiszen az úgynevezett kutatótükörrel sajnos nem lehet minden üregbe belátni. OFRO alkalmas lehet a várakozó sorok közti járőrözésre, előzetes felderítésre, megakadályozandó az ellenőrzés nélküli határátlépéseket, azonban alkalmazásánál figyelembe kell venni azt is, hogy a gépjárművezetőket erre előzetesen fel kell készíteni, nehogy baleset legyen a vége. Vasúti határátkelőhelyeken a járőrözésre OFRO szintén alkalmas, azonban a szerelvények átvizsgálásához (forgózsámolyok környéke) a TeleMax használhatóbb. Repülőtereken a kifutópályák őrzésére szintén alkalmas a német robot, talán ezzel lehet a legtöbb személyi állományt kiváltani. A repülőgépek esetleges átvizsgálására viszont a TeleMax kiváló lehetőséget nyújt. Erre jó példa az Egyesült Államokban lévő Atlanta városának nemzetközi

[6] Kép forrása: Sarah Gingichashvili: Future Robotic Squadrons to Patrol Military Bases, The future of things June 25, 2008 - http://thefutureofthings.com/news/1211/future-robotic-squadrons-to-patrol-military-bases.html Letöltés ideje: 2010. november 5.

repülőtere, ahol ilyen módon is alkalmazzák, a cél azonban más: a repülőgépen elhelyezett robbanóanyagok feltalálása. [21]

Zöldhatár ellenőrzéshez egyértelműen a legjobb döntés lenne a bemutatottak közül az AvantGuard, de kiegészítő elemként (letelepült hőkamerás autó mellé) OFRO is helyes elhatározásnak bizonyulhat.

5.3. Légi járművek

A Magyar Honvédség rendelkezik Skylark I-LE típusú repülőgépekből álló rendszerekkel. Ennek kipróbálásával könnyebben el lehetne dönteni, hogy alkalmas-e határellenőrzési feladatok ellátására. Gondolatommal, mely szerint e rendszereket alkalmazni lehetne, nem vagyok egyedül, hiszen egy cikk részeként már hivatkoztak e lehetőségre (ld. [11]). Legnagyobb előnyének azt látom, hogy bárhonnan felbocsátható s könnyen irányítható.

A pilóta nélküli repülőgépek közül néhány kategóriával feljebbről [22] választottam a másik lehetőséget. Közepes magasságon repülő UAV-E osztályba tartozik a MQ-9 Repear (Predator B), melyet a General Atomics Aeronautical Systems gyárt. (Néhány forrás szerint ez már UCAV, hiszen hasznos teherbírása is van, képes bombákat szállítani és eljuttatni a célba.)



3. kép. A „határőr” MQ-9 Repear (Predator B)[7]

Azonban a Predator B-nek létezik egy civil alkalmazása is. Az Egyesült Államok Vám- és Határvédelmi Hivatala (ld. 3.sz. kép) szolgálatba állított több, egyenként 3 repülőgépből álló rendszert az illegális migráció és az árucsempészet megakadályozása érdekében. [23] A Repear alkalmazásában az létszik előnyösnek, hogy viszonylag nagy az üzem ideje és hatótávolsága.

MQ-9 Repear		**Skylark I-LE**
Repülőtéren	Fel- és leszállás	Helyben
11/20 m	Hossz/fesztáv	1,45/2,9 m
2223/4760 kg	Üres/felsz.tömeg	5,3/6,5 kg
480/300 km/h	Max/utazó seb	90/45 km/h
14-28 óra	Üzemidő	2,5-3 óra
7,5/15 km	Üzemi/max mag.	0,3/1,5 km
900 LE	Motor, teljesítmény	Elektr. kb. 5,2 LE
kb. 500 km	Hatósugár	kb. 15 km
10 millió USD	Ára	?

4. táblázat. Az MQ-9 és a Skylark robotrepülőgépek tulajdonságainak összehasonlítása[8]

[7] A kép forrása: http://www.abacuspub.com/blog/?cat=8 Letöltés ideje: 2010. november 12.

A pilóta nélküli légi járművek tekintetében sokan csak a repülőgépekre gondolnak. Azonban ma már helikoptert is készítenek távirányításos változatban. Ebből a kategóriából – repülőgépek esetleges alternatívájaként az egyesült államokbeli MQ-8B Fire Scoutot választottam. A közel egytonnás, három méter magas, 8,4 méteres rotorral rendelkező helikopter 200 kilométert is meg tud tenni óránként és nyolc órán keresztül bevethető 200 km-es hatósugárban. A legnagyobb előnye lehet az, hogy szinte bárhol leszállhat, ahonnan képes is visszaemelkedni.



4. kép. MQ-8B Fire Scout[9]

A pilóta nélküli légi járművek elsősorban a határőrizetben alkalmazhatóak felderítési és megfigyelési feladattal. Alkalmazásuk azért lenne igazán előnyös, mert van egy olyan felderítési képességük, mely a földi hőkameráknak nincs. Ez pedig a fedett részekre (kukorica-táblák, ritkább erdők, erdei utak) történő rálátás, azaz ezekkel az eszközökkel észlelni lehet a földön történő mozgást. A kisméretű robotrepülőt akár egy közönséges határőr járőr is vihetné magával, saját figyelési feladatának megkönnyítésére. A Predator B-t véleményem szerint Magyarországon nem lehetne kihasználni, ugyanakkor a nagy, viszonylag egyenes vonalú határszakasszal, illetve a tengeri határokkal rendelkező országok igen.

Két másik lehetőséget is látok a beszerzésre. Az egyik az, hogy a Frontex ügynökség vásárolna ilyen eszközt és minden országból kiképeznének néhány embert az eszköz alkalmazására, és a gépeket közös műveletekben alkalmaznák. A másik az lehetne, hogy néhány szomszédos Európai Unió tagállam összefogna és vásárolna, majd azt közösen üzemeltetnék. Ennek azonban jóval kisebb a valószínűsége, mint az ügynökségi vásárlásnak.
A határforgalom ellenőrzésben úgy lehetne felhasználni a gépeket, hogy a feltorlódott gépkocsi sorok felülről figyelhetnék. Így kiszűrhetők lennének a torlódást kihasználni akaró, engedély nélkül átlépni szándékozó, gyalogosan érkező személyek.
Az általam bemutatott három eszköz közül a határellenőrzési feladatra leginkább a helikoptert tartom alkalmasnak. Itt említem meg, hogy korábban a határőrizeti feladatokra is bevetették (MI-8T és MI-2 típusú) helikoptereket, melyekkel a nyugati határ őrizetét erősítették.

---

[8] Adatok forrása: 1. MQ-9: The official website of the US Air Force http://www.af.mil/information/factsheets/factsheet.asp?id=6405 Letöltés ideje: 2010. november 11.
2. Skylark I-LE: Defense Update http://defense-update.com/products/s/skylark1-uav.htm#more Letöltés ideje: 2010. november 12.

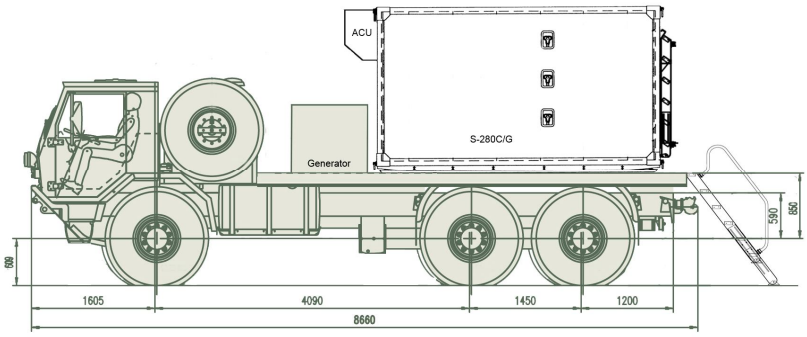
[9] Kép forrása: www.defence-tech.blogspot.com Letöltés ideje: 2010. november 12.

6. TALOS

Talos a görög mitológia alakja, aki a Kréta szigetét naponta háromszor körbejárta, hogy megvédje a szigetet a hódítóktól. Egyes források úgy nevesítik feladatát, hogy megvédje Európát azon személyektől, akik azt szeretnék, hogy elrabolják.

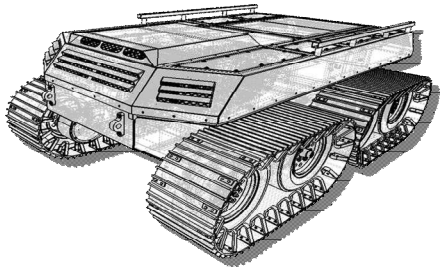
Talán nem véletlenül választották a szárazföldi határok őrizetére fejlesztendő rendszer alkotói ezt a nevet: Transportable Autonomous patrol for Land bOrder Surveillance system, azaz hordozható automata járőr a szárazföldi határőrizeti rendszerhez. A rendszer fejlesztése 2008-ban kezdődött, a projekt 20 millió eurós költségvetéséhez az Európai Unió 13 millióval járult hozzá. 10 ország (Belgium, Észtország, Finnország, Franciaország, Görögország, Izrael, Lengyelország, Románia, Spanyolország és Törökország) 14 szervezetének (műszaki egyetem, vállalkozások, kutató intézetek) konzorciuma alakítja és csiszolja a rendszert. Mint azt a projekt honlapjáról [24] megtudhatjuk, TALOS célja az, hogy segítsen felfedni, nyomon követni és elfogni azon személyeket, akik megpróbálják átlépni a szárazföldi határokat illegálisan a határátkelőhelyek között.

A rendszer elemei lennének: szállítójármű, felderítő (megfigyelő) jármű, elfogó jármű, irányító központ.



5. kép. A TALOS rendszer szállítójárműve[10]

A felsoroltakon kívül a rendszerhez tartozik egy adó-vevő torony, mely az információ áramoltatását végzi, valamint szükséges járőrök alkalmazása is, akik az elfogó jármű által feltartóztatott személyeket előállítanák, illetve a rendszer kiegészíthető légi robotjárművekkel is. Maga a TALOS megalkotása a három jármű kifejlesztésére szolgál.



6. kép. A TALOS rendszer alapjárműve, melyből kialakításra kerül a robotjármű[11]

[10] A kép forrása: Second workshop, „TALOS: Design of the subsystems” előadás (ppt) http://talos-border.eu/index.php?option=com_content&view=article&id=55&Itemid=63 Letöltés ideje: 2010. november 16.
[11] A kép forrása: Uo.

A két távirányított jármű egyenként négy lánctalppal rendelkezik, melyek 42 cm szélesek és 92 cm hosszúak és képessé teszik helyben megfordulásra. A járművek szélessége 2 méter, hosszúsága 3 méter, magassága 1,2 méter lenne, tömegük 1600 kg.

Motorként 3800 cm3-es, 100 lóerős dízel erőforrás szolgálna – az adatok alapján valószínűsítem, hogy ez azonos az AvantGuardhoz felhasznált hajtóművel – mely a járműveket mintegy 35 km/órás sebességre tudná gyorsítani.

Terepjáró képessége kiváló: 30 százalékos be- és kilépővel rendelkezik, és képes 35 százalékos emelkedőn közlekedni. Félméteres akadályt képes leküzdeni, hasonló mélységű hóban, valamint 40 cm-es vízben tud járni. Ezen kívül 1200 kg hasznos terhet tud szállítani.

A projekt az idei évi munkaülésen elhangzottak alapján a megadott ütemterv szerint zajlik. [25] Az alrendszerek közül mindegyiknek a magas szintű tervezését végrehajtották, a parancs és vezérlő-alrendszer kialakítása folyamatban. Két és háromdimenziós térképeket fejlesztik. Navigáció, érzékelés-, parancs- vezérlőmodulok, és kommunikációs rendszer fejlesztése elkezdődött.

Amennyiben a projekt a továbbiakban is a megfelelő ütemben halad 2012-ben lesz kész a prototípusa, melynek tesztelése után elkezdődhet a rendszerbe állítása.

ÖSSZEFOGLALÁS

Az Európai Unióba évente több mint 150 ezer ember kíván illegálisan bejutni. Ebből Magyarországon tavalyi évben majdnem 10 ezer ember követett el illegális migrációhoz köthető cselekményt. A határellenőrzést ellátók létszáma viszont folyamatosan csökken. Az ezekből fakadó kihívásnak valahogy elejét kell venni. A megoldási utakat ismertettem, cikkemben - a konferencia témájához kapcsolódóan – bővebben a robotjárművek alkalmazhatóságával foglalkoztam.

Megállapítottam, hogy a robotjárművek alkalmazásával a határellenőrzés minőségét lehet növelni, a személyi állomány létszámát lehet csökkenteni, a feleslegessé váló erőket átcsoportosítani, vagy a hiányzó létszámot pótolni. Ugyanakkor megállapítottam, hogy a robotjárművek határellenőrzési célú alkalmazására nincs szabályozás, sőt a pilóta nélküli légi járművek alkalmazása különösen nehézkes. Ennek kiküszöbölésére jogszabályalkotást javasoltam, mely szerint a Magyar Honvédség, a rendőrség és a katasztrófavédelem pilóta nélküli légi járművei a korlátozott légteret külön engedély nélkül használhassák.

Az egyes robotok alkalmazása, rendszerbe állítása előtt fontos a pontos típuskövetelmények meghatározása, a mire és hol alkalmazzuk, valamint azt hogyan alkalmazzuk kérdéseinek figyelembe vételével. Ezen kívül nem szabad megfeledkezni a határőrizeti alapelvekről sem az alkalmazás során.

A jelenleg már létező robotok közül egy vízi, három szárazföldi és három légi járművet mutattam be legfontosabb adataikkal. Az előbb javasolt vizsgálati kérdésekre adott válaszoknak megfelelően lehet közülük kiválasztani, amire szükségünk van. A Protector nevű vízi járművet Dél-Európában tudnák hasznosítani. A szárazföldi robotok közül véleményem szerint mindegyik alkalmazható lenne hazánkban, míg a pilóta nélküli légi járművekből a helikopter kiválasztása lenne a legjobb döntés.

Az utolsó fejezetben pedig bemutattam a jelenleg fejlesztés alatt álló szárazföldi határok őrizetét elősegítő, hordozható, távirányított járművekből álló rendszert. A projekt jelenlegi állása alapján várhatóan - a terveknek megfelelően – 2012-ben elkészül a prototípus.

Azt gondolom, hogy a Talos rendszer fejlesztése is bizonyítja elgondolásom, hogy a határellenőrzésben a robotok alkalmazása lehetséges, sőt egyes helyeken szükségessé is válhat.

A robotok alkalmazása elősegíti a felderítést, folyamatos megfigyelést tesz lehetővé és növeli a meglepetésszerűséget, aktivitást.

Felhasznált irodalom

[1] Magyar Köztársaság Nemzeti Biztonsági Stratégiájáról szóló 2073/2004. (III. 31.) Kormányhatározat http://www.mfa.gov.hu/NR/rdonlyres/0AA54AD7-0954-4770-A092-F4C5A05CB54A/0/bizt_pol_hu.pdf

[2] Az illegális migráció és az ahhoz kapcsolódó más jogellenes cselekmények elleni hatósági fellépés hatékonyságának növeléséről, illetve összehangolásáról szóló 8/2010. (II. 19.) IRM–SZMM–PM–KHEM együttes utasítás Hivatalos Értesítő, XIII. ÉVFOLYAM 13. szám Budapest, 2010. február 19.

[3] Lipics László: A schengeni információs rendszer szerepe az integrált határbiztonsági rendszerben, Hadmérnök 2010/3 Interneten elérhető: http://www.hadmernok.hu/2010_3_lipics.pdf

[4] Fekete Gy. Attila: Vámhatárőrség? - A VPOP-hez kerülhet a határellenőrzés, Népszabadság, 2010. augusztus 13.

[5] Jan Hildebrand: Wie EADS vom Mauerbau in Saudi-Arabien profitiert Welt Online, 05.10.2010 Forrás: http://www.welt.de/wirtschaft/article10080765/Wie-EADS-vom-Mauerbau-in-Saudi-Arabien-profitiert.html Letöltés ideje: 2010. október 7.

[6] Lipics László: A Stockholmi Program hatása az integrált határbiztonsági rendszerre, Hadtudomány 2010. évi elektronikus száma

Elérhető: http://mhtt.eu/hadtudomany/2010_e_22.pdf

[7] Az Európai Unió Tagállamai Külső Határain Való Operatív Együttműködési Igazgatásért Felelős Európai Ügynökség felállításáról szóló 2007/2004/EK Tanácsi rendelet (2004. október 26.) Az Európai Unió Hivatalos Lapja L 349., 2004.11.25., 1—11. o.

[8] A gyorsreagálású határvédelmi csapatok felállítására szolgáló eljárás bevezetéséről, valamint a 2007/2004/EK tanácsi rendeletnek ezen eljárás tekintetében történő módosításáról és a kiküldött határőrök feladatai és hatáskörei szabályozásáról szóló Európai Parlament és a Tanács 863/2007/EK rendelet (2007. július 11.) Az Európai Unió Hivatalos Lapja L 199., 2007.7.31., 30—39. o.

[9] Öt éven belül létrehoznák a biztonság egységes térségét Forrás: http://www.bruxinfo.hu/index.php?lap=dokument/dokument&dok_id=26865 Letöltés ideje: 2010. június 20.

[10] Elektronikus utazási engedély Forrás: https://esta.cbp.dhs.gov/esta/esta.html?_flowExecutionKey=_c921B2F35-A893-6E2D-517E-94E168365F6B_k15ECCE31-155C-E921-80BB-AECD06D56E8F Letöltés ideje: 2010. július 4.

[11] Papp Csaba - Solymosi Krisztina - Horváth László - Hullám István: A biztonság fokozása a Magyar Köztársaság schengeni külső határszakaszán, Hadmérnök 2010/2 391-403.o. Elérhető interneten is: http://hadmernok.hu/2010_2_papp_etal.pdf

[12] Dr. Teke András (PhD): A „helyettesíthetőség” kérdése a határbiztonság-szolgáltatás vonatkozásában Határrendészeti Tanulmányok (A Rendőrség Tudományos, Technológiai és Innovációs Tanács Határrendészeti Munkacsoport tudományos, szakmai kiadványa) 2010/1. Szám, Budapest, 2010. 40-96.o.

[13] Dr.Sándor Vilmos: A határrendészetet ellátó szervezetek össztevékenységében ható törvényszerűségek és általános elvek (Ideiglenes jegyzet) Zrínyi Miklós Katonai Akadémia, Budapest, 1995.

[14] Túlságosan fiatal a rendőri állomány 2008.10.27. Forrás: http://www.securifocus.com/portal.php?pagename=hir_obs_reszlet&&i=22062 Letöltés ideje: 2010. november 8.

[15] A Magyar Köztársaság Kormánya és a Horvát Köztársaság Kormánya között a határokat átlépő bűnözés elleni harcban történő együttműködésről szóló Megállapodás kihirdetéséről szóló 2009. évi LXVI. törvény Magyar Közlöny 2009. évi 92. szám, Budapest, 2009. július 3. 23655-23669.o.

[16] A magyar légtér igénybevételéről szóló 4/1998. (I. 16.) Kormányrendelet 4. § (1) Forrás: http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=99800004.KOR Letöltés ideje: 2010. november 12. és

A Nemzeti Közlekedési hatóságról szóló 263/2006 (XII.20) Kormányrendelet 5. § (1) Magyar Közlöny, 158. szám Budapest, 2006. december 20. 12514-12518 o.

[17] Dr. Wührl Tibor: Kisméretű pilóta nélküli repülők légtérhasználati kérdései Forrás: http://www.uav.hu/publikaciok/whurl_tibor/Wuhrl_Tibor.pdf Letöltés ideje: 2010. november 10.

[18] Az Országos Rendőr Főkapitányság és a Combat Kereskedelmi Kft. között kötött Szállítási szerződés 1 db Robot manipulátor… beszerzésére http://www.police.hu/data/cms650280/Szerzodes_combat.pdf Letöltés ideje: 2010. november 11.

[19] Alexander Visser: Kollege fürs Grobe, Der Tagesspiel (Berlin) 05.01.2006 Forrás: http://www.tagesspiegel.de/berlin/kollege-fuers-grobe/672600.html Letöltés ideje: 2010. november 11.

[20] AvantGuard Unmanned Ground Combat Vehicle, Israel

Forrás: http://www.army-technology.com/projects/avantguardunmannedgr/ Letöltés ideje: 2010. november 5.

[21] Kelly Yamanouchi: Airport police use growing fleet of robots to ferret out bombs, The Atlanta Journal-Constitution, August 2, 2010 Forrás: http://www.ajc.com/business/airport-police-use-growing-583454.html Letöltés ideje: 2010. november 5.

[22] Unmanned Aerial Vehicles (UAVs) Forrás: http://www.globalsecurity.org/intell/systems/uav-intro.htm Letöltés ideje: 2010. november 5.

[23] Az Egyesült Államok Vám- és Határvédelmi Hivatalának pilóta nélküli légi járművekre vonatkozó programja Forrás: http://nemo.cbp.gov/opa/videos/2010/uas_texas.wmv Letöltés ideje: 2010. november 5.

[24] The Project, 01 September 2009 Forrás:

http://talos-border.eu/index.php?option=com_content&view=article&id=52&Itemid=60 Letöltés ideje: 2010. november 15.

[25] Second workshop, „TALOS: General information” előadás (ppt) Forrás:

http://talos-border.eu/index.php?option=com_content&view=article&id=55&Itemid=63 Letöltés ideje: 2010. november 16.

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Molnár András
Molnar.Andras@nik.uni-obuda.hu

Stojcsics Dániel
Stojcsics.Daniel@nik.uni-obuda.hu

KISMÉRETŰ ROBOTREPÜLŐGÉPEK FEDÉLZETI ROBOTRENDSZEREINEK ROBOSZTUS KIALAKÍTÁSA

Absztrakt

A pilóta nélküli légi járművek fedélzeti robotrendszereinek kialakítása során rendkívüli jelentőséggel bír e rendszerek robosztus kialakítása. A robotrepülőgépnek folyamatosan alkalmazkodnia kell az állandóan változó közeghez, amelyben repül, oly módon, hogy a repülés biztonságát eközben meg kell őriznie. Különböző parciális rendszerhibák esetén megengedhetetlen, hogy a repülőgép irányíthatatlanná váljon. Ennek érdekében a fedélzeti robotrendszereket úgy kell kialakítani, hogy azok a különböző szoftveres vagy hardveres (pl. szenzor-, program- vagy beavatkozó szerv hiba) meghibásodások esetén is képesek legyenek a feladatuk végrehajtására. A robotrepülőgép üzemeltetéséhez elengedhetetlen a különböző részegségek többszörözése. A biztonságos manuális vezérléshez szükség van kettő darab rádióvevőre, melyek közti átkapcsolást a fedélzeten meg kell oldani. A fejlesztési, tesztelési lépésekhez szükséges a robot illetve az ember vezette kormányfelületek homogén átkapcsolására, lehetőleg diszkrét áramköri elemekkel, kizárva a szoftveres hibákat. Célszerű egy olyan interfész panelt kialakítani, melyhez csatlakoznak a különböző beavatkozó szervek és a vezérlést biztosító rádióvevők illetve a robotvezérlő. A panelt ellátva több robotvezérlő interfésszel megoldható a robotrendszer robosztusságának kérdése. A vezérlők egyenként komplett rendszert alkotnak (teljes szenzorblokk, tápellátás, I/O rendszer és központi processzor), csupán egy darab is képes a repülőgép vezérlésére, viszont több darab együttes alkalmazásával hiba esetén a meghibásodott vezérlőtől át lehet adni az irányítást a hibátlan robot vezérlőnek.

The robust design of the onboard systems for small size unmanned aerial vehicles (UAVs) is quite important. The UAV has to adapt continuously to the changing environment and the local airflows while the safety of the flight must be kept. It is impermissible that the UAV became uncontrollable due to different partial system failures. For this purpose the onboard systems must be designed to resist any

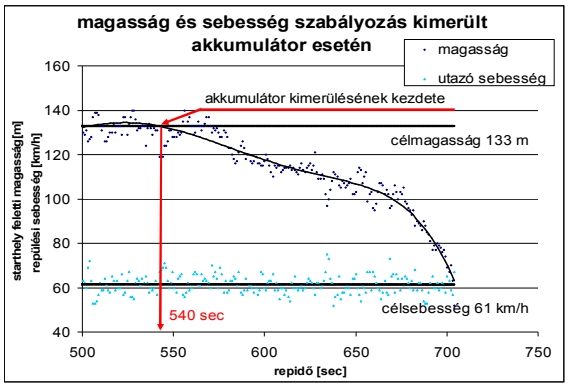
software and hardware failures (such as sensor, actuator or program error) and should be able to continue the mission task.
The multiplication of the different subsystems is necessary for the safety. Two different radio receivers with a diversity controller are needed for manual flight. A switching module is needed to change the control signal of the control surfaces between manual and autonomous mode in the development and testing phase of the UAV. An interface board should be designed which connects the different control surfaces, the radio receivers and the autopilot. The robust design of the system can be solved if this board has multiple autopilot interfaces. Each autopilot forms a complete system (full sensor array, power supply, I/O system and core processor). A single unit can control a UAV but using many units connected to the interface board, when a unit fails the UAV is still controllable.

Kulcsszavak: *robot, UAV, vezérlés ~ robot, UAV, control*

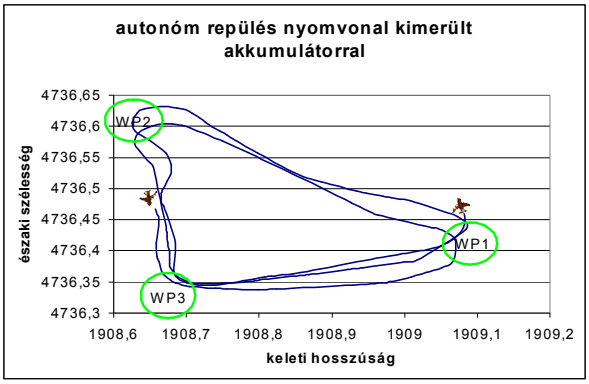
ELŐZMÉNYEK

A robotegységgel számos kísérlet elvégzésére került sor. A mérések során vizsgálat tárgyát képezték a magasság- és a sebességszabályzó rendszerek viselkedései mellett az útvonalszabályzó rendszerek is, mivel azok hatása közvetve szintén kihat a sebességre, illetve a magasságra.

Az 1. és a 2. ábrák egy olyan kísérleti repülés adatait ábrázolják, amely során az



1. ábra, sebességtartás csökkenő motorteljesítmény esetén

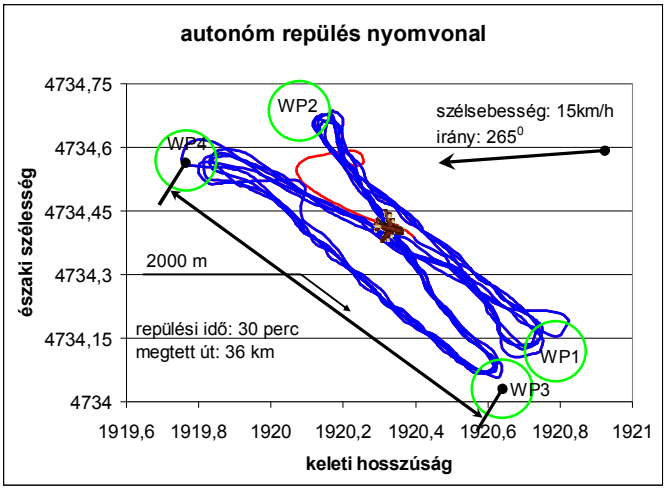


2. ábra, repülési nyomvonal csökkenő motorteljesítmény esetén

elektromos hajtású repülőgép akkumulátorai kimerültek. Mivel az alkalmazott Lithium-polimer akkumulátorok kisütési karakterisztikájának végső kisülési szakasza rövid, a vonóerőcsökkenés viszonylag hirtelen következik be, és azt követően a hajtómű hamar leáll. Mint az 1. ábrán látható a teljesítménycsökkenéstől a hajtóműleállásáig mindössze 160 másodperc telt el. Ezt követően a repülőgép motor nélküli siklással ért földet, amit a diagramok már nem ábrázolnak. A 2. ábrán a csökkenő hajtóműteljesítménnyel repülő UAV nyomvonala látható. Megfigyelhető, hogy a szabályzók mind a repülés irányát, mind annak sebességét kielégítően tartják, miközben az akkumulátorok kimerülése okán a magasságtartás már nem valósul meg [1].

A 3. ábra egy 30 perces autonóm repülés nyomvonalát szemlélteti. A teszt célja az volt, hogy alkalmas lehet-e a rendszer egy hosszú távú, autonóm repülésre. A repülés azonos magasságban négy fordulópont által meghatározott „nyolcas” nyomvonal mentén történt. A

pályakialakítás során szempont volt, hogy legyenek jobb, illetve bal fordulói, valamint rendelkezzen oldal-, hát- és szembeszeles szakaszokkal. Mivel a kísérlet az egyensúlyi állapot tartós fennállását vizsgálta, a fel- és a leszállás távirányított módon történt.

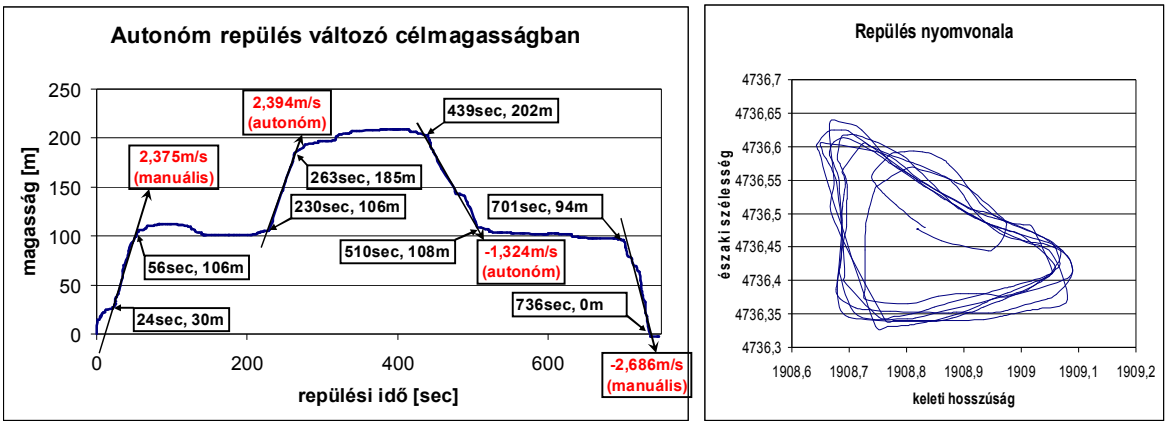


3. ábra, 30 perces autonóm repülés nyomvonala

Vizsgálatok történtek a magasságváltoztatás (emelkedés süllyedés) képességének optimalizálása céljából. A repülések során a kísérleti repülő úgy lett beprogramozva, hogy három fordulópont által meghatározott nyomvonalon repüljön. Három kört követően (ennyi idő alatt beálltnak volt tekinthető az állandósult állapot) a repülőgép utasítást kapott 150 méter emelkedésre. Ezt követően további három kört repült, majd újabb utasítás hatására visszasüllyedt a teszt kiindulási magasságára, ahol ismételten három kört tett meg. Az egyik ilyen repülés magassági profilját a 4. ábra szemlélteti.

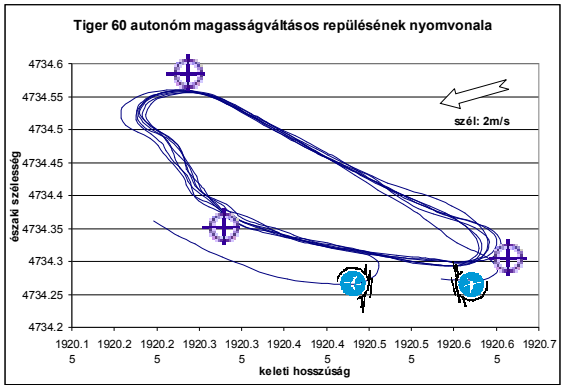
Az ábra tartalmazza az autonóm repülést megelőző és az azt követő manuális (távirányított) repülési szakaszokat is, így mód nyílik a robot és a pilóta repülési profiljának összehasonlítására is. Az ábrán látható emelkedési és merülési értékek jól szemléltetik, hogy a robot gyakorlatilag a pilóta által még biztonságosnak ítélt emelkedési és süllyedési manővereket hajtotta végre. Fontos megjegyezni, hogy az autonóm repülés során előálló függőleges sebességek nem lettek előre beprogramozva. Azok az előre meghatározott vízszintes repülési sebességből, valamint a repülőgép dinamikai tulajdonságaiból (le nem programozott!) adódtak.

Az iránytartás a kísérletek során nem mutatkozott kielégítőnek.



4. ábra, változó magasságú autonóm repülés magasságprofilja és nyomvonala.

Szimulációkkal kimutattuk, hogy a hibát az irányszabályozó függvény egyik faktora okozta. A további kísérletek célja az volt, hogy megvizsgáljuk a módosított útvonalszabályzó függvény hatását. Az első kísérleteket egy Tiger 60-as modellrepülőgépbe épített robotegységgel végeztük. A Tiger 60 egy 12 cm3–es belsőégésű motorral ellátott, 1,8 m szárnyfesztávolságú, 4 kg felszálló tömegű modellrepülőgép.

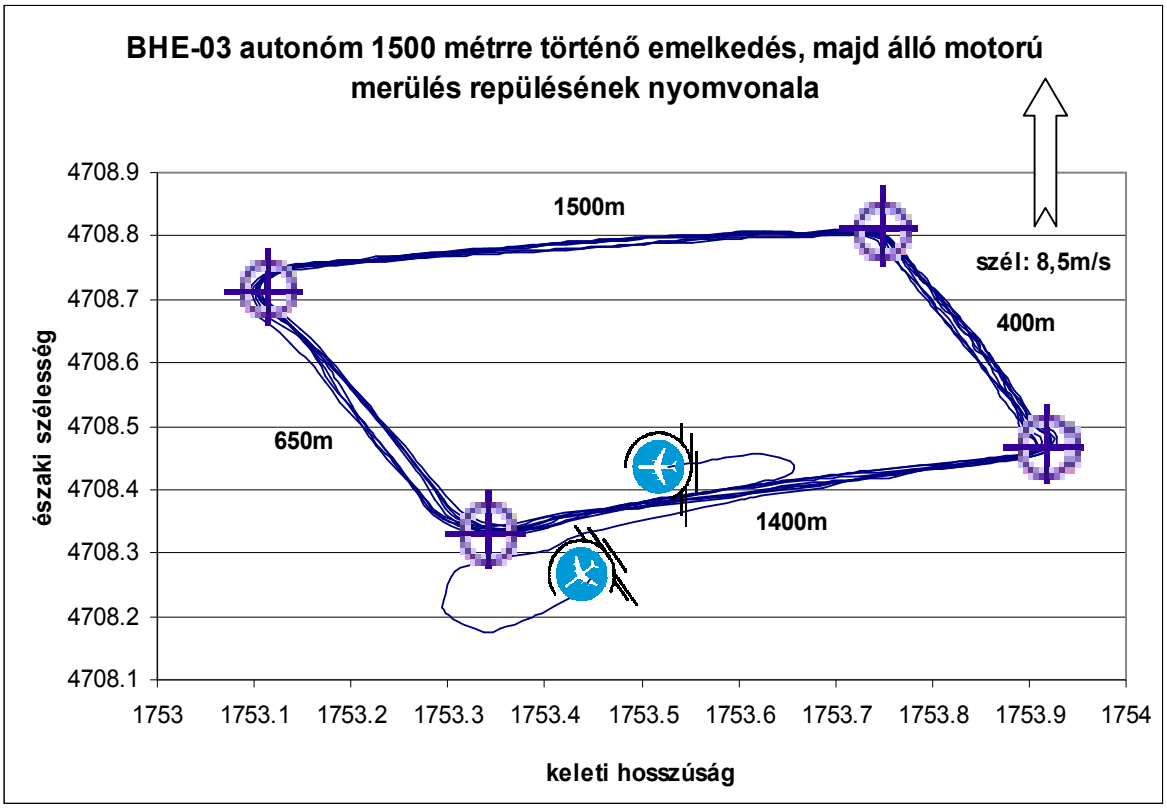


5. ábra, Három fordulópontos autonóm repülés nyomvonala

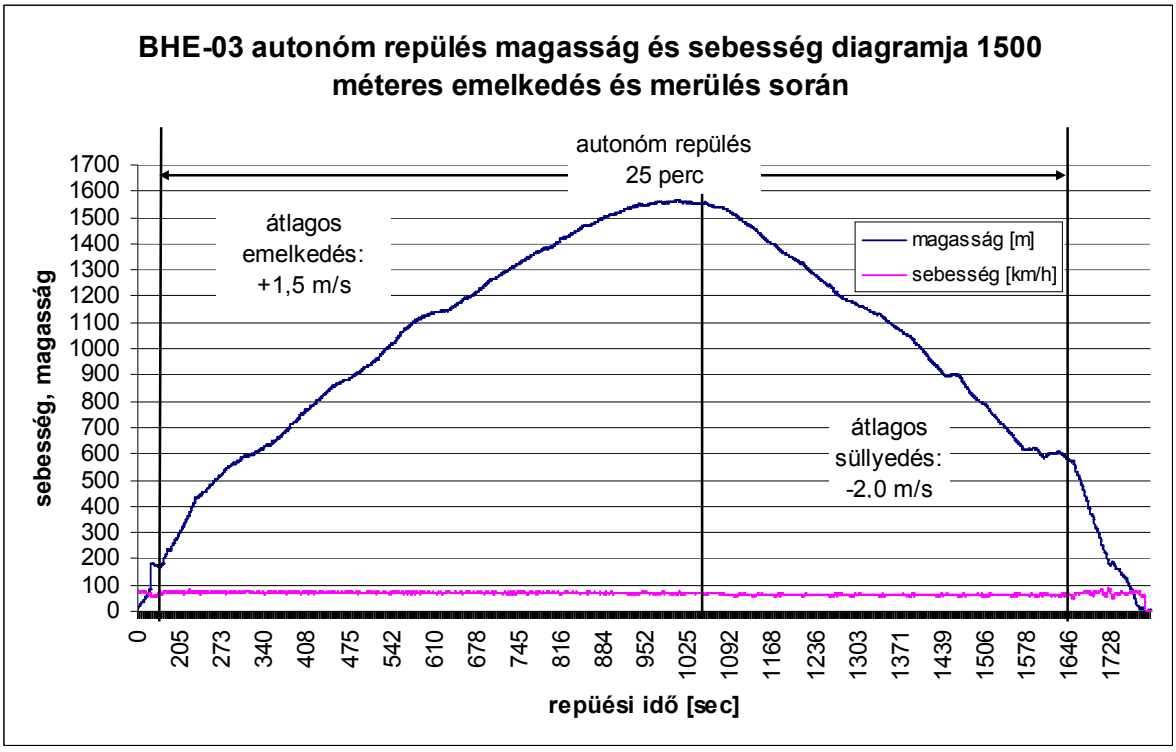
Az 5. ábrán jól látható, hogy a repülés nyomvonala az eddigi nyomvonalakhoz képest simább, az egyes körök közötti eltérés mértéke jelentős mértékben csökkent. A kísérlet során a gép repülési sebessége 80 km/h, magassága 140 méter volt starthely felett.

A pontosabb mérések érdekében szükségessé váltak hosszabb egyenes szakaszokból felépített repülések. Ezeket a kísérleteket már csak zárt légterekben lehetett végrehajtani, mivel a repülés teljes időtartama alatt már nem volt biztosítható a közvetlen manuális vezetés. A 6. ábra egy nagy magasságú (1500 méter startpont felett) repülés nyomvonalát szemlélteti. A repülőgép egy négy fordulóponttal kijelölt zárt pályán repült. A kísérlet célja az volt, hogy megvizsgálhassuk a tartós emelkedés során a repülőgép viselkedését, valamint mérési adatokat gyűjthessünk a hajtómű nélküli repülésről. A repülőgép akkumulátorának kimerüléséig a gép folyamatosan emelkedett, majd a vonóerő megszűnését követően siklórepüléssel folytatta a kijelölt pályán a repülést. A nyomvonal elemzése során a motoros és a siklórepülés között eltérés nem mutatkozott, ami igazolta a szabályzórendszer elvileg megjósolt viselkedését.

A 7. ábra a 6. ábra nyomvonalának repülése során rögzített magassági adatokat szemlélteti. A diagramon jól látható az akkumulátor kimerülésének hatása és az abból következő siklórepülésbe történő átmenet.



6. ábra, Négy fordulópontos autonóm repülés nyomvonala



7. ábra, négy fordulópontos autonóm repülés magasságprofilja

A kísérletek eredményei alapján lehetőség nyílott nagyobb távolságú és nagyobb magasságú repülésekre. Ugyancsak zárt légtérben történtek sikeres repülések 20 km-es távolsági, illetve 2000 méteres magassági céllal. Annak érdekében, hogy a repülőgép nagy biztonsággal legyen üzemeltethető szükségessé vált a fedélzeti rendszer megbízhatóságának fokozása. Tekintettel arra, hogy a robotrendszer nem igényli az állandó kapcsolattartást a földi követő állomással, a megbízhatóság növelését elsősorban a fedélzeti, autonóm rendszer módosításával kívánjuk elérni.

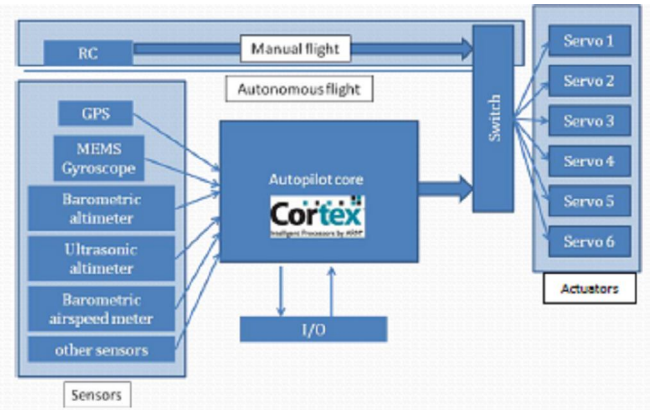
REDUNDÁNS KÉZI IRÁNYÍTÁS

A robotrepülőgép fejtesztelése során a tesztrepülések alkalmával kiemelt szerepet kap a manuális irányítás. Annak érdekében, hogy a fedélzeti szenzorokat, telemetriát be lehessen kalibrálni, szükséges több kézi repülés végrehajtása. Csak azután lehet a különböző szabályzóköröket behangolni, miután a rendelkezésre állnak megfelelő pontosságú és felbontású szenzoros értékek. A manuális irányítás biztonságát szem előtt tartva szükséges kettő darab, különböző frekvenciájú RC vevő elhelyezése a repülőgépen, oly módon, hogy a vevőantennájuk egymással 90 fokos szöget zárjanak be. A két vevőt egy vevő közösítővel kell összekötni, amelyik a vevők failsafe (35MHz analóg rendszerek esetén PCM modulációval vagy bármely 2,4GHz digitális rendszer) csatornáját figyelve mindig azt a modult teszi aktívvá, amelyiknek jobb a vétele.

Manuális repüléssel kellő mérési adat gyűjthető a szenzorok ellenőrzéséhez és kalibrációjához. Amint ez megtörtént, következhet a szabályzókörök független hangolása.

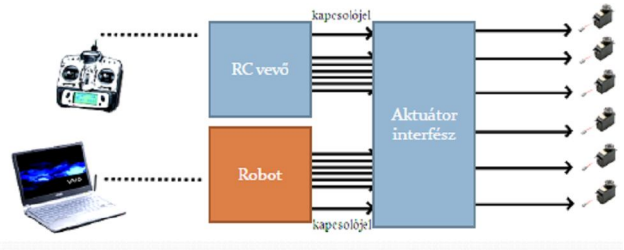
AUTONÓM – MANUÁLIS MÓD ÁTKAPCSOLÓ

A szabályzóköröket célszerű először egymástól függetlenül beállítani, majd utána együtt tesztelni azokat. Szükséges egy olyan kapcsoló interfész kialakítása, amellyel meg lehet oldani repülés közben a manuális és autonóm mód közötti átváltást (8. ábra). A teljes átkapcsolás a korai tesztrepülések során különösen veszélyes, mivel az egyes szabályzó körök még nincsenek finom hangolva. Ezen szabályzókörök független tesztelését esetén csak úgy lehet megoldani, hogy a kábelezéskor ki kell iktatni a manuálisan vezérelt kormányfelületek esetén a kapcsolót.



8. ábra, Autonóm – manuális mód kapcsoló sémája

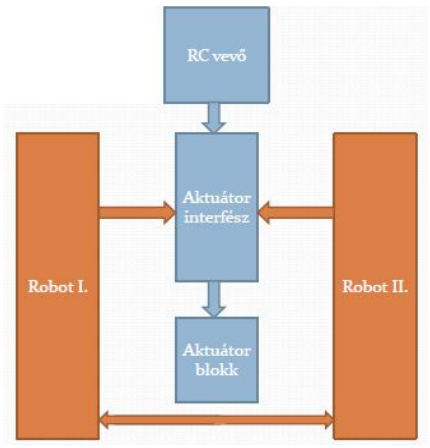
Mivel a szabályzókörök független teszteléskor a robotrepülőgép kormányfelületeit részben az robotpilóta, részben pedig az emberi berepülőpilóta irányítja (pl. magasságtartás esetén a robot vezérli a motor csatornát, a többit pedig az emberi pilóta), célszerű, hogy a csatornák jelének forrását tetszőlegesen lehessen, akár repülés közben állítani. Ehhez egy autonóm/manuális kapcsoló interfészre van szükség.



9. ábra, Kapcsoló interfész

Az interfésznek három bemenete van. Az egyik a vevő közösítő kimenete, a második pedig a robotpanelről érkező vezérlőjelek. A harmadik bemenete egy kiválasztó - kapcsoló logika, amely meghatározza, hogy az aktuális kormányfelületre melyik bementi vezérlő jel kerüljön (9. ábra). Ezt a földi állomásról küldött parancsokkal lehet konfigurálni a robotpanelen keresztül [2].

Az interfész kimenetére a repülőgép kormányfelületeit vezérlő aktuátorok vannak csatlakozatva. A kapcsolót lehetőség szerint diszkrét áramköri elemekből célszerű összeállítani processzoros feldolgozás helyett, megelőzve a szoftveres hiba miatti komoly károkat.



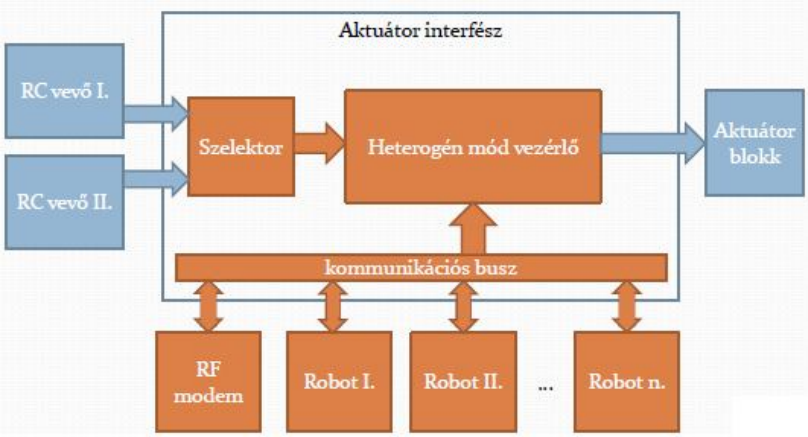
10. ábra, Redundáns robotvezérlő

REDUNDÁNS ROBOTVEZÉRLŐ

Természetesen az autonóm repüléskor is biztosítani kell a redundáns működést [3]. Nem elég csupán kettő ekvivalens robotpilóta alkalmazása (pl. több vezérlő processzor), hanem a teljes fedélzeti rendszert duplikálni kell (10. ábra). Több független robotpanelre van szükség, amelyik mindegyikének komplett rendszert kell alkotnia, különálló táprendszerrel és szenzorblokkal (GPS,

barometrikus szenzorok stb.) kell rendelkeznie. Ehhez az interfész panelt ki kell egészíteni oly módon, hogy több ekvivalens robotpanelt lehessen csatlakoztatni hozzá. Az egyik panel a „mester”, a másik a „szolga”. A robotpanelek egymással alacsony szinten kommunikálnak, és hiba esetén a „szolga” el tudja venni az irányítást a „mestertől”.

Kettő panel alkalmazása esetén ez nem lehet megfelelő biztonsággal eldönteni, hogy melyik robot a hibás. Az egyszerű áramköri elemekből felépített interfész panel további bővítése viszont az alkatrészsűrűséget és bonyolultságot túlzott mértékben növeli, ezért azt le kell cserélni egy FPGA áramkörre (11. ábra).

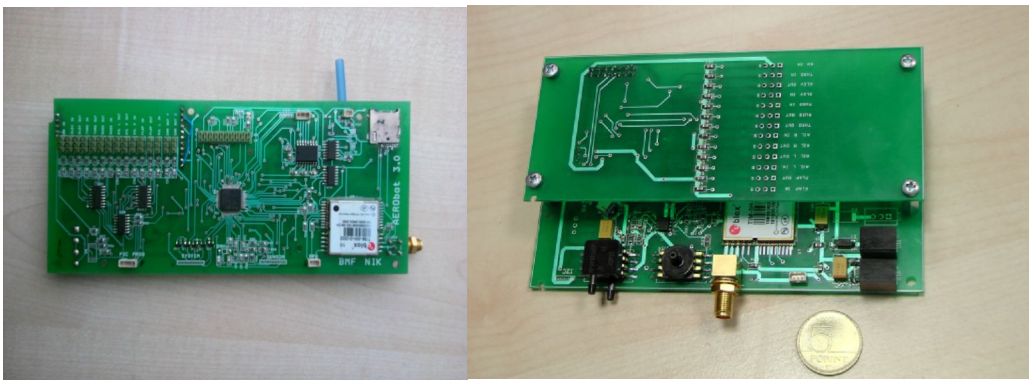


11. ábra, Fejlett redundáns robotvezérlő

Ehhez a központi interfészhez csatlakozik a két RC vevőegység analóg (9 PWM csatorna) módon, valamint egy közös buszrendszerre a több (min. 3) független robotpanel és az RF modem. A buszrendszeren történik a robotok közti valamint a robot és föld közötti kommunikáció, és az érvényre jutó robot jelének kiválasztása. Az azonos adatot mérő robotok figyelmen kívül tudják hagyni a hibásat.

ÖSSZEGZÉS

A robotrepülő vezérlő több lépcsős fejlesztése és különböző kialakítású repülőgépeken végrehajtott tesztelése során megszerzett tapasztalatok alapján a rendszer újratervezése megtörtént. (12. ábra). Az újratervezés során kiemelt figyelmet fordítottunk a moduláris felépítésre és a repülésbiztonság növelésére a fedélzeti rendszerek redundanciájának



12. ábra, Régi és új robotvezérlő

növelésén keresztül. A moduláris felépítésnek köszönhetően az új rendszer képességi bizonyos határok között skálázhatóak. Ennek köszönhetően a rendszer autonóm repülések megvalósítása tekintetében alkalmas az egyszerű, alacsony költségű robotrepülőtől a bonyolult, nagyméretű és drága robotrepülőgépekig.

Hivatkozások

[1] Molnár, A. (2010). Robotrepülőgépek repülésstabilizálásának és navigációjának új megközelítése, XVII. Repüléstudományi Napok Konferencia kiadványa, Budapest, 2010. november 11-12.

[2] D. Stojcsics: "Heterogenous control of small size unmanned aerial vehicles", Proceedings of 10th International Symposium of Hungarian Researchers on Computational Intelligence and Informatics, ISBN: 978-963-7154-96-6, Budapest, Hungary, 2009, pp. 745-752.

[3] Makkay, Imre (2010) Design the Advanced Avionics for "FanWing" UAV, Repüléstudományi Közlemények különszám 2010 április 16.

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Muha Lajos
muha.lajos@zmne.hu

Fleiner Rita
fleiner.rita@nik.uni-obuda.hu

ADATBÁZISOK BIZTONSÁGÁNAK KEZELÉSE A KÖZIGAZGATÁSBAN

Absztrakt

A publikáció az adatbázis biztonság szabályozásával foglalkozik. A szerzők bemutatják az adatbázis-biztonság szabályozását a magyar közigazgatásban és az Egyesült Államok haderejében. A publikáció az említett szabályozók alapján javaslatot tesz a magyar szabályozás megvalósítására.

The publication studies the regulation of database security. Authors describes regulation of database security in the hungarian government and the US Armed Forces. The authors proposed a base of database security regulation in the hungarian government.

***Kulcsszavak**: adatbázis-biztonság, adatbázis-biztonság szabályozása, Adatbázis-biztonsági útmutató, közigazgatás, Egyesült Államok Védelmi Minisztériuma ~ database security, database security regulation, ,, Database Security Guide, government, Department of Defense*

BEVEZETÉS

Az elektronikus közszolgáltatásoknak, illetve a közigazgatási szerv informatikával támogatott folyamatainak szükséges és alapvető feltétele az adatok, nyilvántartások elektronikus tárolása, mely leggyakrabban adatbázisok segítségével valósul meg. Az áttekinthetően és hatékonyan működő központi adatbázisok megléte az elektronikus közigazgatás alapvető eleme. Az adatbázisok biztonságának megsértése (működésképtelenné tétele, meghamisítása, a tárolt adatok jogtalan megismerése) az adott informatikai rendszer és az általa nyújtott szolgáltatás biztonságát fenyegeti. Ebből következően lényeges kérdés az adatbázis-biztonság megvalósítása és ennek szabályozása, támogatása.

Technológiai szempontból biztonságosan kifejlesztett (például egy magas Common Criteria szerinti minősítést elnyert) adatbázis-kezelő rendszer biztonságos működésének számos technikai és eljárásbeli feltétele van. Az adatbázis környezet telepítésekor, konfigurációjakor és működtetésekor számtalan szükséges beállítást és eljárást kell figyelembe venni, követni ahhoz, hogy az adatbázis-kezelő rendszer védve legyen már ismert támadási módszerektől. A biztonságos beállítások mellett olyan eljárásokkal is szükségszerű körültekintően eljárni, mint például a mentési, helyreállítási, audit és jogosultság beállítás folyamatok. Továbbá az adatbázis-kezelő rendszer az informatikai rendszer egyéb összetevőivel (operációs rendszer, hálózat, adatbázist elérő alkalmazások) is szoros kapcsolatban áll, ezek biztonsága nem kezelhető elkülönítve, mivel az informatikai rendszer egy komponensének nem biztonságos működése kihathat a vele együttműködő összetevőre.

A hazai közigazgatási informatika védelmére készült 223/2009. (X. 14.) Korm. rendelet, valamint a KIB 25. és 28. számú ajánlásai az informatikai védelem átfogó, komplex szabályozását nyújtják, de még emellett is szükséges az informatika egyes részterületeinek védelmét részterületi védelmi rendszabályokkal, útmutatókkal, ajánlásokkal elősegíteni, különös tekintettel a működés kritikus területeken. A közigazgatási informatika védelemben fontos részterület az elektronikus adatok tárolását és kezelését megvalósító adatbázis-kezelő rendszerek, illetve az azokban tárolt információk védelme, melynek jövőbeni szabályozásának kérdéseit, lehetőségeit vizsgálják a szerzők jelen cikkükben.

Az Egyesült Államok Védelmi Minisztériuma (Department of Defense, DoD) az informatika különböző részterületeinek védelméhez részletes szabályozó dokumentumokat dolgozott ki. Jelen publikációban feltárjuk a hazai informatika biztonság jelenlegi szabályozási rendszerét, megvizsgáljuk a DoD által kidolgozott szabályozókat, különös tekintettel az Adatbázis-biztonság Technikai Megvalósítási Útmutatóra, majd elemezzük a hazai adaptáció lehetőségeit, korlátait, illetve javaslatot fogalmazunk meg a magyar adatbázis-biztonsági szabályozás rendszerére.

A KÖZIGAZGATÁSI INFORMATIKAI BIZTONSÁG SZABÁLYOZÁSA ADATBÁZISOK SZEMSZÖGÉBŐL

Az elektronikus közigazgatás biztonságát elsősorban a 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról [1] határozza meg, támogatva a Közigazgatási Informatikai Bizottság 25. és 28. számú ajánlásával. A kormányrendelet hatálya kiterjed az elektronikus közszolgáltatásokra, azok működtetőire, üzemeltetőire, az elektronikus közszolgáltatások nyújtásában részt vevő szervezetekre és személyekre, valamint az elektronikus közszolgáltatások igénybe vevőire.

A 223/2009. kormányrendelet a közszolgáltatást végző informatikai rendszerek személyi, szervezeti és műszaki követelményeit tartalmazza. A kormányrendelet főbb előírások a következők:

- Az elektronikus közszolgáltatásoknak meg kell valósítaniuk a bizalmasság, sértetlenség, törvényes adatkezelés és kockázatarányos védelem elveit.

- Az elektronikus közigazgatási rendszerek biztonsági felügyeletét a kormány informatikai biztonsági felügyelője látja el.

- A magyar kritikus információs infrastruktúra védelméért a Nemzeti Hálózatbiztonsági Központ a felelős.

- Az érintett szervezeteknek információbiztonsági irányítási rendszert kell létrehozniuk. Ezen belül meg kell valósítani a minőségbiztosítást és szabályzati rendszert kell létrehozni.

- A kritikus rendszereket naplózni, menteni és archiválni kell.

- Meg kell oldani az ügyféltámogatást.

- Speciális esetekben az üzemeltetés kiszervezhető, de ilyenkor is be kell tartani a biztonsági előírásokat.

- Vírusvédelmet kell megvalósítani.

- Adattovábbítás során kriptográfiai megoldásokat kell használni az üzenetek titkosítására.

- A hozzáférés-védelmet mind logikai, mind fizikai szinten gondosan meg kell tervezni és valósítani.

- Az üzemeltetés biztonságai elveinek kialakítása során a legjobb gyakorlatokra kell alapozni.

- Az elektronikus közszolgáltatásokat biztonsági auditnak kell alávetni az erre felhatalmazott szervezet által.

Ezek mellett még a központi rendszer biztonsági szabályozása is megtalálható a jogszabályban.

A Közigazgatási Informatikai Bizottság (a továbbiakban: KIB) 2008-ban adta ki a 25. számú, majd rövidesen a 28. számú ajánlását. A KIB 25. számú ajánlása a Magyar Informatikai Biztonsági Ajánlások (MIBA) címet viseli. Ez tulajdonképpen egy ajánlássorozat, amelynek fő célja, hogy nemzetközi szabványokhoz és ajánlásokhoz igazodva biztonságos informatikai rendszerek kialakítását és fenntartását segítse elő. A MIBA három fő részből áll:

- A **Magyar Informatikai Biztonsági Keretrendszer (MIBIK)** [2] szervezeti szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBIK a biztonságos informatikai rendszerek irányításáért, menedzseléséért felelős vezetőknek, illetve a szervezet egészére vonatkozó követelmények teljesülését értékelő szakembereknek szól. A MIBIK az ISO/IEC 27001:2005, ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványokon, valamint az irányadó EU és NATO szabályozáson alapul. A MIBIK része az Informatikai Biztonsági Irányítási Rendszer (IBIR) [3]**,** amely a szervezet informatikai biztonságának tervezésére, üzemeltetésére, ellenőrzésére és javítására vonatkozik. A MIBIK további részei az Informatikai Biztonság Irányítási Követelmények (IBIK) [4], amely az informatikai biztonság kezelésének hatékonyabbá tételéhez nyújt segítséget, lehetőséget teremtve a követelmények és feladatok szakmailag egységes kezelésére, illetve az Informatikai Biztonsági Irányítás Vizsgálata (IBIV) [5], amely az informatikai biztonság ellenőrzéséhez ad módszertani segítséget.

• A **Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS)** [6] technológiai szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBÉTS célközönsége az informatikai rendszer kialakításáért, fejlesztéséért felelős vezetők, valamint az informatikai termékek és rendszerek biztonsági értékelését és tanúsítását végző szakemberek köre. A MIBÉTS az ISO/IEC 15408:2005 és ISO/IEC 18045:2005 nemzetközi szabványokon, illetve a nemzetközi legjobb gyakorlatokon és nemzeti sémákon alapul. Keretet biztosít arra, hogy az informatikai termékek és rendszerek tekintetében a biztonsági funkciók teljessége és hatásossága értékelésre kerüljön. Értékelési módszertana alkalmas az operációs rendszerek, hardverek (pl. hálózati eszközök, tűzfalak, behatolás észlelők, intelligens kártyák), szoftveralkalmazások (pl. különböző programnyelveken megírt kritikus alkalmazások) speciális biztonsági szempontjainak értékelésére. Ezzel a MIBÉTS a megbízható harmadik felek által végzett biztonsági ellenőrzés és audit egységes szempontrendszerét alkotja meg.

• Az **Informatikai Biztonsági Iránymutató Kis Szervezetek Számára (IBIX)** [7] olyan szervezeteknek nyújt segítséget biztonságos informatikai rendszereik kialakításához, amelyek nem rendelkeznek jelentősebb informatikai rendszerrel, illetve ehhez elkülönült informatikai személyzettel. Az IBIX elsődleges célja, hogy segítséget nyújtson az informatikai biztonság megfelelő szintjének kialakításához önkormányzati és más informatikai szempontból kis méretű környezetben. Javasolt az anyag azon szervezetek számára, ahol a szervezet méreténél fogva nem áll rendelkezésre külön emberi és egyéb erőforrás az informatikai rendszerek biztonságának kialakítására és üzemeltetésére, hanem ezt „házon belül” kell megoldani.

A KIB 28. számú ajánlása [8] egy Követelménytár, amely az elektronikus közigazgatás fejlesztéséhez és üzemeltetéséhez szükséges szabványokat, követelményeket és előírásokat tartalmazza. Az *IT biztonsági követelmények*, és a *Termékek, szolgáltatások értékelésének, auditjának előkészítése* a 25. számú ajánlásra épülve, azt kiegészítő vagy végrehajtását támogató előírásokat tartalmaz, illetve a Egyéb követelmények, ajánlások számos biztonsági szabványt mutat be.

Az *IT biztonsági követelmények* részei:

- Biztonsági tervezési útmutató;
- IT biztonsági követelményrendszer - biztonsági szintek követelményei;
- IT biztonsági Követelményrendszer érvényesítésének módja;
- IT Biztonsági Politika követelményei;
- IT biztonsági stratégia követelményei;
- IT Biztonsági szabályzatok követelményei;
- IT biztonsági szintek és biztonsági kategorizálási minta;
- Közigazgatási Operatív Programok IT biztonsági környezete, követelményrendszere;
- Szabályzatmenedzsment rendszer követelményei;
- Útmutató az IT biztonsági szintek meghatározásához.

Termékek, szolgáltatások értékelésének, auditjának előkészítése rész tartalma:

- IT biztonsági értékelő labor koncepció;
- Létező tanúsítások megfeleltetése - Technikai leírás;
- Összetett termékekre vonatkozó értékelési módszertan;

- Rendszerekre vonatkozó értékelési módszertan;
- Termékekre vonatkozó értékelési módszertan;
- Útmutató akkreditorok számára;
- Útmutató rendszer-értékelők számára;
- Útmutató rendszer-integrátorok számára;
- Útmutató tanúsítók számára.

A KIB 25. számú ajánlása IBIR kötete meghatározza, hogy, hogy a közigazgatási informatikai rendszerek biztonsági szabályozása milyen elemekből álljon.

- **Informatikai Biztonsági Politika (IBP)**: „Az Informatikai Biztonsági Politika kinyilvánítja a menedzsment biztonság iránti elkötelezettségét, a biztonsági célt, valamint magas szintű biztonsági elvárásokat fogalmaz meg, amelyek a biztonsági cél elérését szolgálják, és amelyeket érvényesíteni kell a védelmi intézkedések specifikálása során."

- **Informatikai Stratégia**: „Az Informatikai Biztonsági Stratégia célja, hogy a szervezet üzleti igényeinek jövőbeni változásaival összhangban meghatározza az információbiztonság fejlesztésének tervét (középtávú, hosszú távú)."

- **Informatikai Biztonsági Szabályzat (IBSZ)**: „Az Informatikai Biztonsági Szabályzat rögzíti az IBIR működéséhez, működtetéséhez szükséges folyamatokat, megadja az érintett szereplők (pl.: információbiztonsági vezető, üzemeltető, rendszergazda, fejlesztési vezető, adatgazda stb.) feladatait, felelősségeit, hatásköreit. Rögzíti az információfeldolgozó rendszer elemeivel (dolgozók, alkalmazások, technológiai elemek, helyiségek stb.) kapcsolatos biztonsági követelményeket. Az Informatikai Biztonsági Szabályzatot olyan mélységig kell elkészíteni, hogy technológiafüggetlen tudjon maradni."

- **Informatikai Felhasználói Szabályzat (IFSZ)**: „A dokumentum részletesen szabályozza a felhasználók kötelességeit az informatikai eszközök használata során, meghatározza azokat a peremfeltételeket, melyek között a felhasználó kapcsolatot létesít az informatikai osztállyal, vagy az adatgazdákkal. A szabályzat részletesen kifejti a felhasználó által elvégezhető és tiltott tevékenységeket, megadja a számonkérés formáját és módját, rögzíti a biztonsági események jelentésével kapcsolatos kötelezettségeket."

- **Eljárásrend gyűjtemény**: „Az eljárásrend gyűjteménybe tartozó végrehajtási utasítások olyan alacsony szintű szabályzatok, amelyek részletesen, rendszer specifikusan rögzítik azokat a tevékenységeket, melyeket az informatikai biztonsági szabályzat rendszer függetlenül megkövetel."

A KIB 25. és 28. számú ajánlása szerint (legalább) három, a bizalmassági követelményeket előtérbe helyező szinten kell az informatikai rendszerek védelmét megvalósítani: a kiemelt szint, amely a minősített adatokat feldolgozó rendszerek, a fokozott, amely a belső használatú, bizalmas információkat kezelő rendszerek, valamint az alap, amely a széles körben, interneten keresztüli hozzáférést biztosító rendszerek védelmi szintje.

Bár a közigazgatás informatikai rendszerei igen jelentős mértékben adatbázis rendszerek, ennek ellenére az adatbázisok biztonságára vonatkozó specifikus előírást a hazai jogszabályok és ajánlások nem tartalmaznak.

AZ AMERIKAI MODELL

A következőkben bemutatjuk az Amerikai Egyesült Államok Védelmi Minisztériuma (a továbbiakban: DoD) által kidolgozott és alkalmazott adatbázis-biztonsági szabályozás rendszerét, majd ennek alapján következtetéseket vonunk le a lehetséges hazai adaptációra.

A DoD az USA hadereje adatbázisainak védelme érdekében adatbázis-biztonság megvalósítását szabályozó dokumentumokat dolgozott ki. A dokumentumok nyilvánosak és bármely szervezet számára hasznosíthatóak, így a civil szféra is szabadon felhasználhatja.

Fontosnak tartjuk kiemelni, hogy az említett DoD adatbázis-biztonsággal foglalkozó szabályozása egy nagyobb egységnek, az Egyesült Államok haderején belüli teljes informatikai rendszerre vonatkozó, az informatikai védelem megvalósításával és ellenőrzésével foglalkozó **Informatikai Védelmi Direktívának** [9, 10] és az erre épülő **Informatikai Védelmi Megvalósítási Utasításnak** [11] a része, melyek. Az említett dokumentumok meghatározzák az informatikai biztonság alapvető szintjét, a megvalósítandó ellenőrzési célok együttese formájában. Az előírt ellenőrzési célok a rendszerek működésbiztonsági kategóriáitól és bizalmassági szintjeitől függően kerülnek meghatározásra.

A **működésbiztonsági kategória** az informatikai rendszerek által kezelt információknak a DoD célkitűzéseinek, különösen a harci küldetéseknek megvalósításában betöltött jelentőségét tükrözi. A szabályozóban három kategória van meghatározva [10, 19. o.] Az **információk bizalmassági szintje** az informatikai rendszerek elfogadható hozzáférési követelményeinek (személyi biztonsági ellenőrzések és háttérvizsgálatok, hozzáférési engedélyek, tudnia-kell szabályozások, összekapcsolási ellenőrzések és engedélyek) és felhasználói hozzáférési módszereinek (intranet, Internet, vezeték nélküli kapcsolat) meghatározására szolgál. A védelmi minisztérium három bizalmassági szintet használ: minősített, bizalmas és nyílt. [11, 16. o.]

A különböző rendszer-összetevőkre vonatkozó részletes informatikai biztonsági ellenőrzési célokat, az alkalmazandó védelmi rendszabályokat, eljárásokat biztonsági beállítási (konfigurációs), vagy megvalósítási útmutatók rögzítik. Az Egyesült Államok hadereje esetében ezeket a Védelmi Informatikai Rendszerek Ügynöksége (Defenese Information Systems Agency, DISA), valamint a Nemzetbiztonsági Ügynökség (National Security Agency, NSA) készíti el és bocsátja ki.[14]

A DISA által kidolgozott **Biztonsági Technikai Megvalósítási Útmutató** (Security Technical Implementation Guide, STIG) segédeszköz a DoD informatikai rendszerek védelme minőségének növeléséhez. Az egyes útmutatók az adott informatikai rendszerösszetevő ismert biztonsági komponenseit, sérülékenységeit és a DoD informatikai védelmi politika által tárgyalt, ezekhez kapcsolódó kérdéseket tartalmazzák.

A DISA útmutatókhoz, az azokban foglaltak ellenőrzéséhez általában rendelkezésre állnak biztonsági ellenőrző listák és a biztonsági készenlétet ellenőrző szkriptek. Mindkettő lényegében azt ellenőrzi, hogy a vizsgált rendszer (rendszer-összetevő) megfelel-e az útmutatóban előírt követelményeknek (ellenőrzési céloknak), vagyis megfelelően van-e telepítve és konfigurálva, illetve megfelelően van-e felügyelve, kezelve.

Az informatikai rendszer biztonságos működésének ellenőrzését nyolc csoportba sorolják be, melyek a következők [11, 48-49. o.]:

1. Biztonság tervezése és konfigurálása
2. Azonosítás és hitelesítés
3. Alrendszer és eszközrendszer
4. Alrendszer határvédelem
5. Fizikai és környezeti biztonság
6. Személyi biztonság
7. Működésfolytonosság
8. Sebezhetőség és incidenskezelés

Az adatbázis rendszerekre – mint az informatikai rendszer egyik összetevőjére – is rendszer specifikus módon kidolgoztak biztonsági útmutatókat és biztonsági ellenőrzési listákat. Ezen dokumentumokban szereplő irányelvek betartása olyan biztonsági környezetet eredményez, mely teljesíti vagy felülmúlja a 2. működésbiztonsági kategóriába (MAC II.) sorolt, bizalmas adatokat kezelő információs rendszerek biztonsági szintjét.

Az **Adatbázis-biztonság Technikai Megvalósítási Útmutatója** [12] az adatbázis-kezelő rendszerek biztonságára vonatkozóan nyújt általános útmutatást gyártó független módon, illetve a DoD informatikai rendszerének részét képező adatbázis rendszerekre fogalmaz meg kötelezően betartandó biztonsági követelményeket. A biztonsági követelményeket csoportokba szedve tárgyalja a dokumentum, amiket egy általános leírással vezet be, majd az adott követelmény csoporthoz összegyűjti az oda tartozó ellenőrzési pontokat, de csak azokat, melyek általánosan érvényesek minden adatbázis-kezelő termékre. A következő példával szemléltetjük a leírtakat:

- **Biztonsági követelmény csoport neve**: Rendszer könyvtárak kezelésének ellenőrzése
- **Biztonsági követelmény csoport általános leírása**: Az adatbázis-kezelő rendszer és a vele kapcsolatos alkalmazások fájljai, könyvtárai megfelelő védelem hiányában sérülékenyek lehetnek jogosulatlan módosításokkal szemben. A jogosulatlan módosítás negatív hatással bírhat az adatbázis-kezelő rendszer és az alkalmazások adatainak integritására és elérhetőségére.
- **Biztonsági követelmény csoporthoz tartozó termék független ellenőrzési pont:** Az adatbázis-kezelő szoftver egy felhatalmazott alkalmazás tulajdonos tulajdonában van.

Az adatbázis rendszerekre vonatkozó általános biztonsági követelményeket az általános informatikai rendszerekre vonatkozó csoportosítás alapján gyűjti össze és tárgyalja. A fentiekben ismertetett nyolc pont szerint, abból az adatbázis rendszerekre önmagában nem releváns 5. és 6. pontokat kihagyva a következő csoportosítás szerint épül fel:

1. Biztonság tervezése és konfigurálása,
2. Azonosítás és hitelesítés,
3. Alrendszer és eszközrendszer,
4. Alrendszer határvédelme,
5. Működésfolytonosság,
6. Sebezhetőség és incidenskezelés.

Az általános követelményeket megfogalmazó Útmutató ellenőrzési pontjainál megtaláljuk azt a szerepkört, aki az adott ellenőrzési pont betartásáért felel. Az Útmutató a következő négy szerepkört használja: informatikai biztonsági menedzser, informatikai biztonsági munkatárs, adatbázis adminisztrátor, adatbázis szerver operációs rendszer adminisztrátor. Minden ellenőrzési ponthoz tartozik sérülékenységi kategória, mely a sérülékenység súlyosságának fokát jelzi az adott követelmény be nem teljesülése esetén. A következő kategóriákat határozták meg:

- 1. kategória: olyan sérülékenységet jelent, ami a támadónak közvetlen hozzáférést ad az adatbázis rendszerhez, ott superuser hozzáférést eredményez.
- 2. kategória: olyan sérülékenységet jelent, ami olyan információt nyújt a támadó számára, ami nagy valószínűséggel az adatbázis rendszerhez történő hozzáférés megszerzéséhez vezethet.
- 3. kategória: olyan sérülékenységet jelent, ami olyan információt nyújt a támadó számára, ami az adatbázis rendszer megsértésének lehetőségét hordozza magában.

Az Útmutatóhoz tartozó **Adatbázis-biztonsági Ellenőrző Lista** [13] gyártó specifikusan nyújt a biztonsági követelmények teljesítéséhez segítséget. Az Útmutató általános követelményeihez adatbázis-kezelő rendszerfüggő követelményeket fogalmaz meg - szintén **ellenőrzési pontoknak** nevezve el -, melyek gyakorlatilag egy konkrét biztonsági követelményt, annak részletes megvalósítási eljárását és ellenőrzési módját írják le. Az Oracle, MS SQL, DB2 adatbázis-kezelő rendszerekhez speciálisan elkészített ellenőrző listák jöttek létre, illetve a többi típust egy platform független módon megfogalmazott ellenőrző lista támogatja. Az adatbázis rendszerek automatikusan megvalósítható biztonsági auditját szkriptek segítségével is támogatják, ezek viszont kizárólag a DoD szervei számára elérhetőek.

JAVASLAT A MAGYAR SZABÁLYOZÁS KIEGÉSZÍTÉSÉRE

A következőkben az adatbázis-biztonság szabályozásának lehetőségeit tekintjük át a magyar közigazgatáson belül. Abból indulunk ki, hogy egyrészt a hazai informatikai biztonság szabályozásában már sok fontos lépés történt, ezt a cikk első felében már felvázoltuk Másrészt a jelenleginél szigorúbb és részletesebb hazai központi szabályozás szükséges az informatika egyes részterületeinek védelme tekintetében (különös tekintettel a működés kritikus területeken), ezen belül a publikációban az adatbázis rendszerek védelmére koncentrálunk. A magyar szabályozásban e tekintetben jelenleg egy hiányzó láncszemet érzékelünk. Célunk a nemzetközi szabványokhoz és a hazai KIB 25. számú ajánláshoz igazodó adatbázis-biztonság megteremtéséhez és fenntartásához szükséges lépések megfogalmazása.

Az Egyesült Államok Védelmi Minisztériuma által kidolgozott informatikai biztonsági és ennek részét képző adatbázis-biztonsági szabályozás egy nagyon precízen felépített rendszert alkot, aminek egyes részeit kívülálló szervezetek is felhasználják a saját informatikai védelmük tervezésére, megvalósítására. A hazai közigazgatáson belüli informatikai védelem szempontjából is például szolgálhat az amerikai modell oly módon, hogy fel kell tárni, mik a hazai adaptációra alkalmas részei, illetve mi az, ami a magyar viszonyok között nem alkalmazható. Az amerikai modell vizsgálata kapcsán annak két fontos tulajdonságát mindenképp célszerű szem előtt tartani:

(1) Az adatbázis-biztonsági szabályozás a teljes informatikai biztonsági szabályozás keretein belül helyezkedik el, annak struktúrájához és terminológiájához illeszkedik,

(2) Az adatbázis-biztonsági szabályozás két nagyobb egységből áll. Egyrészt egy általános adatbázis-biztonsági útmutatóból, másrészt a konkrét adatbázis-kezelő rendszerekhez kidolgozott ellenőrzési listákból.

A leendő magyar adatbázis-biztonsági szabályozásnak keretet kell, hogy jelentsen a már meglévő hazai informatikai biztonsági szabályozás, de ez nem lesz olyan szoros kapcsolat, mint az amerikai modell esetén. Gyakorlati szempontból ez azt is jelenti, hogy egy adatbázis-biztonsági útmutató vagy adatbázis-biztonsági ellenőrző lista szerkezetét tetszőlegesen fel lehet építeni, ennek nem kell egy már adott struktúrához igazodnia.

A magyar közigazgatásban jelenleg nincs és valószínűen még sokáig nem is lesz egy olyan központi szerv, mely fel tudná vállalni azt a feladatot, hogy a jelentősebb adatbázis-kezelő rendszerek esetében adatbázis-biztonsági ellenőrző listákat állít fel és tart karban. Ugyanakkor egy általános adatbázis-biztonsági útmutató kiadását célszerű lenne a magyar elektronikus kormányzat számára kiadni, majd az erre épülő, termékfüggő adatbázis ellenőrzési listák elkészítését az adatbázis üzemeltetők feladatául lehetne kijelölni.

Az általános adatbázis-biztonsági útmutató és az adatbázis ellenőrzési listák a KIB 25. számú ajánlása IBIR kötetében meghatározott informatikai biztonsági szabályozási szintek közül az Eljárásrend gyűjtemények körébe tökéletesen beilleszkedik. Azonban önmagában egy jó eljárásrend kiadása még kevés[1]. Használatát elő kell írni. Szintén elő kell írni, hogy a külső és belső informatikai biztonsági auditok során az alkalmazását vizsgálni kell.

Javaslatunk szerint a magyar szabályozásnak tartalmaznia kellene az adatbázis rendszerek üzemeltetésére, telepítésére, konfigurálására vonatkozó biztonsági követelményeket, gyártó független módon megfogalmazva. A szabályozás hatálya alá eső szervezetnek (azaz, aki megfelelően kritikus adatbázist üzemeltet) a biztonsági követelményeket át kell fogalmaznia konkrét biztonsági elemek, ellenőrzési pontok halmazává, ami a saját adatbázis-kezelő rendszerére és az aktuális működési környezetre érvényes. Ebből épülne fel a szervezet adatbázis biztonsági szabályzata.

Az adatbázis-biztonsági útmutatót kiadó központi szerv feladatába tartozna továbbá az alá tartozó szerveken történő felügyelet gyakorlása. A központi szerv feladat lenne annak ellenőrzése, hogy a kritikus adatbázisokat üzemeltető szervek létrehoztak-e ellenőrzési listát és elvégzik-e ennek alapján a biztonsági vizsgálatot. Elő kell írni központilag, hogy milyen gyakran kell a szervezetben a biztonsági szabályozás alapján az ellenőrzést lefolytatni, annak eredményét dokumentálni kell és külső audit során a biztonsági szabályzat meglétét és az annak való megfelelés dokumentumát be kell mutatni. A központi szerv javaslatokat, segítséget nyújthat abban, hogy a termékfüggő adatbázis ellenőrző listákat milyen forrásokra támaszkodva tudják az üzemeltető szervezetek elkészíteni.

Az **Adatbázis-biztonsági útmutató** tehát az adatbázis rendszerek üzemeltetésére, telepítésére, konfigurálására vonatkozó biztonsági követelményeket tartalmazza gyártó független módon megfogalmazva. Az amerikai modellel ellentétben - ahol az Útmutatót egy előre megadott felépítést követ – a magyar szabályozás felépítése követheti az adatbázis-kezelő rendszer és a tárolt adatok védelmének középpontba állítását. Az általános útmutató szerkezetének eltervezésekor érdemes figyelemmel lenni arra, hogy az üzemeltetők által elkészítendő ellenőrző lista alapjául is szolgálhasson a választott struktúra.

[1] Nagyon jó példája ennek a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottságának 12. számú ajánlása [15]. Igen széles körben kötelezően használtak, kivéve a közigazgatást, amely számára készült.

A következőkben megvizsgáljuk, hogy az adatbázis biztonsági követelményeket milyen szempontok szerint lehet csoportosítani, rendszerezni. A biztonsági követelményeket csoportosíthatjuk aszerint, hogy az a védendő objektum mely részelemének védelméért felelős. Az adatbázis rendszer védendő objektumának meghatározásakor elsőként kell említeni az adatbázisban tárolt adatok védelmét, illetve az adatbázis-kezelő rendszer védelmét. Ugyanakkor ezek közvetlen kapcsolatban állnak az informatikai rendszer más részelemeivel, melyek biztonsága szorosan kihat az adatbázis biztonságra is. Itt meg kell említeni az adatbázis-kezelő rendszer számítógépének operációs rendszerét, a hálózatot és az adatbázist elérő alkalmazásokat, de ezeknél az informatikai rendszer elemeknél csak az adatbázis biztonságra kiható biztonsági követelmények meghatározására szorítkozunk.

A védendő objektum-elemekhez kötődő követelményeket megkülönböztethetjük aszerint, hogy:

1. az adatbázis-kezelő rendszer biztonságos működéséhez köthető,
2. az adatbázisban tárolt objektumokkal kapcsolatos,
3. az adatbázis-kezelő rendszer gépének operációs rendszeréhez kötődik,
4. az adatbázis-kezelő rendszerrel érintkező hálózati kommunikációval függ össze vagy
5. az adatbázisokat elérő alkalmazásokkal kapcsolatos.

Javasoljuk, hogy két fő kategóriát állapítsunk meg:

(1) az adatbázis-kezelő rendszer védelmét és

(2) a tárolt adatok védelmét.

Az operációs rendszer, a hálózat és az alkalmazások védelmét az (1) pont alá, mint annak alkotóelemeit helyezzük be.

A biztonsági követelmények egy másik típusú rendszerezése az adatbázis rendszerek biztonságos működtetéséhez kapcsolódó különböző folyamatokra, eljárásokra épül. Az adatbázis-kezelő rendszerek működésével kapcsolatos folyamatokhoz sorolhatjuk a teljesség igénye nélkül a következőket:

1. adatbázis-kezelő rendszer telepítése és biztonsági frissítése,
2. adatbázismentés és helyreállítás,
3. adatbázis audit, log elemzés,
4. felhasználó azonosítás,
5. jogosultság kezelés,
6. incidenskezelés és
7. egyéb eljárások.

(Az utolsó egy olyan kategória, melybe az előző kategóriák egyikébe sem elhelyezhető elemek tartoznának például az éles és fejlesztői környezetek szétválasztásának kritériuma).

Az adatbázis rendszerek biztonsági követelményeinek rendszerezéséhez az előző két módszer ötvözésére épülő, hierarchikus felépítést javasolunk. Három fő kategóriát különböztetünk

meg; kettőt a védendő objektum részelemei alapján, illetve harmadikként a működtetési folyamatokat, eljárásokat, azaz:

(1) az adatbázis-kezelő rendszer védelme,

(2) az adatbázisban tárolt adatok védelme,

(3) működtetési folyamatok, eljárások.

Ezekbe, mint alkategóriák helyezzük el az operációs rendszer, a hálózat és az alkalmazások védelmét, a különböző működtetéssel kapcsolatos részfolyamatokat, illetve az egyéb összetartozó követelmény csoportokat. A következő táblázatban foglaljuk össze az adatbázis biztonsági útmutató egy lehetséges felépítését:

Fejezet címe	Fejezet alcímei
Adatbázis-kezelő rendszer biztonsága	• Adatbázis-kezelő rendszer konfigurációs követelményei • Operációs rendszer biztonsága - Adatbázis-kezelő rendszer program könyvtárának és fájljainak védelme - Adatbázis adatfájljainak védelme - Adatbázis rendszerrel kapcsolatos operációs rendszer szintű felhasználók beállításai • Hálózati biztonság - Listener védelme - Port védelem - Az adatbázis-kezelő rendszer külső interfészeinek és ezeken áramló információknak a védelme - Külső objektumok elérése és külső eljáráshívás - Tükrözés, elosztott rendszerek, database link - Távoli hozzáférés adminisztrációs feladatok elvégzésekor • Adatbázist elérő alkalmazások biztonsági beállításai
Adatbázisban tárolt adatok biztonsága	• Adatbázis objektumok védelme hozzáférés szabályozással - Általános elvek - Objektum privilégiumok - Rendszer privilégiumok • Adatbázis szerepkörök - Adatbázis adminisztrátori szerepkör - Alkalmazás fejlesztői szerepkör - Adatbázis alkalmazás felhasználói szerepkör - Adatbázis alkalmazás adminisztrátori szerepkör • Adatok védelme titkosítással - Hálózaton - Adatbázisban
Működtetési folyamatok,	• Ügyrendi, biztonsági és egyéb eljárások szabályzatok • Adatbázis-kezelő rendszer telepítése és biztonsági fris-

eljárások	sítése - Adatbázis-kezelő rendszer telepítésének és frissítésének tesztelése - Az adatbázis-kezelő rendszer frissítése - Az adatbázis-kezelő rendszer elkülönítése, a nem használt komponensek eltávolítása • Felhasználók azonosítása, hitelesítése, bejelentkezése - Adatbázis felhasználók - Csoportos azonosítás és hitelesítés - Egyéni azonosítás és hitelesítés - Inaktív felhasználók - Jelszavak tárolása és tulajdonságai - Tokenekre és tanúsítványokra vonatkozó szabványok - Adatbázis rendszerekbe történő belépések • Adatbázis audit, log elemzés - Általános követelmények - Az audit tartalma - Audit nyomvonal, monitorozás, elemzés és jelentés • Éles és teszt környezetek szétválasztása • Adatbázismentés és helyreállítás

1.táblázat. Adatbázis biztonsági útmutató szerkezeti felépítése

FELHASZNÁLT IRODALOM

[1] 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról

[2] *Muha Lajos*: Magyar Informatikai Biztonsági Keretrendszer (MIBIK), Budapest: Miniszterelnöki Hivatal, 2008.

[3] *Berkes Zoltán, Déri Zoltán, Krasznay Csaba, Muha Lajos*: Informatikai Biztonsági Irányítási Rendszer (IBIR), Budapest: Miniszterelnöki Hivatal, 2008.

[4] *Déri Zoltán, Lobogós Katalin, Muha Lajos, Sneé Péter, Váncsa Julianna*: Informatikai Biztonság Irányítási Követelmények (IBIK), Budapest: Miniszterelnöki Hivatal, 2008.

[5] *Balázs István, Déri Zoltán, Lobogós Katalin, Muha Lajos, Nyíri Géza, Sneé Péter, Váncsa Julianna*: Informatikai Biztonság Irányításának Vizsgálata (IBIV), Budapest: Miniszterelnöki Hivatal, 2008.

[6] *Balázs István, Szabó István*: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)), Budapest: Miniszterelnöki Hivatal, 2008.

[7] *Krasznay Csaba, Muha Lajos, Rigó Ernő, Szigeti Szabolcs*: Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX), Budapest: Miniszterelnöki Hivatal, 2008.

[8] e-Közigazgatási Keretrendszer Kialakítása projekt (2008): A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár, IT biztonsági műszaki követelmények

[9] DoD Directive 8500.1, Information Assurance (IA). – USA Department Of Defense, 2002.10.24.

[10] DoD Directive 8500.01E, Information Assurance (IA). – USA Department Of Defense, 2007.04.23.

[11] DoD Instruction 8500.2, Information Assurance (IA) Implementation. – USA Department Of Defense, 2003.06.06

[12] Database Secrity Technical Implementation Guide, Version 8, Release 1, 19 September 2007, Developed by DISA for the DoD

[13] Database Security Checklist, Version 7, Release 2.2, 30 October 2006, Developed by DISA for the DoD

[14] *Munk Sándor, Fleiner Rita*: Az adatbázis-biztonság szabályozása és megvalósítása az Egyesült Államok haderejében, Bolyai Szemle, XVIII. évfolyam 4. szám., 2009.

[15] *Bodlaki Ákos, Csernay Andor, Mátyás Péter, Muha Lajos, Papp György, Vadász Dezső*: Informatikai Rendszerek Biztonsági Követelményei (Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság ajánlása; 12.), Miniszterelnöki Hivatal, Budapest, 1996.

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Papp Zoltán
pappz.szeged@gmail.com

AZ ÚJ TECHNOLÓGIÁK VESZÉLYEI: RFID ÉS AZ ELEKTRONIKUS ÚTLEVÉL

Absztrakt

A tudomány és technika legújabb vívmányai szinte észrevétlenül jelennek meg a társadalom hétköznapjaiban, anélkül, hogy ezek jelenléte a felhasználókban tudatosulna. Úgy használják, hogy tisztában lennének a működés elveivel, technikai hátterével, így az új szolgáltatások előnyeit anélkül élvezik, hogy az alkalmazás esetleges veszélyei nem válnak ismertté előttük, ami a visszaélések elleni védekezés hatékonyságára is negatív hatással van. A cikkben a szerző egy, az élet szinte minden területén egyre nagyobb teret nyerő új technológiát, az RFID-t és annak veszélyeit mutatja be.

The latest achievements of science and technology become a part of everyday life in our society, without the users being really aware of their presence. They use them without properly knowing the principles of their operation, technological background so they enjoy the benefits of the new services without becoming aware of the potential threats lying in their applications, which has a negative impact on the efficiency of protection against abuse. In this article, the author presents RFID, a new technology that gains an increasing role in nearly all areas of life, as well as its risks.

Kulcsszavak: *RFID, terrorizmus, elektronikus útlevél, terrorism, electronic passport*

Napjainkban világszerte egyre nagyobb hangsúlyt fektetnek a terrorellenes küzdelemre, melyek érdekében újabb és újabb biztonsági intézkedéseket foganatosítanak, illetve újabb és újabb technológiákat vetnek be, melyektől a fejlett országok kormányzatai a biztonsági helyzet javulását remélik. A várakozások szerint ezekkel az új intézkedésekkel és az új eszközökkel a terrorcselekmények potenciális elkövetői kiszűrhetők, országhatárokon történő mozgásuk és tevékenységük akadályozható. A közvélemény azonban ezeket a szabályokat, illetve technológiákat sok esetben kényszerintézkedésként éli meg, mivel személyes

szabadságjogaik és személyes adataik védelmének korlátozását látják bennük, ami csökkenti a bevezetett technológiák támogatottságát a társadalom körében. A hatóságok eszköztárában egyik ilyen újdonság az elektronikus adatokkal ellátott útlevél lett.

Az útlevél egyik borítólapjába egy úgynevezett RFID chip-et tartalmazó lemezkét ültetnek be, amelyet a külső oldal felől, a papír-műanyag kompozit borítóba elhelyezett árnyékoló fémháló véd az illetéktelen letapogatás ellen. Az útlevelekbe beépített chip a szokásos, a vizuálisan is megjelenítethető adatokon túl a tulajdonos más biometriai adatait is tárolhatja, melyek tipikusan a fénykép, az ujjlenyomat, valamint a retinalenyomat lehet, melyek alapján ki lehet jelenteni, hogy egy ilyen típusú útlevél egy adott személyt teljes hitelességgel tud azonosítani.



1. ábra. Az RFID chip egy lehetséges elhelyezkedése az útlevélben
(forrás: www.meritummedia.com)

Az RFID rövidítést a Radio Frequency Identification (rádiófrekvenciás azonosítás) szavak kezdőbetűiből képezték, és az egyedi azonosító technológiák (AUTO ID) családjába tartozik, hasonlóan a vonalkódokhoz, csak épp működési elvében tér el. Ez egy olyan automatikus azonosításhoz és adatközléshez egyaránt használt technológia, melynek lényege adatok tárolása és továbbítása RFID címkék és jelolvasó eszközök segítségével.

Az RFID elvének megszületése a II. Világháború idejére tehető, amikor a radart feltaláló Sir Robert Watson-Watt vezetésével egy titkos projekt keretében a britek kifejlesztették az első aktív saját-repülőgép felismerő rendszert. Ennek előzménye az volt, hogy a radar rendszerek katonai felhasználását nagyban nehezítette, hogy a radarképernyőn megjelenő repülőgépekről a légvédelem nem tudta eldönteni, hogy melyik katonai erőhöz tartoznak, ami folyamatosan megnehezítette a radar készülékek adatainak értelmezését, illetve lehetetlenné tette a hatékony légvédelmi reagálást. A németek észlelték először, hogy amikor a pilóta billegteti a repülőgép szárnyait, a gépről visszaverődő rádióhullámok által a monitoron megjelenő kijelzések megváltoznak. Ez a kezdetleges módszer nevezhető az első passzív RFID rendszernek, mely alkalmas volt egy objektum azonosítására. A britek tovább fejlesztve az alapelgondolást egy adót helyeztek el saját légierejük gépeire, mely amint jeleket vett a hazai földi radarállomástól egyedi azonosító jeleket kezdett visszasugározni, majd ezt a jelet a földi állomás érzékelve sajátként azonosította a repülőgépet. Ezzel a britek megalkották az első aktív saját repülőgép

felismerő rendszert (IFF - Identify Friend or Foe). Az aktív RFID rendszerek azonosításának elve gyakorlatilag pontosan ugyanez [1].

A chip köré épített áramkör a bejövő rádióhullámokból indukál áramot, így gyakorlatilag a leolvasó hozza működésbe az eszközt, és a benne lévő adatokat az egyben antennaként is funkcionáló áramkörön keresztül sugározza vissza a leolvasó egységnek. Az adatok általában egyszer kerülnek betöltésre, később már nem írhatóak át, azaz a leggyakrabban használt chip-típus az egyszer-használatos, eldobható. Az RFID címkéknek több típusa van, közös jellemzőjük, hogy rendelkeznek antennával. A címkéket elsősorban energiaellátásuk alapján különböztetik meg [2]:

- Passzív RFID

  A passzív címkék nem tartalmaznak saját energiaforrást. Az olvasó által kibocsátott rádiófrekvenciás jel elegendő áramot indukál az antennában ahhoz, hogy a lapra épített apró, CMOS technológiával készült integrált áramkör feléledjen, és választ küldjön az adatkérésre. Az antenna tehát speciális tervezést igényel: nem elég, hogy összegyűjti a szükséges energiát, a válaszjelet is közvetítenie kell. A válaszjel általában egy egyedi azonosítószám, de előfordul, hogy a címke egy kisméretű memóriát is tartalmaz, ami lekérdezéskor ennek tartalmát is továbbítja az olvasó felé. Passzív címkék 125 kHz, 13,56 MHz, és UHF (860-960 MHz) tartományban működnek. Némely rendszer a 2,45 GHz-es sávot illetve egyéb sávot is használhat. A passzív lapkák rendkívül kisméretűek, jelenleg 0.4x0.4 milliméteres felületű, papírnál is vékonyabb címke a kereskedelemben kapható legkisebb darab. A passzív lapok hatótávolsága néhány méterig terjed, azaz ekkora távolságból olvasható ki a tartalmuk a használt frekvenciától függően. Alacsony előállítási költségének köszönhetően jelenleg ez a legelterjedtebb típus.

- Fél-passzív RFID

  A fél-passzív azonosítók annyiban térnek el a passzív társaiktól, hogy tartalmaznak egy apró, beépített elemet. Ez lehetővé teszi, hogy az integrált áramkör folyamatosan üzemeljen. Nincs szükség az antenna energiagyűjtő kialakítására, ezért azt adásra optimalizálják. Ennek köszönhető, hogy az ilyen típusú azonosítók válaszideje jobb, és az olvasási hibák aránya kisebb, mint passzív társaik esetén.

- Aktív RFID

  Az aktív RFID címkék vagy jeladók beépített energiaforrással rendelkeznek, melyek elegendő energiát biztosítanak bármilyen integrált áramkör üzemeltetéséhez és magához a jeladáshoz is. Nagyobb hatótávolságot és memóriakapacitást biztosíthatnak passzív változatuknál, némelyik még a vevő által küldött adatok rögzítésére is képes. A használt frekvencia általában 455 MHz, 2,45 GHz vagy 5,8 GHz és az olvasási távolság általában 20-100 méter. Néhány aktív címke impulzusszerűen üzemel, hogy takarékoskodjon az energiával, így akár 10 évig is képes üzemelni. A jelenleg kapható legkisebb aktív RFID jelző nagyjából fémpénz méretű.

A szakirodalomban elterjedten használják még a működési frekvencia szerinti csoportosítást is [3]:

- LF 125 kHz

  E frekvenciával működő chipek olvasási távolsága 0,5 méternél kisebb, energiaellátásuk alapján általában passzív (induktív csatolás) kategóriába sorolhatók. Hátránya, hogy még nagy mennyiségben gyártva is relatíve drágának számít, mivel az alacsony frekvencia drága rezet igényel. Legelterjedtebben beléptető rendszerekben, állatok nyomkövetésében, járművek indításgátlóiban alkalmazzák.

- HF 13,56 MHz

  Ezen a frekvencián működő chipeknek általában 1 méter az olvasási távolsága, túlnyomórészt passzív (induktív vagy kapacitív csatolás) energiaellátásúak. Előnye, hogy előállításuk olcsóbb az LF chipekénél. Tipikusan Smart-Card-ok és termék nyomkövetés esetében alkalmazzák.

- UHF 868-915 MHz

  E tartományban üzemelő chipeknek maximális olvasási távolsága 3 méter. Az aktív működésű chipek általában elemmel működnek, míg a passzívak kapacitív csatolásúak. Előnye, hogy az IC technológia fejlődése révén olcsóbb mind az LF, mind a HF chipeknél, illetve sok chip párhuzamos olvasásának esetében is megbízható. Fő felhasználási területük raklap és konténer nyomkövetés, csomagkezelés és díjfizető rendszerek.

- Mikrohullám 2,45 GHz és 5,8 GHz

  Ezen a magas frekvenciatartományban működő chipek olvasási távolsága 1 méter. Energiaellátásuk hasonló az UHF chipekéhez, az aktív chipek elemmel működnek, míg a passzívak kapacitív csatolásúak. Az UHF-hez hasonló olvasási karakterisztikával rendelkezik. Főleg ellátási láncokban és díjfizetési rendszerekben alkalmazzák.

Az RFID technológia fontos eleme az olvasó, melynek mérete, kivitelezése nagyban függ attól, hogy milyen funkcionalitással bírnak. Léteznek „buta” olvasók, korlátozott számítási képességekkel, és „okos” olvasók, melyek már beépített számítógépet tartalmaznak, így képesek az adatokat szűrni, tárolni, illetve különböző parancsokat végrehajtani. A gyors olvasók képesek többféle protokollal kommunikálni a chipekkel, továbbá léteznek olyan multi-frekvenciás olvasók is, melyek különböző frekvenciájú chipeket képesek olvasni.

Az RFID olvasók külső, illetve belső antennával egyaránt rendelkezhetnek. A külső antennával rendelkező RFID olvasókhoz egy, vagy akár több porton keresztül csatlakoztatható az antenna. Az olvasó rendelkezhet bemeneti és kimeneti portokkal, amelyeken keresztül külső eszközök csatlakoztathatók. Az olvasó rendelkezhet egyéb portokkal, amelyeken keresztül számítógéphez vagy hálózathoz csatlakoztatható. A régebbi típusú olvasók soros porttal rendelkeznek, azonban a legtöbb új típusú olvasó már USB, Ethernet, vagy akár Wi-Fi portokkal rendelkezik [3].

Az RFID chipeknek más technológiákkal szembeni nagy előnye, hogy tetszőleges helyen rögzíthetők, vagy akár be is építhetők az azonosítani kívánt objektumba, ami lehet tárgy, például egy árucikk, vagy alkatrész, illetve lehet élőlény is, így akár egy ember is. Már RFID

címkéket használnak a nagy logisztikai cégek, alkatrész raktárak, áruházak stb. a vonalkód helyett, hiszen így a különböző tárgyakon nem kell megkeresni a vonalkód helyét az azonosításhoz, ami jelentős időmegtakarítással jár. A gyorsaság mellett további nagy előny, hogy olcsó is, és a parányi méretéből adódóan egészen apró tárgyak azonosítására is alkalmas [4].

Az útlevelek esetében kizárólag a passzív chipeket használják, melyek – mint a bevezetőben már megemlítésre került – a vizuálisan is megjelenítethető adatokon kívül az okmány tulajdonosának más biometriai adatait is tárolhatja. A terrorfenyegetettségre hivatkozva a fejlett világ egyre több országa döntött az ePassport, vagyis az RFID chip-et tartalmazó elektronikus útlevél alkalmazása mellett, ami alól az Európai Unió tagállamai sem kivételek, így már Magyarországon is bevezetésre került ez a technológia.

Az érintett országok az új okmányok bevezetésére óriási pénzösszegeket áldoztak, ami azonban a szakértők véleménye szerint nem áll arányban a technológia által nyújtott biztonsággal. Már a bevezetés megkezdése előtt informatikai szakértők jelezték, hogy a technológia biztonsága korántsem akkora, mint azt a bevezető országok próbálják meg elhitetni állampolgáraikkal. Az e-útlevél gyengesége pontosan az, aminek érdekében az RFID technológiát kitalálták: egy adatszolgáltató rendszer, amely kérésre készségesen kiadja az érintettek személyes adatait, például vámvizsgálatnál, a repülőtereken, illetve más hivatalokban. A Nemzetközi Polgári Repülési Szervezet (ICAO) az elektronikus útlevél használatával kapcsolatosan ajánlásokat is megfogalmazott, mivel a kételkedő szakértőkhöz hasonlóan a szervezet sem osztotta a bevezetés mellett döntő országok optimizmusát, mely szerint az új típusú útlevél majd drasztikusan képes lesz csökkenti a visszaélések számát.

Az elektronikus útlevelek használatának metódusa nem tér el a chip nélküli okmányokétól. Határátlépéskor a hivatalnok a kinyitott útlevelet vizuálisan ellenőrzi, miközben az utas ujjlenyomatát az ujjlenyomat olvasómodulon keresztül beszkenneli egy számítógép. Magasabb fokú biztonság esetén egy kamera a szivárványhártya mintázatát is rögzítheti. A nyitott útlevél RFID chipjéből eközben a gép kiolvassa az információkat, melyeket összevet a szkennelt adatokkal, a hivatalnoknak egy képernyőre kivetíti az útlevél tulajdonosának fényképét, aki pedig eldönti, hogy az utas arca azonos-e a szkennelt fényképpel. Ez a procedúra szinte nem is vesz igénybe többlet időt a hagyományos útlevél ellenőrzéséhez képest.

Közelebbről megvizsgálva a technológiát, illetve annak felhasználási módját, az RFID chippel ellátott útlevél már közel sem tűnik olyan biztonságosnak. Egy nemzetközi konferencián egy Lukas Grünwald nevű német hecker az általa két hét alatt kidolgozott módszer segítségével saját útlevelén mutatta be, hogy teljesen legálisan és könnyen beszerezhető eszközökkel – laptop, RFID chipolvasó, üres RFID chip, chip-író – az útlevél adatai egy üres útlevél chipjére pillanatok alatt rögzíthetők.

Részleges biztonságot jelent az a tény, hogy az eredeti chip adatai nem írhatók át, tehát az ellopott, elvesztett útlevelet nem tudják közvetlenül felhasználni más személy biometriai adataival, viszont a tulajdonos személyiségét ellophatják. Ez azok számára lehet értékes zsákmány, akik valamilyen tiltólistán szerepelnek (például beutazási és tartózkodási tilalom alá esnek), viszont a megszerzett adatokkal a szabad mozgás lehetősége megnyílik számukra. Egy kis gondatlanságot, biztonsági rést kihasználva idegen adatokkal és egy kis szerencsével átjuthatnak az ellenőrzéseken.

Valójában azonban arra sincs szükség, hogy megszerezzék a kérdéses útlevelet. Akár egy táskába rejtett, megfelelő érzékenységű RFID olvasó segítségével gyakorlatilag észrevétlenül hozzájuthatnak az adatokhoz. Csak annyit kell tenni, hogy az olvasót a „hivatalos" olvasó közelébe kell jutatni. Amikor az útlevél kisugározza az adatokat a „titkos" olvasó, - ha megfelelő távolságon belül van - szintén veszi és rögzíti azokat. Ezután akár a helyszínen egy gépkocsiban, vagy mosdóban is megírható az új chip, a kérdéses útlevél elektronikus klónja. A klónozási eljárás legnehezebb pontja talán az üres RFID chippel rendelkező biankó útlevél megszerzése, vagy egy hamisított útlevélben a chip és a fénykép kicserélése.

Az elmúlt idők tapasztalatai azt mutatják, hogy a terroristák minden, számukra elérhető eszközt igyekeznek felhasználni akcióik végrehajtása során. A terrorszervezetek fiatalabb generációinak felnövésével arra lehet számítani, hogy az új technológiákra elődeiknél már jóval fogékonyabb fanatikus fiatalok jelentősen ki fogják bővíteni a terrorizmus eszköztárát. E generációnak már nem jelent problémát a számítástechnika, a programozás, a telekommunikáció. Az RFID technológia esetében nem a klónozás egyszerűsége az egyetlen veszélyforrás. Az említett konferencián a Flexilis Inc. munkatársai bemutattak egy videofilmet, amely egy megdöbbentő kísérletet rögzítettek. A jelenlegi, nem megfelelő árnyékolással rendelkező útlevélmodell nem mindig rejti el az adatokat. Amennyiben táskában, zsebben kicsit megnyitva van az útlevél, annak adatai már kiolvashatók. A videofilm azt mutatta be, amint egy bábu zsebébe helyezett útlevél adatait egy szemeteskukába rejtett leolvasó kiolvasta, majd az adatok alapján egy detonátort indított el.

Azonban egy RFID olvasó beállítható oly módon is, hogy akár csak egy nemzet útleveleire, vagy akár egyetlen kiválasztott személynek az adataira adjon jelet a detonátornak. Különböző megfontolásokból (például parkolási és autópálya díjbeszedés, sorompók mozgatása) ma már RFID chipeket szerelnek a járművekre is, így a fenti példához hasonlóan támadhatóak ezek is. Ettől kezdve a bombák akár személyre, járműre, illetve különböző tárgyakra is szabhatók.

A közeljövőben várható, hogy az Európai Unió több tagállama fog rendszeresíteni különböző, RFID technológiára épülő személyi azonosító kártyákat (például személyazonossági igazolványt), melyeknek az árnyékolása még annyira sincs megoldva, mint az útleveleké, így ezekből az adatok még könnyebben, még messzebbről kiolvashatóvá válnak. Fantáziánkat szabadra engedve azt is elképzelhetjük, hogy a nem túl távoli jövőben egy állampolgár egy ilyen személyi okmánnyal a zsebében belép egy épületbe, ahol már az ajtóban nevén köszöntik, majd személyére szabott információkat kap egy kijelzőn. A kiolvasott információk birtokában egy számítógép akár azt is könnyen meghatározhatja, hogy a chip birtokosa melyik marketing-célcsoportba tartozik, így annak a piaci szegmensnek szánt multimédiás reklámot közvetíti.

Az RFID azonosítási technológia terjedése megállíthatatlan, az élet egyre több területén (raktározás, gyártás-ütemezés, biztonsági beléptető-rendszerek, postai és futárszolgálatok, légi szállítás, tömegközlekedés, elektronikus fizetőkártyák, háziállatok azonosítása) alkalmazzák. Népszerűségét jelezheti az is, hogy 2006-ban az Egyesült Államokban, a Kaliforniai Egyetemen már RFID felsőfokú képzést is indítottak. Az RFID technológián alapuló azonosítási rendszerek tulajdonságaiból, alkalmazási területeiből szinte törvényszerűen következnek a jogvédők aggályai is, akik látomása szerint, ha a kormányzat vagy a multinacionális cégek megfelelő szenzorokat helyeznek el az utcákon, különböző épületekben, járműveken akkor nyomon követhetővé válnak az állampolgárok, felderíthetővé válnak szokásaik, az általuk fogyasztott termékek, baráti vagy tágabb ismeretségi körük. Az RFID és más új azonosítási technológiák a jogvédők megítélése szerint közelebb hozzák

George Orwell 1984 című regényében már vizionált, a „Nagy Testvér szemmel tart” jelmondat valósággá válását.

Összegzés

A tudomány területéről a hétköznapokba beszivárgó új technológiák értelemszerűen a társadalom szélesebb köre, a biztonsági szakterület és a gazdasági szektor számára is előnyökkel bírnak, az emberek kényelmét, a szolgáltatások színvonalát, a termelékenységét-költséghatékonyságot, vagy épp az ellátás biztonságát növelik, így elterjedésük megállíthatatlan. Azonban ezeknek a technológiáknak nem körültekintő felhasználása, vagy épp az alaprendeltetéstől merőben idegen területen történő alkalmazása, arra való ráerőltetése során olyan nem kívánt mellékhatások is jelentkezhetnek, melyek a technológiák által nyújtott előnyöket kérdésessé teszik. A cikkben vázolt példa is ezt támasztja alá, az elektronikus okmányok terjedése összességében növeli a társadalom biztonságát, azonban a személyes adatok biztonsága területén pedig mind az állam, mind pedig a bűnözők számára kiszolgáltatottá teszi az egyént.

Irodalomjegyzék

[1.] Vonalkód Centrum – Az RFID technológiáról (letöltve 2010. szeptember 15. (http://www.vonalkodcentrum.hu/index.php?page=234))

[2.] Wikipedia (letöltve 2010. szeptember 17. (http://hu.wikipedia.org/wiki/RFID))

[3.] BCS Hungary RFID Tudástár (letöltve 2010. december 4. (http://www.bcs.hu/hu/tudastar/tudastar_centrum/rfid_tudastar/))

[4.] Turcsán Tamás - RFID - Mi mindent lát a Nagy Testvér? (letöltve 2010. szeptember 16. (http://nonstopuzlet.hu/rfid-mi-mindent-lat-a-nagytestver-20090216.html))

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Serege Gábor
serege.gabor@zmne.hu

HEKKERTÁMADÁSOK A TÁVOL-KELETRŐL

Absztrakt

Az elmúlt évek során bizonyos változásokat figyelhettünk meg a hekkertámadások jellemvonásaiban. A világ „legtehetségesebb" hekkereit adó USA és Oroszország mellett új hekker generáció jelent meg a távol-keletről. Ezzel párhuzamosan egyre több ország esett áldozatul a kínai a régióból indított támadásoknak. Az elkövetők kilététére utaló nyomok felkutatása szinte lehetetlen, azonban mégis sokan nyíltan a kínai rezsimet állítják az akciók hátterébe.

By inspecting the past years, we could realize the changing of the features of hacker attacks. A new hacker generation has appeared from the Far East besides the classical American and Russian hackers. Since this time more and more nations have felt a victim to hacker attacks from region of China. In most cases finding evidence is impossible, but in the face of this fact, they suspect the governance of the People's Republic of China.

Kulcsszavak: *hekkertámadás, Kína, hálózati biztonság, Internet ~ hacker attack, China, network security, Internet*

BEVEZETÉS

Az információs technológia rohamléptékű fejlődésének eredményeként olyan új infokommunikációs berendezések tulajdonosaivá válhatunk, amelyek néhány évvel ezelőtt még csak tudományos elképzelésként szerepeltek a médiában és elérhetetlennek tűntek. Az információs társadalom befogadóképessége, illetve az új csúcskategóriás eszközök iránti igény nyújtja az IT szektor mozgatórugóját, amely cserébe elárasztja a piacokat a mindennapi életünket kényelmesebbé tevő szolgáltatásokkal és berendezésekkel. Példaként említhetjük a navigációs berendezéseket, az okostelefonokat, az internetes bankolást, illetve fizetési lehetőségeket, melyeket valószínűleg már használjuk is, vagy jövőbeli használatuk a terveink között szerepelnek.

A könnyen megszerezhető kényelemnek azonban hatalmas ára is lehet. Az említett eszközök és szolgáltatások közös jellemzője, hogy működésük alappillérét az Internethez való csatlakozás jelenti, ami egyrészt utat nyit számunkra a világ felé, másrészt potenciális

célponttá tesz bennünket. Az országok népességéhez viszonyított internetes csatlakozások számát felmérő kutatásban Észtország az elsők között szerepel, amely egyben utal lakosságának Internetes szolgáltatásoktól való függőségére is. A történelem során Észtországnak kellett elsőként szembesülnie a hálózati kapcsolatra épülő csúcstechnológia sötét oldalával, amikor 2007 májusában elvesztette az IT infrastruktúrája ellen indított hekker hadjáratot. [1]

A jól szervezett hekkertámadások jellemzője, hogy a támadó kiléte ismeretlen marad. Eljutni a tényleges kiindulópontig szinte lehetetlen, azonban meghatározni a földrészt, országot vagy épp régiót már könnyebb feladat. Amíg a XXI. század első éveiben a támadások meghatározó részét egyértelműen amerikai vagy épp orosz területekről hajtották végre, addig a 2005-ös évtől kezdve egyre gyakrabban indulnak támadások távol-keleti szerverekről. Ez a tény arra enged következtetni, hogy a távol-keleti informatikai „szakemberek" képzettségben, tudásban és technikai támogatottságban egyre jobban felzárkóznak a legkiemelkedőbbek csoportjába. [2]

A hekkertámadások kiemelt jelentőségéből adódóan vizsgálatom célja egyrészt megadni a hekker szó napjainkban használt jelentését, másrészt összefoglalni az utóbbi évek legjelentősebb távol-keleti szerverekről indított offenzíváit. Továbbá a megtámadott országok által kiadott jelentések alapján beazonosítani a támadók nemzetiségét és röviden bemutatni az Amerikai Egyesült Államok álláspontját megfogalmazó „Műveletek a cybertérben" elnevezésű doktrínát.

KI AZ A HEKKER?

Az elmúlt évek során a hekker szó jelentése gyökeres változáson ment keresztül, ezért ebben a fejezetben be kívánom mutatni, hogy mit takart ez az elnevezés a múltban és mit értünk alatta most, a jelenben.

Áttekintve a média szóhasználatát megállapítható, hogy a mindennapi szóhasználatban a hekker elnevezést hallhatjuk minden olyan esetben, amikor a számítógép rendszerek biztonsági réseit felismerő emberekről közölnek híreket. Egyszerűen a hekker elnevezés, mint gyűjtőnév terjedt el, ezért általában csak a hír tartalmából derül fény arra, hogy az esemény mögött ténylegesen milyen szándékú, illetve képzettségű személy vagy személyek állnak.

Meglátásom szerint azonban érdemes különbséget tenni, főleg azért mert a múltban a hekker elnevezést csak a kiemelkedő tudással rendelkező szakemberek érhették el. Ezek a szakemberek nem feltétlenül csak az informatika területéről kerülhettek ki, hanem egyéb más, mint például elektronikai, műszaki szakterületekről is. Köztük a kapocs a kimagasló alkotói szakértelem, az elismertség és a köztisztelet volt.

Ezzel ellentétben a mostani jelentés nem ennyire egyértelmű. Az előbb említett hagyományos értelemben vett használata megszűnni látszik. A hekker egyre inkább valamilyen számítógépes bűnözőt takar, aki tevékenységével az informatikai biztonság egyes összetevői ellen indít offenzívát. Céljai között elsőként szerepel az adatok ellopása, módosítása, törlése vagy épp az adott szolgáltatást biztosító informatikai rendszer rendelkezésre állásának a negatív befolyásolása. Azonban ez a leírás, a hekker szó által aggregált 3+1 csoportok egyes részeire igaz csak.

A hekker szó a következő csoportokat foglalja magába:

1. *Fekete kalapos (Black-hat) hekker:* Tevékenységére a fentebb leírtak jellemzők. Motivációs eszközök a pénz, az elismertség (alvilági körökben) és egyes esetekben a szélsőséges meggyőződés.[1]

[1] A fekete kalapos hekkerek műveleti területe az információs társadalom informatikai infrastruktúrájával együtt növekvő cyber-tér, amely egyben lehetőséget biztosít az aszimmetrikus hadviselés országhatárokat átlépő megvívására is.

2. *Fehér kalapos (White*-hat) hekker: kiemelkedő informatikai tudását legális megbízás alapján használja fel. Célja az adott számítástechnikai rendszer sebezhetőségének vizsgálata a szerződésben meghatározott kritériumok alapján. Feltárja a biztonsági hiányosságokat és javaslatot tehet azok kijavítására. A fehér kalapos hekker másik elterjedt elnevezése az etikus hekker.
3. *Szürke kalapos (Grey*-hat) hekker: mind fehér, mind fekete kalapos hekker megbízásokat is elvállal, így tevékenységére a kettősség jellemző.
4. *Script kiddie*[2]*:* az előző három csoport képviselőivel ellentétben nem rendelkezik kimagasló informatikai tudással. Tevékenységének alapját az Internetről letölthető és testre szabható kártékony alkalmazások adják. Általában iskoláskorú számítógépes vandálnak tekinthető, akinek célja az adott informatikai hálózat (például: iskola) szolgáltatásainak a támadása, illetve az abban való károkozás. Motivációs tényező a vandalizmus, a csínytevés.[3]

Összefoglalva megállapítható, hogy a hekker szó jelentése elvesztette eredeti tartalmát. Jelenleg kizárólag csak az informatikához kapcsolható, illetve gyűjtőnévként használva nem tesz különbséget a különböző céllal és motivációval rendelkező csoportok között. Az egyes csoportok jól elkülöníthetők egymástól, azonban érdemes megemlíteni, hogy az esetek jelentős százalékában a fehér kalaposok közé olyanok kerülnek, akik a fekete kalapos oldalon már bizonyítottak. [4]

AZ ELMÚLT ÉVEK HEKKERTÁMADÁSAI

Az első hekker támadás John Draper nevéhez köthető, aki az 1960-as évek elején elsőként generált olyan speciális telefon hangimpulzust, amellyel annak nem várt működését tudta előidézi. A kezdeti, kizárólag telefonhálózatokhoz köthető hackelések a 4. generációs számítógépek széles körű elterjedésétől számítva az informatikai hálózatok irányába tolódtak el. Napjainkra a hekkertámadásokról szóló hírek a média állandó szereplőjévé váltak, ami alátámasztja azt a tényt, hogy azok mindennapos események, illetve számuk ugrásszerűen megsokszorozódott.

A támadások döntő része amerikai vagy orosz hekkerek tevékenységéhez volt köthető. Az ezredforduló második felétől, azonban megfigyelhető egy fontos változás: új hekkercsoportok kezdtek megjelenni a Távol-Keletről.

Ebben a fejezetben össze kívánom foglalni mindazon kiemelkedő jelentőségű hekkertámadásokat, amelyek az elmúlt 3 év során kerültek nyilvánosságra és a kiinduló pontjuk a Távol-Keletre tehető. Fontosnak tartom hangsúlyozni, hogy a támadások hátterében állók pontos adatai (név, nemzetiség, megbízó) igen ritkán fedhetők fel, éppen ezért az általam bemutatott esetekben is csak feltételezni tudták a támadók kilétét.

A TÁVOL-KELETRŐL INDÍTOTT LEGJELENTŐSEBB HEKKERTÁMADÁSOK 2007-2010 KÖZÖTT

2007. augusztus: A „Sárga kémek” címmel jelent meg egy cikk a „Der Spiegel” német napilapban, amely arról számolt be, hogy a kormányzati informatikai hálózat több szegmensében trójai faló típusú programra bukkantak. A számítógépekhez hátsó kaputnyitó kódok Microsoft Office dokumentumokba rejtve kerültek a célhálózatba.[5]

[2] A „script kiddie” angol elnevezésnek magyar megfelelője még nem ismert.

A kémkedési ügy hatalmas felháborodást keltett Németországban, mondván Kína így akarja ellopni a technológiai újdonságokat.

A támadás kiindulási pontját pontosan nem tudták meghatározni, azonban egyértelműen Kínát állították az eset hátterébe.[6]

2007. szeptember: A brit külügyi iroda számolt be távol-keleti támadásokról, mintegy csatlakozva a németországi incidenshez. A hivatalos értesítők alapján a kormányzati szektort nap, mint nap érik informatikai támadások, azonban a Távol-Keletről kiindulók száma jelentősen megnőtt.[7]

Ez év végén a brit biztonsági hivatal vezetője levelet küldött a magasabb beosztású állami alkalmazottaknak, illetve a polgári szféra jelentősebb vezetőinek, amelyben felhívta figyelmüket a kínai informatikai kémtevékenységre.[8]

2007. október: Az Amerikai Egyesült Államok nemzeti laboratóriumának informatikai rendszerében fedeztek fel illetéktelen alkalmazásokat. A németországi támadáshoz hasonlóan a fő cél az adatok eltulajdonítása volt az állomásokon nyitott hátsó ajtókon keresztül. Ez az intézmény kiemelt fontossággal bír a mai napig is, hiszen több olyan szigorúan titkos technológiai dokumentációt tárolnak itt, mint például a nukleáris fegyverekkel kapcsolatos információkat.

A betörés körülményeit vizsgáló csoport jelentése alapján a támadás, amely az alkalmazottak elektronikus levelezésének a felderítésével, majd a megfelelő csatolmánnyal ellátott email elindításával kezdődött egy jól szervezett és irányított hekker csoportra utalt. John Markoff biztonsági szakértő nyilatkozata alapján a támadás nyomait felkutatva Kínába vezető szálakat találtak, ami természetesen nem bizonyíték arra, hogy kínaiak követték volna azt el.[9]

2008 április: Belgium és India csatlakozott azon országokhoz, amelyek az interneten indított támadások miatt nyíltan kezdték vádolni a kínai rezsimet. Belgium álláspontja szerint az akciók hátterében Kína állt. A fő okként Brüsszel kiemelt fontosságát emelték ki a NATO-ban és az Európai Unióban betöltött szerepe alapján.[10]

Indiai nyilatkozatok szerint az országot naponta több száz hálózati támadás érte a szomszédos államból, amelyek célja a kormányzati informatikai hálózat folyamatos figyelése és térképezése volt. Ez a tevékenység nem csak az információk megszerzésére irányult, hanem a kritikus informatikai infrastruktúra gyenge pontjainak a felderítésre is.

2008 november: Távol-Keletről származó támadás érte a Fehér Ház levelező rendszerét. Ugyan ebben a hónapban látott napvilágot a NASA rendszerét 2005-ben ért támadásról tudósító beszámoló is, amelyet addig titokban tartottak. A taiwani szerverekről kiinduló akció során a behatolók több hónapon keresztül zavartalanul másoltak titkos adatokat az űrközpont szuper titkos számítógépeiről, illetve ki tudták terjeszteni hozzáférésüket más kiemelt fontosságú adatbázisokhoz is. A végeredmény 20 GB letöltött adat, mintegy 30 millió oldalnyi csúcstechnológiát tartalmazó dokumentáció.

Az eltulajdonított adatokból származó károk mellett érdemes kiemelni a morális veszteséget is. Az Amerikai Egyesült Államok csúcs kategóriájú informatikai biztonsági rendszerrel ellátott hálózata veszteségként került ki a cybertérben indított támadásból.

2009. április: A támadások középpontjában ismételten Németország állt. A hivatalos tájékoztatók alapján az országot igen jelentős mennyiségű támadás érte távol-keleti szerverekről. Az akció forgatókönyve a már ismert eljárást tartalmazta: a kijelölt célpontok

levelezési címeinek felderítése után megfelelő csatolmánnyal ellátott levelek által kívántak hozzáférni az adatokhoz.

Németországon kívül a hónap során hasonló támadás érte az ausztráliai elnököt is, valamint a dél-koreai kormányzati szektor pénzügyi részét is.[11]

2010. január: Támadás érte a Google rendszerét. Az eddig számbevett esetekkel ellentétben a célpont nem állami rendszer volt, hanem a Kínában jelentős részesedéssel bíró külföldi keresőóriás. Elemzők véleménye alapján a háttérben a Google és Kína nézetkülönbsége állt, ugyanis a vállalat meg akarta szüntetni a keresőmotor „cenzúráját".

A januárban felröppent hírek szerint az akció nem csak a Google-t érintette, hanem másik 34 óriásvállalatot is. Az elkövetés módja ismételten kiemelkedő szervezettségre, szaktudásra és anyagi forrásokra utalt: a támadók olyan szervereket hoztak létre, amelyek weboldalaiba az Internet Explorer biztonsági hiányosságát kihasználó kódot injektáltak.

Összegezve megállapítom, hogy a bemutatott esetekben több hasonlóság is felfedezhető:

- a célpontok meghatározó része a különböző államok kormányzati, kutatási, és technológiai informatikai hálózatai voltak. Ezek a rendszerek különböző szintű minősítéssel rendelkező fontos dokumentumokat tároltak;
- biztonsági szakértők véleménye alapján a behatolások hátterében összehangolt, magasan képzett hekkerek álltak;
- a támadóknak nem csak a kimagasló szakértelemre, hanem jelentős anyagi háttérre is szükségük volt az akciók kivitelezéséhez;
- a támadások kiinduló pontjára utaló nyomok a Távol-Keletre, azon belül is főleg Kína négy nagy városára, illetve Taiwanra mutatnak;
- valamennyi megtámadott ország bizonyos mértékben a kínai államot állította az akciók hátterébe.

KÍNA RÉSZESEDÉSE A HEKKERTÁMADÁSOKBAN

Az előzőekben számba vett hekker műveletek egytől egyig professzionális elkövetőkre utaltak, akik nagy hangsúlyt fektettek az árulkodó nyomok álcázására, illetve megsemmisítésére. A konkrét bizonyítékok ellenére a megjelenő nyilatkozatok a kínai államot tüntették fel megbízóként és az anyagi, technikai háttér biztosítójaként is. Az alfejezet célja bemutatni azokat a tényeket, amelyek a kínai szerepvállalást támasztják alá, illetve cáfolják azt.

Egy informatikai biztonsággal foglalkozó kanadai csoport (Secdev Group) 2009 márciusában egy világméretű „kémhálózat" létét fedezte fel. A rendszer irányításáért felelős szerverek azonosítása által a nyomok egyértelműen egy kínai, rádióelektronikai felderítést végző katonai egységhez vezettek. Ez a „gh0st RAT" trójai alkalmazásra épülő rendszer a világ 103 országára terjedt ki, és mintegy 1300 követségi, kormányzati, gazdasági intézményi célpontot tartalmazott.

A trójai alkalmazás önmagában egy viszonylag egyszerű működési mechanizmuson alapult, amely során először létrehozott egy dll kiterjesztésű file-t, majd elindított egy szolgáltatást, aztán végrehajtotta a szükséges módosításokat a regisztrációs adatbázisban és végül nyitott egy portot. A támadók így teljes hozzáférést kaphattak a „fertőzött" gépekhez, amelyekről nem csak a tárolt adatokat másolhatták le, hanem a csatlakoztatott hang és képrögzítő perifériák vezérlésével meg is figyelhették az adott felhasználót.

A GhostNet leleplezése világszerte óriási felháborodást váltott ki. A kémkedési botrány ugrásszerűen megnövelte azok számát, akik nem csak ezen ügy kapcsán, hanem a többi Távol-Keletről indított támadás esetében is már nyíltan a kínai rezsimet tették felelőssé. Kína

hivatalosan még az egyértelmű bizonyítékok[3] ellenére sem ismerte el a vádakat, ellenben többször hangot adott stratégiai elképzeléseinek, amelyben egyértelműen kinyilvánította álláspontját a cybertérben megvalósítható műveletekkel kapcsolatban.[12]

Véleményem szerint ezek a tények nem elégségesek ahhoz, hogy a kínai állam szerepvállalását egyértelműen bizonyítsák. Kína az elmúlt évtized során hatalmas beruházásokat hajtott végre informatikai infrastruktúrájának fejlesztése érdekében. Jelenleg Kína rendelkezik az egy országra eső legtöbb internet-felhasználóval (400 millió), így a nagy számok törvényét alapul véve feltételezhető, hogy számos kiemelkedő tudású hekker is van közöttük. A rezsimhez köthető szálak nélkül más nemzetek megbízása alapján, vagy szélsőséges ideológiai nézetekkel vezérelve is indíthatták ezeket a támadásokat. Továbbá érdemes megfigyelni az 1. számú táblázatot, amely azokat az országokat mutatja, amelyek a világon a legtöbb ártalmas kódot bújtató webszerverrel rendelkeznek. A lista alapján a kínai szerverek 44,8%-a tartalmazott olyan kódokat, amelyek az adott weboldal meglátogatása során vagy adathalászatra specializálódtak, vagy egyéb alkalmazást próbáltak futtatni a gyanútlan látogató számítógépén. Meglátásom szerint ebből két következtetés vonható le:

1. az adott állami szabályzók nem voltak képesek féken tartani az újdonságként megjelenő kínai hekker generációt;
2. Kína vált a legjobb kiindulóponttá a hekkertámadások végrehajtására, ugyanis a kialakult nemzetközi morál alapján elsőként a kommunista vezetést vádolták.

Top malware-hosting countries

Position	Last month	Country	Percentage of reports
1	1	China (inc. HK)	44.8%
2	2	United States	20.8%
3	3	Russia	11.3%
4	4	Ukraine	7.7%
5	8=	Poland	2.4%
6	5	Germany	1.6%
7	Re-entry	Netherlands	1.1%
8	Re-entry	Italy	0.9%
9=	8=	Canada	0.8%
9=	7	United Kingdom	0.8%
Others			7.8%

1. táblázat. Ártalmas kódokat tartalmazó webszerverek országos megoszlása 2008-ban (Forrás: www.sophos.com)

[3] A nyomozás során feltárt bizonyítékok: egy kínai egyetemista hekkert sikerült beazonosítani és felderíteni a kapcsolatait, amelyek az irányításért felelős központhoz vezettek, a vezérléshez szükséges szálak egy katonai szervezethez vezettek, az óriási mennyiségű információ feldolgozásához kiemelkedő informatikai infrastruktúrára volt szükség, amelynek rendszerben tartása óriási anyagi hátteret feltételez.

Végkövetkeztetések

Összegezve megállapítható, hogy a cybertében végezhető műveletek jelentősége és súlya folyamatosan növekszik. Az információs társadalmat kiszolgáló informatikai infrastruktúra védelmi vonala nem képes megállítani az olyan hekkertámadásokat, amelyek hátterében kimagasló tudású emberek állnak megfelelő anyagi és technikai támogatással. Az elkövetők kilétéhez vezető nyomok felkutatása sokszor lehetetlen. Az alkalmazott titkosító algoritmusok és útvonalvezérlések személytelenné teszik a támadókat.

Az elmúlt évtizedben Kína jelentős lépéseket tett az országa informatikai hálózatának a kiépítésére. Napjainkra fejlett hálózata 400 millió felhasználót szolgál ki. Az infrastrukturális beruházást szakmai felzárkózás követte, amely hatására jelentősen megnőtt a kínai hekkerek száma. Illegális tevékenységük folytatására kedvező táptalajt szolgáltatott az országban kiépülő szerverfarmokon elhelyezhető törvénytelen alkalmazások lehetősége. Természetesen ez az állapot más nemzetek hekkerei számára is „szinte" kihagyhatatlan alkalmat jelentett.

Az említett esetek során a támadást elszenvedett országok igaz változó formában, de mind a kínai vezetést állították az akciók hátterébe. A vádak mögött konkrét bizonyítékokkal- egy eseten kívül (GhostNet)-, nem tudtak szolgálni, mivel csak a távol-keleti kiindulópontot sikerült beazonosítani.

A cybertér „kalózai" között vitathatatlanul megjelent a távol-keleti hekker generáció is, amely eredményeként Bruce Scheiner világhírű biztonsági szakember szavainak aktualitása megnövekedett. Véleménye szerint: „A technológiai fejlődés néha a támadást könnyíti meg, máskor pedig a védekezést. Rohamosan változó technológiai világunkban fontos, hogy figyeljünk az új biztonsági egyensúlyhiányokra."[13, [12 pp.]]

A felbomló egyensúly olyan változásokat idézett elő, amelyek megkövetelték az internetes bűnözés felderítésére alkalmas világméretű monitor hálózat rendszerbeállítását, vagy épp a cybertérhez köthető műveletek doktrinális szabályozását.

Irodalom

[1] Észtország: tájkép hekkercsata után, letöltve: 2010-11-25
http://index.hu/tech/net/eszt2060807/

[2] US report: China is expanding its corporate cyber espionage, letöltve: 2010-11-25
http://www.h-online.com/security/news/item/US-report-China-is-expanding-its-corporate-cyber-espionage-838173.html

[3] Hekker, letöltve: 2010-11-14
http://hu.wikipedia.org/wiki/Hekker

[4] USA Defense Department Recruits New Hekkers From DEFCON Hacking Conference, letöltve: 2010-11-23
http://scforum.info/index.php?PHPSESSID=a975e5c9e872b996cb791807f98cc01c&topic=3069.msg6940#msg6940

[5] Ulf Gartzke: Outrage in Berlin Over Chinese Cyber Attacks, letöltve: 2010-11-24
http://www.weeklystandard.com/weblogs/TWSFP/2007/08/outrage_in_berlin_over_chinese.asp

[6] Southern Weekend: Chinese hekkers are "black"?, letöltve: 2010-11-22
http://www.tekbar.net/hekkers-and-security/southern--weekend-chinese-hekkers-are-black.html

[7] Titan Rain: How Chinese Hekkers Targeted Whitehall, letöltve: 2010-11-23
http://www.buzzle.com/articles/151328.html

[8] MI5 alert on China's cyberspace spy threat, letöltve: 2010-11-22
http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece

[9] China suspected in hacking attempt on Oak Ridge National Lab, letöltve: 2010-11-24
http://www.industrialdefender.com/general_downloads/news_industry/2007.12.10_china_suspected_in_hacking_attempt_on_oak_ridge_national_lab.pdf

[10] Is China attacking Belgian computers?, letöltve: 2010-11-05
http://www.upi.com/Top_News/2008/05/03/Is-China-attacking-Belgian-computers/UPI-70831209790694/

[11] John Goetz – Marcel Rosenbach: 'Ghostnet' and the New World of Espionage, letöltve: 2010-11-20
http://www.spiegel.de/international/world/0,1518,618478,00.html

[12] Tracking GhostNet, letöltve: 2010-11-10
http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

[13] Bruce Schneier: Schneier a biztonságról, HVG Kiadó Zrt, Budapest, 2010, ISBN: 978-963-304-026-3

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Szegediné Lengyel Piroska
l.piroska@t-online.hu

AZ INFORMATIKA „PISZKOS BOMBÁJA" A SZÁMÍTÓGÉPES BŰNÖZÉS
Bevihetők-e az informatika távoktatásába a számítógépes bűnelkövetést lehetővé tevő ismeretek?

Absztrakt

Az informatika radikális fejlődése, illetve a vele együtt rohamosan terjedő számítógépes bűnözés, analóg és hasonló súlyú kérdéseket vet fel manapság, a 21. század elején, mint amilyeneket – például a nukleáris láncreakció békés, illetve pusztító célú alkalmazási lehetőségeinek áldás-átok dilemmája kapcsán – már több mint fél évszázada próbál több-kevesebb sikerrel kezelni az emberiség. Számos irodalom foglalkozik azzal, hogy a legújabb kor legnagyobb katonai és egyúttal társadalmi veszélye már nem az atomháború [1], hanem az informatikai bűnelkövetés következtében jelentkező kockázatok és lehetséges katasztrófák valószínűségének a növekedése. Az informatika hatalmával tehát ugyanúgy, mint ahogyan a nukleáris energia erejével, lehet élni és visszaélni. Hovatovább, a romboló célú informatikai tudást és potenciált, sokkal kisebb anyagi- és energiaráfordítással is meg lehet szerezni, miközben a vele való visszaélés veszélyével, sajnos, sokszorta nagyobb dimenziókban is szükséges számolnunk. Mint a legmodernebb, egyúttal legalattomosabb fegyverek egyike az informatika, pontosabban a – vele együtt elburjánzó – „romboló informatika" mindennél gyorsabb, „sui generis" globalizálódása, gyakorlatilag minden társadalmat, minden háztartást, minden egyes élőlényt, sőt a természetes és az épített környezetünket is egyaránt fenyegeti. Mindezen realitások a – veszély megelőzését, elhárítását, az esetleges bekövetkezett katasztrófák kezelését, a károk enyhítését és reparálását végezni hivatott – civil és a katonai erők számára új kihívásokat jelentenek. A kihívás részeként új dimenzióban jelentkezik az a dilemma is, hogy milyen körben terjeszthetők, oktathatók az informatikai bűnözéshez, és annak kivédéséhez szükséges ismeretek és ezen ismeretek mely halmaza alkalmas arra, hogy távoktatási keretek között is terjeszthető, illetve oktatható legyen. Mindenekelőtt, releváns-e egyáltalán az a kérdés, hogy a nyilvánvalóan bizalmas és nagyon kényes informatikai ismeretek bevihetők-e a távoktatás szférájába?

The radical speed of developments in the field of the informatics and the parallel accelerating pace of cyber criminality are raising similar serious questions, today, at the beginning of the 21st century, as the ones which – connected e. g. to the "boon/curse" dilemma of peaceful and destroying use of nuclear chain reaction – have been tried to be managed by the societies, with more and less success, since more than five decades. Several papers underline that it is not the nuclear war [1] which must have been the most threatening military and, also, social danger in the latest age, but the increasing likelihood of risks and potential catastrophes due to the cyber criminalities. The power of informatics can, as that of the nuclear energy, be used in a good and bad way, as well. Moreover, the "destroying knowledge and potential" can be gained by investing far less material and energy input in case of informatics, while one has to face multiplied dimensions of danger of using it for bad goals. The fastest than ever "sui generis" globalisation of the informatics, more precisely, that of the even growing "destroying informatics", as a weapon among the most up-to-date and, at the same time, most treacherous ones, has been threatening practically all societies, households, each and every being creatures, furthermore our natural and constructed environment, as well. All these realities represent new challenges for the civil and military forces dedicated for avoiding catastrophes, handling the eventually occurring ones, diminishing and repairing the damages. As a part of challenges, a new dimension is added to the dilemma of "what can be the extent of the population to be addressed by teaching materials on cyber criminalities and defending techniques against them and which parts of these materials can be treated as appropriate for spreading over by distance education (e-learning)". Nevertheless, has or has not any relevance the question of "whether to put obviously confidential and very sensitive types of information into the sphere of distance education?"

Kulcsszavak: *távoktatás, informatika didaktika, informatikai intelligencia, számítógépes bűncselekmények, kritikus infrastruktúrák, informatikai biztonság ~ online/distance education, didactics in informatics, intelligence in informatics, cyber criminality, critical infrastructures, security in informatics*

BEVEZETŐ

Az elmúlt években a didaktika „Mit, miért, mivel, hogyan?" kérdése az informatika-oktatásban folyamatosan napirenden volt, függetlenül attól, hogy az oktatás hagyományos vagy távoktatási keretek között folyt-e. Az a dilemma pedig, hogy „miként épüljön fel az informatika tananyag, milyen legyen az elmélet és a gyakorlat aránya, ugyanaz az informatika kell-e mindenkinek, milyen a jó informatika terem, befolyásolja-e az eszköz a gondolkodásmódot, mi legyen az informatika tankönyvben, kell-e az elektronikus tananyag mellé oktató…?", ma, a számítógépes hálózatok, az Internet radikális térhódításának és azzal párhuzamosan a számítógépes bűnözés, az informatikai bűncselekmények terjedésének időszakában, különösen aktuálissá vált és további kérdéseket szül.

A kérdésekkel együtt, természetesen egyre többször vetődnek fel az alábbiakhoz hasonló kétségek, kételyek:

- Az informatikai tananyagok, műveltségi területek milyen speciális részeit, és milyen mélységig tanítsa meg az oktató?
- Az egyes tananyagrészek oktatásához milyen példákat, milyen esetpéldákat célszerű használni?
- Milyen veszélyekkel jár, járhat a valós események modellezése, a valós rendszerek modelleken keresztül való megismertetése?

Az informatikaórákon alkalmazott nevelési feladatok kapcsán felvetődik a jogos kérdés: Hogyan alakítható ki, fejleszthető tovább a pozitív informatikai intelligencia? Az informatikai ismeretek rossz irányú, illetve célú felhasználásának lehetőségeit, módozatait szükséges-e, illetve szabad-e oktatni?

Újfent szemben találjuk magunkat azoknak a „déjà vue" paradoxonoknak a tömkelegével, amelyeket a nukleáris fegyverek, a „szegények atombombái"-nak is nevezett piszkos bombák, a biológiai-, vegyi- és radiológiai fegyverek előállításának problémái kapcsán kezelni véltünk, de megoldani aligha tudtuk. Talán még az elmélet szintjén sem. Legfeljebb lokalizálni sikerült. A paradoxonok lényege ugyanis, miszerint az ilyen fegyverek előállításához szükséges technológia és szakértelem is „duális célú és felhasználású", tehát hasznos, de egyúttal pusztító is lehet, ténykérdés. Ebből fakadóan, a negatív fejlemények és kimenetek eshetősége, mintegy Damokles kardjaként, elkerülhetetlenül, folyamatos fenyegetettségként jelentkezik. A cél pedig a lokalizálás hatékonyságának az erősítése, a negatív fejlemények és kimenetek eshetőségének minél biztonságosabb kizárása, a gerjesztő jelenségek kiszűrése, kivédése, megszűntetése lehet.

E vonatkozásban, kézenfekvő eligazítást kínálnak az előző generációk mindennapjainak példái, amelyekről számos formában találhatunk – az irodalomtól kezdve a tudománytörténetig – plasztikus megfogalmazásokat. Több mint száz évvel ezelőtt, a radioaktivitás első alkalmazásai során például még senki sem gondolt arra, hogy évtizedekkel később majd tömegpusztító fegyvereket fejlesztenek ki a segítségével, inkább az orvosi terápiában látták hasznosan alkalmazhatónak a felfedezett jelenséget. Először Otto Walkhoff és F. Giesel észlelte, hogy a sugárzás roncsolja a szöveteket. Erről értesülve, Pierre Curie tíz órán keresztül tartott a kezén rádiumforrást, majd tapasztalatai alapján arról készített tanulmányokat, hogy az eljárás alkalmas lehet bizonyos bőrbetegségek kezelésére. Bár bizonyos jelek arra mutattak, hogy akár több kára is lehet az alkalmazásnak, mint haszna, mégis egy szörnyű halálesetre kellett várni, hogy felrázza a tudományos életet: egy amerikai üzletemberére, aki éveken át rádiumkészítményt használt közérzetjavítónak.

A paradox helyzet „kiteljesedésére" sem kellett sokat várni. Történelmi léptékkel mérve, pillanatok alatt következett be a nukleáris fegyverek gyors kifejlesztése és katonai alkalmazása. A magyarázathoz a világháborús körülményekre való utalás közismert. Olyannyira, hogy a világ iskolázott része a tananyag részeként, már tizenéves korában megtanulja, hogy az Egyesült Államokban 1939-ben kezdődött a nukleáris fegyver kifejlesztését szolgáló Manhattan-terv. Hogy a kutatások 1945. július 16-án értek be és felrobbantották az első kísérleti atomfegyvert. Hogy az új szuperfegyver alkalmazása is hamarosan bekövetkezett, hogy az amerikai hadsereg augusztus 6-án Hirosimára a Little Boy, 9-én Nagaszakira pedig a Fat Man elnevezésű atombombát dobta le. Miközben kérdéses, hogy mindezen történelmi események megismerése során a tizenéves generációk milyen mélységben gondolják végig a szörnyűséges paradoxonok tényét, illetve az oktatók mennyire érzik kötelességüknek és felelősségüknek ezen típusú empatikus képesség, emberi intelligencia kialakítását és fokozását.

Meggyőződésem, hogy a morálisan helyes oktatói intelligencia magában hordozza az ismeretek duális felhasználhatóságának teljes körű ismeretét, és megismertetési kötelezettségét, bemutatva annak mindennemű erkölcsi és jogi következményeit. Ugyanakkor, természetesen vizsgálni kell, hogy miképpen ellenőrizhető az ismeretátadás megbízhatósága, hogyan oldható meg a felelősségrevonás, amennyiben felmerül a gyanú, hogy a terjesztett ismeretek a társadalomra nézve károsak és hátrányosak. Más szavakkal, foglalkozni kell azzal a kérdéssel, hogy bizonyos ismeretek és tudás átadása meg kell ugyan történjen, az érintettséget, az illetékességet azonban – szakmai, etikai alapon – kénytelen-kelletlen, de elengedhetetlenül szabályozni szükséges.

A probléma, érthetően, egyre sűrűbben vetődik fel úgy az egyedi, mint a hétköznapok bejáratott távoktatásos rendszereinek alkalmazásakor is. Annak ellenére fenyeget, hogy a korszerű keretrendszereknek – pl. Moodly, ILIAS – köszönhetően a nyitott oktatás akár a széles körben alkalmazott megoldások esetében is „zárttá" tehető, technikailag tehát kizárólag csak a kurzusra beiratkozott hallgatók körére szűkíthető. Ezáltal természetesen lokalizálható az érzékeny információk és tudás távoktatásos kereteinek kockázata, teljes mértékben azonban nem zárható ki. A valóságban ugyanis reális lehetőségként kell számolni például azzal, hogy az arra feljogosított felhasználó, bár saját kódjával lép be a rendszerbe, de nem akadályozza meg arra illetéktelen felhasználók jelenlétét, sőt, rosszabb esetben – egyébként akár a rosszhiszeműség legkisebb jele és szándéka nélkül is – előfordulhat, hogy még támogatja is őket a tudás elsajátításában. Elgondolkoztató, Karen F. Owen, a Duke University végzős hallgatójának esete, aki „kvázi" diplomamunkát készített „An education beyond the classroom: excelling in the realm of horizontal academics" címmel, amelyben mintegy tucatnyi fiatalember, nevekkel ellátott legprivátabb adatait rögzítette, majd néhány ismerősének bizalmasan e-mail-ezte, akik szintén bizalmasan, továbbküldték másoknak, végül a világhálón kötött ki. [10]

HOGYAN? MIVEL?
A TÁVOKTATÁS MÓDSZERTANA

Az oktatás eszközrendszerének számbavétele kapcsán fontos leszögezni, hogy az Informatikai ismeretek a távoktatásos formában való közvetítésre ugyanúgy alkalmasak, mint bármely más ismeretanyag [2], ugyanakkor a tantárgy speciális területei – számítógépes hálózatok elleni támadások, informatikai bűncselekmények – újfajta távoktatásos módszertant igényelnek.

Paradigmaváltásra, új gondolkodásmódra, újfajta problémafelvetésre van szükség, amiből újfajta problémamegoldás fakad. A javasolt megközelítési mód találóan összegezhető a relativizmus atyjának, Albert Einsteinnek egyik híres mondásával: „Egy problémát nem lehet ugyanazzal a gondolkodásmóddal megoldani, mely a problémát előidézte."

Mindenekelőtt le kell szögezni, hogy az Informatika ismeretek távoktatása csak akkor lehet hatékony, ha a hagyományos tantermi oktatást – aminek alapja az „oktató és hallgatók közötti személyes kapcsolat", mint tantárgy specifikusság – teljes mértékben képes pótolni, ha a „távolság" nem csorbítja az oktatás minőségét, az átadott tudás tartalmát. Természetesen még nagyon sok olyan oktatási terület létezik, ahol elengedhetetlen az oktató és a hallgatók közötti személyes közreműködés, ugyanakkor az informatika előbb említett néhány speciális anyagrésze, a szakanyag közlésén túl, komoly nevelési feladatokat, azonnali reakciókat, reagálásokat követel meg az oktatótól.

Figyelembe véve az említett nevelési feladatokat, az Informatika tantárgy távoktatásának módszertani megoldásai céljára, hasznosnak ítélem a – Számviteli ismeretek e-könyveimben már sikerrel alkalmazott [11] – négyszintű modell [3] rövid áttekintését.

Az Informatika tantárgy távoktatásának négyszintű oktatási modellje		
Stratégia	**Módszer**	**Technológia**
Tanulás információn keresztül	Információ átadás **elektronikus könyveken** keresztül	Internet CD
Tanulás interakcióval	**Interaktív tanulás** Tanulás szimulációk, játékok, modellek segítségével. Saját ütemezésű tanulás on-line előadásokon	Multimédiás eszközök
Tanulás együttműködve	**Kooperatív-munka** **On-line foglalkozások** virtuális oktató termekben	Személyes kapcsolat Együttműködés
Tanulás csoportban	**Pódium - Drámapedagógia** **Tapasztalat-orientált oktatás, a szerzett ismeretek elmélyítése** szerepjátékok, esettanulmányok, projekt feladatok	Személyes kapcsolat Együttnevelés

A négyszintű modell egyik alapelve a fokozott együttműködés. A modell az ismeretátadás és az együttműködés lépcsőfokain halad előre, az alapvető információk megszerzésétől a felsőfokú ismeretek szintjéig terjed.

Ez a modell arra igyekszik rávilágítani, hogy a távoktatásra szánt anyag tantárgyi programjának kidolgozása során nem szabad megfeledkezni arról, hogy az e-oktatás teljes mértékben nem helyettesítheti a tantermi oktatást, a képességek fejlesztésének bizonyos fokán mindig is szükség van az oktatóval, az adott téma szakértőjével való találkozásra.

A tanulási folyamat első szintjén – **„Tanulás információn keresztül”** – az alapvető ismeretek átadása, az alaptudás biztosítása az „Olvasd!”módszeren alapszik. Cél, hogy a tanuló könnyen és egyszerűen megtalálja az információt, könnyen és gyorsan elsajátítsa azt, amit a tananyag, a könyv közölni akar. A módszertanilag és didaktikailag átgondoltan szerkesztett könyv alapján a felhasználók világosan átlátják a tananyag elsajátításának lépéseit, az abban való haladás ütemét.

A második szinten – **„Tanulás interakcióval”** – a **„**Fedezd fel!”módszer az alapvető képességek fejlesztésére fókuszál: az új alkalmazások, eljárások megismerése szimulációk, modellek, esetleg játékos feladatok közvetítésével történik, időfüggetlen on-line előadásokon.

A harmadik szint – **a „Tanulás együttműködéssel”** – a **„**Vitasd meg!” alapvetően a társakkal való együttműködési technikákra épül, ahol a képzés nevelési feladatainak meghatározó elemeként megjelenik a tanterem. A felhasználók virtuális osztályteremben csoportos feladatot kapnak, véleményt cserélhetnek, tapasztalataikból közösen tanulhatnak. A háttérben megjelenik/megjelenhet az oktató, akinek lehetősége nyílik az egyéni képességek feltérképezésére, a felhasználók gondolkodásmódjának megismerésére.

A negyedik a – **„Tanulás csoportmunkával" – „**Játszd el**!"** szinten**,** a tanterem mellett az oktató is a tanulási folyamat „főszereplőjévé" válik. A modellnek ez a szintje, a tanulási folyamat eredményeként jelentkező, az igazán fejlett, illetve színvonalas ismeretek és képességek birtokában használható hatékonyan, az alapfokú tudástranszfernél nem. A gyakorlati feladatok és konkrét esetek kivitelezése során felhasználói oldalról lehetővé válik az ismeretek elmélyítése, oktatói oldalról, pedig a felhasználók elsajátított tudásszintjének felmérése, gyakorlati problémamegoldó képességük megismerése.

MIT? MILYEN MÉLYSÉGIG? A TANTÁRGYI PROGRAM

A tantárgyi program összeállításakor nem kis dilemmát okoz, hogy az informatikai tananyagok, műveltségi területek milyen speciális részeit és milyen mélységig tanítsa meg az informatika-oktatásra vállalkozó szakember, illetve tanár?

Gyorsan változó világunk és a globalizáció, az Informatika-oktatást is komoly kihívások elé állította. Magyarország esetében is egyértelművé vált, hogy a NATO és az Európai Unió tagjaként csak akkor maradhatunk versenyképesek a társországokkal szemben, ha korszerű, az információs technológiák rohamos fejlődésével lépést tartó, versenyképes tudást tudunk közvetíteni a felhasználók/tanulók felé. Ha a tudást nem csupán egy lexikális adathalmazzal azonosítjuk, hanem olyan aktív készletnek tekintjük, amely az összefüggések rendszeréből táplálkozik.

A felhasználó/tanuló fejlődéséért felelősséget vállaló oktatónak/tanárnak arra kell törekednie, hogy felkészítse a felhasználót/tanulót a gazdasági, társadalmi folyamatokban való aktív részvételre, ami napjainkban kizárólag magas színvonalú, elmélyült, gyakorlat-orientált informatikai oktatás mellett valósítható meg. Természetesem az informatika gyakorlati alkalmazásakor a szinte korlátlan lehetőségeken túl, az előbbiekben bemutatottak szerint, nem feledkezhetünk meg arról, hogy a romboló célú alkalmazhatósága komoly veszélyeket is hordoz. Ezzel együtt és mindenekelőtt tekintettel arra, hogy az informatikai eszközök és tudás alkalmazása normális mindennapjaink elengedhetetlen részévé vált, szükség van egyfajta kompromisszumos megoldásra a tanterv kidolgozása terén.

Véleményem szerint ez a kompromisszumos megoldás egy **„két szinten" történő probléma-megközelítést** igényel. Jelen írás rövid terjedelme nem teszi lehetővé ennek részletes kidolgozását, ezért alapvetően csak az irányok meghatározására szorítkozik.

AZ ELSŐ SZINT

Az első szintet a **tömegek elérését célzó szintnek** is nevezhetjük. Először is, a távoktatás a számítógépes bűnözés általános veszélyeinek, a megelőzésnek, az elhárításnak, illetve az esetleges károk reparálásának a nagy tömegekkel való megismertetéséhez a lehető legszélesebb mértékben alkalmas. Ezért, illetve ennek érdekében indokolt és szükséges a távoktatás legkorszerűbb módszereit alkalmazni, azaz, a legkorszerűbb tananyagokat kifejleszteni és terjeszteni. Amikor nagy tömegekről beszélünk, ennek azért van rendkívüli jelentősége, hogy tudatosuljon az informatika tömeges, mindennapi használói számára az „informatikai hirosimák és nagasakik", az „informatikai piszkos bombák" veszélye és ártalmassága, megelőzésük és kivédésük fontossága.

Ha például az informatika oktatás során a feldolgozandó téma **az elektronikus adatfeldolgozó és adatátviteli rendszer,** akkor a rendszer felépítésének, működésének ismertetése nem lehet teljes körű a rendszerbe történő illetéktelen belépés módozatainak, hatásainak ismertetése, megvitatása nélkül. Az oktatónak szakmai, de nevelési célzattal is fel kell vetnie a "jó hacker" és „rossz hacker” kérdést [4], meg kell vitatnia a felhasználókkal/tanulókkal a rendszerbe történő jogszerű/illetéktelen belépés direkt és indirekt előnyös/kártékony hatásait. Felelősen állást kell foglalnia a „hacker munkáról”, be kell mutatnia és kommentálnia kell az eseteket: például a jó hacker letörli a gyűlöletkeltésre alkalmas uszításokat, a szélsőséges politikai és vallási nézeteket tükröző képeket, a kábítószer fogyasztását vagy a bombakészítést népszerűsítő oldalakat, a valóságos háborúkat rendszeresen kísérő cyber-háborúskodás üzengetéseit, megtévesztő híreit, illetve arról az esetről is amikor „csak egy jó hecc”, „egy jó balhé” [5] kedvéért betör például egy bank informatikai rendszerébe**.** Konkrétan, visszautalva a felvázolt oktatási modell „Tanulás csoportmunkával” szintjére, a „jó hacker”, illetve „rossz hacker” tevékenységének elemzése a filozófiai, az erkölcsi, etikai problémák részletes mélységéig hatolhat. A felhasználók/tanulók állásfoglalásait, véleményeit az oktató/tanár kiegészítheti, az esetleges téves elgondolásokat jó mederbe terelheti. A felhasználó/tanuló és az oktató/tanár közötti személyes kapcsolat megteremti a lehetőségét annak, hogy utóbbi tudatosítsa az előbbiekben, hogy a „jó hacker”, bár beavatkozásával a rendszer tökéletlenségeit kijavíthatja (például a leginkább használt fájlokat könnyebben elérhetővé teheti), a védelmi, biztonsági elemek hiányosságait felfedheti, ugyanakkor bármennyire nemes szándék is vezérli, mégis egy védett rendszerbe lép be jogosulatlanul és azon túl, hogy ezzel vagyoni, de sokszor pénzben ki sem fejezhető kárt okoz a helyi hálózat üzemeltetőjének (a weboldalak újraépítése, a jelszavak, kódok ismételt előállítása), számolnia kell az illetéktelen belépés jogi következményeivel is.

Érheti-e tehát az a vád az informatika-oktatást, az informatika tanárt, a távoktatási anyag készítőjét és terjesztőjét, hogy segíti a „fehérkalapos” bűnözés [4] terjedését?

A kompromisszumos megoldás ezen első szintjének esetében, amennyiben a számítógép, a programok és az adatok ellen véghez vitt intellektuális támadásokat, a programok és információhordozók jogosulatlan megszerzését, másolását, a bankkártyákkal történő visszaéléseket, a mobiltelefonokhoz tartozó SIM-kártya manipulálását, valamint az interneten elkövethető, azokon megjeleníthető jogellenes cselekmények oktatásának részleteit elutasítja, de az ellenük való védekezési módokat hangsúlyosan beépíti a tananyagba, akkor a jó célt tartva szem előtt, közvetlenül nem kell tartania a megvádolhatóság veszélyétől, miszerint a „fehérkalapos” bűnözést segíti.

Ezen első szint vonatkozásában szükséges külön kitérni azon szempont fontosságára, miszerint az oktatásnak elengedhetetlenül ki kell terjednie a tudatos Internet használatra. Az Internet által az emberi közösségek számára kitárul a világ, bárki számára hozzáférhetővé válnak addig ismeretlen, vagy nehezen hozzáférhető információk, felgyorsul a kommunikáció. Az Internet hihetetlen lehetőségek tárát nyitja meg, amely újfajta gondolkodást igényel a felhasználóktól, és erre az újfajta gondolkodásmódra való felkészítésben az oktatásra különös feladat hárul. Ezzel együtt, az Internet a számítógépes bűnözés „táptalaja”: az Internet segítségével világszerte, nehezen ellenőrizhető módon, nagy gyorsasággal lehet elkövetni számítógépes bűncselekményeket. [5]

Amennyiben áttekintjük a számítógépes bűnözés fejlődését, észrevehetjük, hogy míg a technika és a szakképzés nem vált tömegessé, addig nem is ölthetett olyan méreteket, mint napjainkban.

Az Interneten végrehajtott támadások napjainkig egyelőre főleg helyi jellegűek voltak, határozott és pontos célokkal, csak néhány esetben fordultak elő globális méretű kihatások, illetve nagyobb közösségeket, vagy a globális társadalmat jelentős mértékben érintő katasztrófa-következmények, ám a jövőben – pusztán az Internet egyre gyorsuló, globális elterjedésével és széles körű használatával párhuzamosan – az „Internet-oldali fenyegetettség", az „Internetes piszkos bombák" szaporodásának a veszélye növekszik. Nem zárható ki például, hogy több támadás ér majd olyan rendszereket, amelyek létfontosságú infrastruktúrák, katasztrófavédelmi és pénzügyi létesítmények működését támogatják.

Mindez megköveteli, hogy a jövőben, az oktatásban, ezen belül a távoktatási keretek között kellő hangsúlyt kapjon a számítógépes bűnözés elleni védekezés, mivel az emberek csak kellő informáltság mellett képesek felkészülni az ellenük irányuló támadásokra.

A MÁSODIK SZINT

A megközelítés általam javasolt második szintjén azokról **az érzékeny ismereteket jelentő legszofisztikáltabb és legmélyebb informatikai technológiákról és tudásról**, illetve mindezek megfelelő alkalmazásáról van szó, aminek elérhetőségét kizárólag és szigorúan csak az illetékes, arra feljogosított személyek részére kívánjuk biztosítani. Ezen szint esetében a távoktatásos megoldásokat – megítélésem szerint – csak korlátozott mértékben indokolt és szabad alkalmazni.

Álláspontom alapja az a tény, hogy korunkban, az információs társadalom korában megnőtt az információs támadásokkal való fenyegetés és bekövetkezésének veszélye. Az információs terrortámadások és agressziók olyan reális veszélyforrások, amelyek elleni védekezés csak országos (*sőt, globális*) szinten lehet hatékony [6]. A megelőző intézkedések megtételében, a veszélyhelyzetre való felkészülésben, az elhárításban a katonai-védelmi szféra felelőssége megkérdőjelezhetetlen. Az információs társadalom reális elvárása tehát, hogy a katonai szférában az informatikai oktatás programjából ne hiányozzanak a kritikus információs infrastruktúrák [7] [8], a kritikus infrastruktúrák elleni lehetséges támadások témakörei [9].

Ennek kapcsán sokszor felvetődik a kérdés: a távoktatás módszereivel kezelhető-e a szuper érzékeny informatikai ismereteknek és tudásnak – például a kritikus infrastruktúrák informatikai veszélyeztetési módszerei, technológiája, konkrét célpontok stb. – az illetékesekhez való eljuttatása? Véleményem szerint, az ilyen típusú ismeretanyagnak a távoktatásos átadása, még a legkifinomultabb megbízhatósági kritériumokhoz igazított zártkörű felhasználói környezetben is, mindenképpen kockázatosabb a hagyományos tantermi oktatási körülményekkel szemben. Bármilyen szűk körű ugyanis egy hálózat és bármilyen erős biztonsági kritériumokkal is látják azt el, annak puszta léte kockázatnövelő tényezőként jelentkezik. Egyrészt, a virtuális körülmények talaján megnövekszik az információbirtokosoktól történő esetleges információkijutás/kijuttatás veszélye. Ezt mutatja a már hivatkozott Owen-botrány, de még számtalan hasonló esetre lehetne utalni. Másrészt, egy ilyen távoktatási hálózat kialakítása esetén, pótlólagos kockázatként automatikusan megjelenik a külső behatolás veszélye is.

Ezzel együtt a második szinten is lehetnek olyan területek, amelyek a távoktatás eszközeivel kezelhetők, például a már bekövetkezett kritikus infrastruktúrák elleni támadások elemzése, vagy a már publikussá vált, a szakma képviselői számára már elérhető – bizalmas információ-átadást nem jelentő – információk, technikai, technológiai kérdések megvitatása.

Véleményem szerint, az oktatási koncepció analóg kell legyen a 21. századi hadviselésben bekövetkezett változásoknak megfelelően kialakított katonai doktrínákkal [6]:

ahogy az új hadviselési modellben különös figyelmet kap a kritikus infrastruktúrák, a számítógépes hálózatok védelme, a nemzetközi terrorizmust nyíltan vagy burkoltan támogató országok aszimmetrikus csapásainak elhárítása, úgy a katonai informatikai oktatás témaköreinek palettájáról sem hiányozhatnak ezek a témakörök.

.

ÖSSZEGZÉS

Ma, az információs társadalom – a tudomány eredményeinek intenzív és folyamatos felhasználására alapozott társadalom – korában, az informatika-oktatásban új típusú oktatási modellre van szükség. A „high-tech" kultúra, az informatikai és számítógép-hálózati alapú termelés, szolgáltatás, egyéni és közösségi életvitel, azaz a fejlett számítógépes technika társadalmi beágyazódása új kihívások elé állítja az oktatást.

Az informatika-oktatásnak jelentős szerepe van abban, hogy a fiatalok a társadalom hasznos tagjaivá váljanak, sikeres, elégedett életet éljenek. Ennek megfelelően egyfelől olyan tartalmat kell közvetítenünk a felhasználók/tanulók felé, amelynek gyakorlati haszna megkérdőjelezhetetlen, amelyet az élet legkülönbözőbb területein hasznosítani tudnak, másfelől törekednünk kell olyan gondolkodásmód kialakítására, amely az állandó változásokhoz képest időálló, képes azokkal együtt haladni, képes azokra gyorsan reagálni.

A technika fejlődésével megjelenő legmodernebb jogsértéseket, informatikai bűncselekményeket a hagyományos tantermek falait áttörve, a nyitott, virtuális teremben, a távoktatás keretei között is lehet, sőt a Life Long Learning, illetve a Life Wide Learning követelményeként szükséges is oktatni, de a megvalósítandó feladatoknak, célkitűzéseknek védelmi szempontúaknak kell lenniük.

A védekezés orientáltság dominanciáján túl, az érzékeny, speciális ismereteket, intellektust igénylő módozatok oktatása terén, pedig egyelőre a tradicionális képzési megoldások képesek biztosítani az elvárt biztonsági követelményeket. E területen tehát az e-learning hálózatok alkalmazása felé csak nagyon korlátozott és kontrollált szinten indokolt elmozdulni.

Oktatási intézményeinkkel, illetve rendszereinkkel szemben fontos elvárás, hogy a fiataloknak egyrészt magas szintű, az üzleti életben is hasznosítható informatikai ismereteket oktassanak, másrészt, hogy kiemelt hangsúlyt fordítsanak az információbiztonsági műveletek oktatására.

Az oktatásnak a cyber-terrorizmus nemzetközivé válásával is lépést kell tartania. A számítógépes hálózatok világméretűvé válásával ugyanis nem zárható ki, hogy illetéktelenek bármilyen távolságra lévő hivatal vagy intézmény bármilyen adatállományához hozzáférhetnek, ami egyrészt növeli a bűncselekmények veszélyét, másrészt felhívja a figyelmet a bűnüldözés nemzetközi összefogásának szükségességére, ami a képzést is újabb és újabb feladatok elé állítja.

Felhasznált irodalom

[1] Hanka László - Dr. Vincze Ádám - Dr. Solymosi József: A nukleáris terrorizmus, mint potenciális fenyegetettség napjainkban, ZMNE, Hadmérnök, On-line tudományos folyóirat, II. évfolyam, 4. szám, 2007. december, ISSN 1788 1919 p.: 4-24

[2] Szegediné Lengyel Piroska: Ötven éves a távoktatás? Hadmérnök On-line tudományos folyóirat, V. évfolyam, 3. szám. 2010. szeptember, ISSN 1788 1919 p.: 246-263

[3] Szegediné Lengyel Piroska: Élménypedagógia a virtuális térben, Selye János Egyetem „Társadalmi jelenségek és változások” II. Nemzetközi Tudományos Konferencia Tanulmánykötet, CD, Komárno, 2010

[4] Kovács László: Az információs terrorizmus eszköztára, ZMNE, On-line tudományos folyóirat, Különszám, 2006. november. ISSN 1788 1919 http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html (letöltés: 2010. április 07.)

[5] Szegediné Lengyel Piroska: Fiatalok a cyber-térben, Hadmérnök On-line tudományos folyóirat, V. évfolyam, 2. szám. 2010. június, ISSN 1788 1919 p.: 366-379

[6] Dr. Várhegyi István, Dr. Haig Zsolt, Dr. Kovács László: Információs műveletek, Multimédiás tananyag, CD-ROM, ZMNE, 2005

[7] Dr. Kovács László: Kritikus információs infrastruktúrák, ZMNE, Egyetemi jegyzet, CD, Budapest, 2007

[8] Dr. Kovács László: Kritikus információs infrastruktúrák, ZMNE, Multimédiás oktató program, CD, Budapest, 2007

[9] Kovács László, Krasznay Csaba: Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság, III. évfolyam. 1. szám. 2010. február ISSN 1789-5286 p.: 44-56.

[10] http://www.cbsnews.com/8301-504763_162-20018888-10391704.html

[11] http://www.lengyelpiroska.hu/elkonyv.html

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Vizi Pál Gábor
vizip@rmki.kfki.hu

MICRO AND NANO ROBOTS IN MILITARY, SPACE, SECURITY AND SAFETY TECHNOLOGY

Absztrakt / Abstract

A mérnöki technológia egyik legfontosabb és legérdekesebb kérdése a kisméretű és könnyű azaz mikro- és nanorobotok tervezése és megvalósítása különleges működési területekre. A cikk kitér néhány kisméretű automatikus robotra, roverre, űrszondára, a kutatásra és a megoldásokra, kezdve az oktatástól egészen a legújabb kihívásokig. A szerző áttekinti az eredményeket, a vizsgálati és kutatási módszerek helyét, szerepét, problematikáját a témakörben.

Designing and implementing smaller and lighter robots for special operating places e.g. micro and nano robots in military, space and safety technology is one of the very important and interesting questions of engineering technology. Subject of this article is about automated small robots, rovers and probes, research and solutions from training to new challenges. The author gives an overview about methods, results of checking up, the system of research works and problems in point of view of some problems of topic.

Kulcsszavak/Keywords: *mikro nano robot rover űrszonda műhold érzékelés környezetvédelem katasztrófa megelőzés ~ micro nano robot rover space-probe satellite sensing detecting environment saving disaster-prevention*

INTRODUCTION

Micro and nano robots in military, space, security and safety technology - is the title of my doctoral topic. In this article I review the topic and I briefly describe the results of the present world and availability of future. The article presents the news and ideas of my research, e.g. the “minimal plan” and its modularity.

It talks about expertise, knowledge management and about the education and teaching of young experts. It also reports about results and edification of the “Competition of the Hungarian Applied Engineering Sciences” “magyarokamarson”=magyarokamarson.hu[1] which becomes simply the popular name of competition.

I shortly talk about vacuum and climatic test of Hungarian MaSat-1 CubeSat program[2], which satellite is made from simple commercial parts and devices and developed only by Hungarians.

I introduce to you the Google Lunar X Prize (GLXP) [3] and the Hungarian GLXP team, which is an attempt to reach the goal and about its results and edification of brainstorming and new ideas.

Finally I summarize new trends of the future e.g. nano probes. I draw the attention to the newly evolved risks and dangers in military context e.g. terror from direction of space with relatively cheap solutions. There are the new challenges and applications which are significant part of NATO research in close connection to NASA and ESA.

INTRODUCTION INTO TOPIC

The research is about small sized robots, rovers, space probes, space robots which are suitable for military, space, and security/safety purposes.

The main advantages are the following: climatic observation, catastrophe prevention and preparedness, estimating agricultural production, prevent against agricultural insects on a lower cost and participate in the field of security observation in situ or from remote distance e.g. from space.

The minimization means to minimize the necessary - to reduce or keep it - to a minimum. Minimization is like Occam's razor, having no more than necessary.

The small size is nowadays a real reality. It is used by other ground technologies, not only by military and space technologies. In addition in space technology the old Space Shuttle program is in state of under final countdown, the main Constellation Program was cancelled at the beginning of 2010.

Small technologies are beneficial to reduce the cost. It is important to focus on new evolved dangers; low cost technologies are easily available for terroristic purposes.

SPECIAL MEANING OF MICRO AND NANO IN THIS TOPIC

Micro is used to name of one per million „micro-” μ 10−6 and nano means one per billion „nano-” n 10−9 in SI system. Meanings of original ancient Greek words are “small” and “dwarf”. Here, in this subject names are freely mixed together, SI meaning the original meaning. Therefore micro probes are sized near one cubic decimeter and nano robots are invisible to the naked eye. Significance of small devices are the small weight, cheap and wide accessibility for anyone. Typically uses nowadays ready small, cheap commercial off-the-shelf (COTS) electronics components. COTS is a term to define technology which is ready-made and available for sale, lease, or license to the general public. The term often refers to computer software or hardware systems and may also include free software with commercial support. COTS purchases are alternatives to in-house developments or one-off government-funded developments. COTS typically requires a configuration that is tailored for specific

uses. The use of COTS has been mandated across many government and business programs, as such products may offer significant savings in procurement, development, and maintenance. [4]

Furthermore there are lots of very cheap or cost free waste materials from demolition of computers, cars or device shops which are usable for sophisticated purposes. From those materials a few engineers are enough to make a brand new product based a brand new idea. During my research I was lucky because a few enthusiastic people made several good examples together and I can show them in this article.

SIGNIFICANCE OF SMALL SIZE AND MASS

The main advantage is: small devices can be delivered more easily to a destination; in space technology the main cost is to elevate the device into orbit. The major powers like the U.S., Russia and China today are no longer necessary to take a big effort to reach this goal. Only the price of a few family houses is enough for example to reach the Space e.g. the Danish commercial rocket plan. In addition their goal is to send humans into the space (see below).

Smaller devices can be navigating (accelerating and breaking) more easily and can hardly be recognized.

THE WORLD'S RESEARCH RECENT AND PRESENT RESULTS

Where is the research today in the world? Let us look around for sample data.

JAXA: Space Technology Demonstration Research Center 1998- Micro LabSat program started in 2002 and during 2004 they reduced the total mass to 50 kg. The Micro LabSat (Micro- OLIVe Experiment) program represented a complex mission that yielded target, approach, maneuver, and docking from relatively short distances in LEO orbits. Following this, the Micro LabSat program, this consisted of a microsatellite that flew on a piggyback mission. For more than thirty years Japan had spent considerable effort learning how to build bigger and more complex satellites; now, in line with technology and policy trends, it needed to learn how to also build small ones. What is clear at this stage is that with technology now opening up whole new vistas, the basic frame and mission descriptions below show that the idea of ever- smaller satellites has become increasingly institutionalized in Japan's government agencies. Micro LabSat 1 made that paradigm shift possible in the early 2000s. The stated purposes behind its development were to nurture younger engineers, acquire small satellite bus technology, and obtain high performance at low cost and short time frames. Seen by its makers as a first step toward spreading small satellite technology that was inexpensive and mass produced with commercial- off - the- shelf (COTS) components, it also helped spawn research and development (R&D) cooperation between NASDA, CRL, NAL, Toshiba, and the University of Tokyo. Micro LabSat 1 was merely a 70- by- 50- centimeter octagonal-shaped 50- kilogram microsatellite that flew in an 800- kilometer orbit. More remarkable than its dimensions was the fact that it helped demonstrate that Japan could equip its satellites with technologies for autonomous capabilities, something which is considered the most important and fundamental issue in space robotics.

The emphasis is on the low- cost, high- speed construction of highly functional satellites that can be used for disaster monitoring (or early warning), weather observation, and mobile communication.. [5]

Jet Propulsion Laboratory's (JPL) Microdevices Laboratory develops several different types of nano-scale electronic devices based on carbon nanotubes (CNT). CNT exhibit a coupling between electronic structure and mechanical deformations: mechanical stress or

deformation can result in charge injection into the nanotube, or likewise, charging of a nanotube can result in mechanical deformations. This electromechanical coupling can form the basis for nanotube-based oscillators, signal processors, and RF rectifiers. Nanotube electronic properties, specifically their resistance and current-voltage characteristic, can also change when various molecules bind to their surfaces. This property can form the basis for CNT-based chemical and molecular sensors. For both types of device, CNT are grown directly on silicon substrates in pre-patterned device structures: nanotubes grow by CVD from patterned arrays of particles of catalytic metals, with the pattern of the catalyst determining the pattern of CNT. [6] Chemical Vapor Deposition (CVD) is chemical reactions which transform gaseous molecules, called precursor, into a solid material, in the form of thin film or powder, on the surface of a substrate.

Micro/Nano Electro Mechanical Systems (MEMS/NEMS) technologies Centre for Micro and Nano Systems Aerospace Corporation, El Segundo, California works on nano-satellite prototypes intended to be used for Co-Orbital Satellite Assistance (COSA). COSAs are small daughter nanosatellites (<1kg) that can be used to assist in the maintenance of the mother satellite. The key design parameter is the ability to mass produce these satellites using batch processed micromachining technologies. Nanosatellite constellations will also enable new technologies such as ultra large virtual phase arrays for Space Based Radars (SBRs), low-cost remote sensing, and deep space sensor nodes. [7]

Akatsuki (Dawn), JAXA, 2010.05.20. a Japan mission to Venus. The total mass with the propellant was 480 kg, research payload is 34 kg. It missed orbiting Venus and now it is on hibernation phase for six years. After that they try again orbiting Venus next time when Venus will be reached and the two elliptical tracks will meet again. [8]

Robotic Ant European 7th Framework Program

“Small robots that are able to work together could explore the planet. We now know there is water and dust so all they would need is some sort of glue to start building structures, such as homes for human scientists,” says Marc Szymanski, a robotics researcher at the University of Karlsruhe in Germany.

Szymanski is part of a team of European researchers developing tiny autonomous robots that can co-operate to perform different tasks, much like termites, ants or bees forage collaboratively for food, build nests and work together for the greater good of the colony.

Working in the EU-funded I-SWARM project, the team created a 100-strong posse of centimetre-scale robots and made considerable progress toward building swarms of ant-sized micro-bots. Several of the researchers have since gone on to work on creating swarms of robots that are able to reconfigure themselves and assemble autonomously into larger robots in order to perform different tasks. Their work is being continued in the Symbrion (Symbiotic Evolutionary Robot Organisms) and Replicator projects that are funded under the EU’s Seventh Framework Programme.

Planet exploration and colonization are just some of a seemingly endless range of potential applications for robots that can work together, adjusting their duties depending on the obstacles they face, changes in their environment and the swarm’s needs.

“Robot swarms are particularly useful in situations where you need high redundancy. If one robot malfunctions or is damaged it does not cause the mission to fail because another robot simply steps in to fill its place,” Szymanski explains.

That is not only useful in space or in deep-water environments, but also while carrying out repairs inside machinery, cleaning up pollution or even carrying out tests and applying treatments inside the human body – just some of the potential applications envisioned for miniature robotics technology. [9]

Just a short sentence about MEMS (Micro Electro Mechanical Systems), EADS N.V. group, the European Aeronautic Defence and Space Company eads.net, [10]

There are several other useful solutions using micro and nano robots, for example in health care services and in military technology to spy or to destroy the enemy.

OUR LOCAL RESEARCH - NEW RESULTS AND IDEAS

We can show a part of the actual micro robot and probe research and developing possibilities in Hungary. Now we can report about Simulated Mars Rover Competition www.magyarokamarson.hu (Hungarians on Mars) [1], shortly about results of MaSat-1 (Hungarian Satellite 1) Vacuum and Climatic test [2], about Google Lunar X-Prize (GLXP) [3] Hungarian attempt where the group named Team Puli [11] and Hunveyor the Hungarian UNiversity surVEYOR [12] because Puli project became a part of Hunveyor research. I hope that we can tell good news - there are enough knowledge, motivation and young expert for this research and applied technologies.

Finally we look after some briefing about nano robots[13], because of the novelty we are talking especially about nano space robots.

COMPETITION “HUNGARIANS ON MARS”

We report about organization and management Simulated Mars Rover Competition www.magyarokamarson.hu (Hungarians on Mars) [1]. This is a competition of applied engineering sciences. We talk also about collected experience and results at place of tournament Kiskunhalas, II. Rákóczi Ferenc High School (2006-2010) and Hungary and Óbuda University (2010). Organizers of the competition are independent persons and organizations work together with High School and enthusiast sponsors. Founder of the competition is Mr. SIPOS, Attila electrical engineer.

What are our ideas? We do not get the knowledge together with life. To start young people to get more experience is one of the most important things nowadays.

What is our mission? The actual goal of the competition can be achieved by building a device, a rover. The field of competition is hidden from direct visibility. Competitors must use video transmission and remote control and the navigation must be delayed by 15 seconds to simulate time of spread of the signal. The jury works mainly automatically, only results are important, but there are experienced members in the jury and one of them is the author of this paper. The track is an 8x8 square meter sized field of sand or special material.

In 2006 competitors had to build a rover which starts from one corner of the field to reach the target crater at the opposite other corner and to collect debris or soil of the crater.

In 2007 Competitors had to search power cubes to collect energy across of field.

In 2008: Competitors had to collect fluid material placed on different positions across the square. [14]

The goal of the 2009 year competition had been achieved by building a device, an amphibian rover with sensors and advanced communication. The track was an 8x8 square meter sized field of water and simulated swimming ice mountains from expanded polystyrene foams above level of water with iron and lead feet. Competitors had to build an amphibian vehicle (rover) which starts from either corner of the pool (simulated shallow sea) to reach the target icy island at the opposite corner. During this mission they must save the crew of some disaster spaceships on small icebergs, simulated by small rubber balloons (yellow and orange). In the secondary high school category the best solution was an amphibian with a 4WD driven and air propeller aligned vehicle. They main plan was to achieve the correct position according to supported “satellite” picture which is set up above the track. The

absolute winner solution was an amphibian with full of sensors, well adjusted and absolutely light weighted. It has on board local "GPS" solution, position lights, navigation cameras and illumination for cameras. The control and correction was powerful. To prevent form drifting it was adjusted by software according to positioning system by gently rotating paddle- wheel and normal gear combination (mainly back). Accurate management was achieved by united information of sensors. Regulation of wheels was made by cooperation of onboard and remote computer from data of sensors with autonomous control.

Mission 2010: The main goal was to reach the target place and there to read and send back to base an DNA sequence represented by a 16 character display inside a model of a small creature. Additional goals were to collect "soil" specimen beneath a model of plant, and had to carry and put the specimen into the Mars space-harbor. At the space harbor there was a space-elevator model. Competitors had to use the elevator with their main robot or with a special elevator unit. At the top of the rod is the space station model. The end of mission was to reach the top of the space. [15]

Teams: For the past five years there were several teams, high school and university departments have been trying to complete missions. Some of them were effective and students were successfully started or have finished Ph.D. studies. Some of them: Budapest University of Technology and Economics (BME), Faculty of Informatics of University of Debrecen (UniDeb); Computer Science Department in Károly Eszterházy; Eötvös Lorand University (ELTE) Institute of Physics, Department of Material Physics. and other team member from Dept. Informatics; Pécs University - Dept. Informatics and G. Technology; Széchenyi István Technical High School, Székesfehérvár; Budapest Tech (BMF from 2010 Óbuda University) Dept. Faculty of Electrical Engineering; Zrínyi Miklós National Defense University (ZMNE) Engineer and Doctoral School of Military Sciences.

Prizes: Prizes are given by sponsors mainly cash and electronic or computer devices. The full price of the competition is about one million HUF is near 5000$. Media: You can find a lot of documentation and media across the internet first of all on the main website of magyarokamarson and for example the webpage of Hungarian Astronomical Society [16] and of course on youtube.com by author „siposattila" [17].

Cooperation: Since 2008 one of the Hunveyor group arrived to our competition. In addition during 2009 we were invited to Robot day Conference. From 2009 the competition became official competition of HAS (Hungarian Astronautical Society, abbreviated as MANT in Hungarian). In 2010 we were accepted at Robot Warfare Conference at ZMNE also.

Sponsors: (year by year and in alphabetic order):

2006.: Emitel Zrt., KFKI RMKI, KFKI RMKI, Rádiótechnika

2007.: Űrvilág.hu, Rádióvilág Ltd, Emitel Zrt, KFKI RMKI Space Technology, SGF Ltd.

2008.: ChipCAD, MCSE, NG project robotplato.hu, Rádiótechnika, SGF Ltd., SOS electronic

2009: ChipCAD, MANT, MCSE, Rádiótechnika, SGF Kft., Távir

2010: BL-Electronics, Bosh, ChipCAD, Compar'97, Diptrace, MANT, Rádiótechnika, SGF Ltd., GalileoWebcast

Conclusion of Competition "Hungarians on Mars": The evolution of simulated mars rover model competition has grown up and reached the goal to train new experts. They can connect to works of Universities. We are continuously working to organize and manage next competitions with new goals. The cooperation is also growing between organizers and high schools, universities and doctoral schools. The results show that small and light devices are suitable for wide-ranging tasks, which meet the requirements for military, aerospace tasks and for security market.

MASAT-1 CUBESAT

A CubeSat is a type of miniaturized satellite for space research that usually has a volume of exactly one liter (10 cm cube), weighs no more than 1.33 kilogram and typically uses commercial off-the-shelf electronics components.

With the aim of introducing spaceborne circuit design to undergraduate students, as well as to train a sufficient number of space specialists, thus facilitating future selection processes for spaceborne developments, two departments of the Budapest University of Technology and Economics decided to jointly launch a long-term educational program in the field of spaceborne circuit development.

These two departments are the Department of Broadband Infocommunications and the Electromagnetic Theory and Department of Electron Devices

They defined the mission criteria in degrees of success.

Minimum success is to design, build and test a satellite which can survive the launch process and the environment in space. To deliver a fully tested satellite to the launch site and get a successfully released acknowledgement from the launch vehicle. Ground Station must be operating reliably 24/7.

Intermediate success is to successfully receive telemetry packets from the satellite and to control the satellite operation modes via telecommands. It is acceptable a correct and reliable operation of all satellite subsystems.

In case of full mission success satellite must be operated reliably 3 weeks after launch and must be received all of scientific data and telemetry of the satellite. [18]

My job was to help the MaSat-1 group during test. We have started the preparations for the termo-vacuum test on 14th July 2010 at KFKI RMKI (Research Institute for Particle and Nuclear Physics). During the measurements, we examined the temperature behavior of the satellite at several temperatures and in high vacuum. We tested it about proper work in the extreme environmental condition. The measurements lasted for two weeks with permanent 24 hours supervision. Results were accepted to have furthermore investigations. [19]

THE GLXP COMPETITION AND THE HUNGARIAN TEAM PULI

The Google Lunar X PRIZE is a $30 million competition for the first privately funded team to send a robot to the moon, travel 500 meters and transmit video, images and data back to the Earth. [3]

Team Puli Space is a Hungarian attempt to reach the goal of GLXP. The group is a private initiative with collaboration of scientific research places, like universities and research institutes. [11]

The aim is to demonstrate abilities of team by landing a self-made probe on the Moon by 2014 and thus complete the Google Lunar X PRIZE challenge. Puli Moon probe - according to plan - will ascend to orbit with the help of a commercially available rocket and journey on its own to land on the lunar surface, explore the nearby area and send high quality imagery and video recordings of its surroundings and itself back to Earth. The project requires the setting up of a functional mission design, researching the necessary components, building a functional module and finally managing its mission to space.

Based on the GLXP experience, independent of the result, they intend to become a player in the growing space industry.

Puli Space also considers it a top priority to promote scientific thinking and to encourage students in choosing a career in sciences.

PULI Space Technologies Ltd has been inaugurated, as an official and functioning company. Headquarters are currently being set up in Budapest, Hungary, which will probably become Puli central soon. Various other legal matters has been taken care of, like bank accounts, tax IDs, non disclosure agreements, organizational and operational regulations and so on. These steps ensure that Team Puli is backed by a legal entity which can appropriately handle funds, pay tax and generally represent the team in business.

Puli's letter of Intent sent to GLXP, it is a positive acknowledgement of intent to take part in the competition. Although this does not yet mean that Puli team is fully registered, the required entry fee of 50 000 USD and complete the registration process the team can call themselves a fully registered team. [11]

THE 'MINIMAL PLAN'

The part of my research is the "Minimal Plan", which is the smallest, lightest and cheapest solution to reach the goal.

The most expensive part of the project must be minimized which is to overcome the Earth's gravity and to reach the orbit. The lightest is the cheapest because of smaller energy demand. In addition when we are light enough, it is possible to become a secondary payload (or in other word piggy-back mission) on another scientific or commercial rocket and application forms can be found to reach secondary payload possibilities. In this case the orbital price is around one percent – Masat-1 will achieve its orbit similarly like other cube satellites.

If we can make a secondary payload, in this case maybe new possibilities will be available. Investors can buy parts of mission for different purposes like business, research or simply to build a monument in memory of themselves.

THE 'MODULAR MINIMAL PLAN'

The "Minimal Plan" must be modular, must be easily expanded. In other words, if a project can collect more money or resources then new parts must be merging into the original design to achieve the extended goal.

First of all the minimal design is the smallest, lightest and cheapest solution to reach the goal, but must be expandable. For a very simple example: if we couldn't supply enough power of rocket to hold an accumulator into the probe beside solar cells originally, then when it will be available there must be a spare place to install, to put there that accumulator.

Evolution of plan can grove in two directions like expanding or multiplying or both together.

Let we see some example about minimal design. To move on the surface of the Moon there is a completely new idea named SunChariot rover, a ball surface with lots of empty sausages which looks like a hedgehog or jumping puli, a spiny ball. The ball is the best wheel which can not be overturned. The ball is a closed unit. If this SunChariot landing on the Moon at dawn then one surface is in shadow and sausages are shriveled flaccid at near absolute zero degree; other side heated by Sun and here are sausages inflating the ball. The final result is a rotation to the shadow direction. This is a minimal design but expandable, because inside there is spare place where we can install solar cells, motor and if necessary accumulators also. The condition of expanding is the power of rocket to orbit. If we haven't enough power to lift up our payload from earth, then lightest solution must be use. But if we have enough power then skill of rover can be improved by adding solar cells, motor and accumulator.

In keywords from minimal to expand some skills are SunChariot or center of gravity moving motor or torque motor; one camera or more 3D cameras; competition to receiving our signals (together with amateurs) or own space communication system. The minimal launch

plan is to become a secondary payload. Expanded plan for launch to collect others to start together. Maximized plan is to make a big enterprise to send a complete probe fleet. Probes are for different purposes, like climate and weather observation, disaster prevention and protection. Whit this idea plan is modular from 'minimal plan' to expandable one.

In this article, I do not want to elaborate in detail the well-known disciplines about reaching the Moon, like orbits, because those are well documented.

I just want to tell only one sentence about a smooth landing facility with a combined orbit modifier and landing braking rocket and airbags because they are similar to landing of Spirit and Opportunity Mars rovers. The braking rockets are on edges of a tetrahedron shaped body and the rover is inside an airbag hanging on a soft wire from tetrahedron.

SIMULATIONS

All of our designs are planned to estimate in virtual software simulations. Most simulation can be achieved by commercial off-the-shelf software and some are usable free of charge. Like Linux, Open Systems, Open (Oxygen) Office, Open Office, Google Sketchup: 3D static, Sketchy Physics, Orbiter the free spaceship simulator, Celestia astronomical simulator; CAD/CAM programs, and educational software. Microsoft operating systems and office programs for Hungarian universities, students and research institutes are available for free according to an agreement between Microsoft and Hungarian Government for learning, educating and researching purposes. [20]

IF YOU DO NOT HAVE ENOUGH MONEY TO BUILD ONE, WHY DO YOU NOT BUILD TWO OR MORE

How can a project collect enough money? If you haven't enough money to build one, let you build two or more. Several useful purposes are available to use benefits of modern micro and nano probes nowadays.

Environmental protection, disaster prevention, climate monitoring, pest and crop estimation for beneficial commodity are exchange appearance. Investors can get out extra profit when discovered in time.

Grenerczy, Gy., U. Wegmüller, Persistent Scatterer Interferometry analysis of the embankment failure of a red mud reservoir using ENVISAT ASAR data, Geophysiscal Research Letters, submitted, 2010GL046184

A red mud reservoir failed and alkaline torrential sludge flooded three settlements. As we were aware of the fact that we have a unique satellite technique that could reveal the past stability and motion history of the broken reservoir, we shifted our resources and requested SAR scenes of the area from ESA. Images were granted outside CAT-1 and we performed a prompt PSI study to contribute to the better understanding of the disaster and more importantly to see if it was possible to prognosticate and consequently prevent this disaster and similarly to avoid such occurrences worldwide in the future.

We investigate the stability and motion history of a red mud reservoir and provide an example of significantly increasing the chance of forecasting a disaster and highlighting the need for deformation monitoring even back to the past with the unique feature of Persistent Scatterer Interferometry.

It is important to present a disaster important to timely be presented to the community of earth scientists and engineers especially to geodesists and structural engineers and field geologists. Prompt information dissemination is also needed to make them aware the factors led to the disaster and make them as sets the status of all reservoirs worldwide. We highlight the risks and most importantly present a unique space based tool that may help in disaster prevention.[21]

Nowadays, until now micro probes were only rarely used for disaster prevention but it will change in the future if we can supply a solution with a national fleet of micro probes.

WHO CAN MAKE THESE MICRO OR NANO SPACE PROBES?

Currently operating research institutes, universities and private technology centers like intentionally founded firms, limited companies, foundations, corporations and consortiums can make these micro or nano space probes. Enthusiastic students and researchers, engineers, managers, investors etc. all together can make efforts to aim the chosen goal. Students can make scientific papers, student research works, independent labs, MSc thesis and PhD research. Lawyers are connected to project to supply the legal background. Media specialists make the necessary PR and marketing mission.

We can report some running research projects, like Hunveyor (see below) and project magyarokamarson (see above).

Present time around 40 enthusiasts are working on the Puli project in Team Puli on different levels, from supporter rookies to hard core members, owners, like technicians, BSc, MSc and PhD degree level managers. Functions are divided into two main parts like "Organization and Business" and "Engineering and Science".

Puli Team earned collaborations with Faculty of Electrical Engineering of Óbuda University, Zrínyi Miklós National Defence University (ZMNE), Hunspace Hungarian Space Cluster, www.magyarokamarson.hu project, ELTE TTK Hunveyor project which gave for Team Puli the Hunveyor registration number 15. Puli Team modestly supported the 51 years old MANT (HAS - Hungarian Astronautical Society, abbreviated as MANT in Hungarian)

Several private persons supported the team and the support is available for firms also, which is a significant specialty of modern recently started space activity and industry, which is the inescapable trend of future.

PULI SPACE TEAM GOT A NEW POSSIBILITY TO EXPAND ITS FEATURES

At Eötvös Loránd University Faculty of Science (ELTE TTK) on base of NASA 1966-1968 Surveyor-program have founded a Hungarian UNiversity surVEYOR [12] practicing space probe model program. They started a teaching program based on original Surveyor concept [22] which has simple, clear structure, easy programmable instruments as a good sample to build experimental practice space probes for students.

First, two Hungarian universities were in competition in developing new instrument-assemblages on their planetary lander type robot, Hunveyor-1 & -2. Both groups built new instrumentation, of which we report

a) the Hunveyor-1 result of developing a spectrometer, thermometer, drill unit,

b) the Hunveyor-2 result of chemical optic-chemical sensor unit,

c) Hunveyor-1 Martian desert landscape,

d) beginning the Hunveyor type lander construction in a high school in Pécs.

Hunveyor experimental university minimal probe was first constructed to the 1998 LPSC [1] on the Eötvös University, Budapest, (Dept. G. Technology). Next year the same Eötvös University group prepared a rover and internet availability. Also in 1999 we made planetary geology park around Hunveyor-1.

They continued developing instrument assemblage supporting their planetary lander type robots Hunveyor -1 and others.

The program not only develops experimental practice with instruments and robotics but makes enthusiastic planetary geology education of students and makes possible studying a simulated planetary terrain. Over these benefits the program in the future may help to design

new instrumentation, trigger initiatives, and make the possibility to realize ideas. Help in keeping fresh the enthusiasm, constructive activity of students in natural sciences. Help selection of new constructional units and measurements and help forming international university community working together on planetary science [23]

WHERE ARE NOW THE OTHER PRIVATE SPACE (GLXP) TEAMS?

Registered Roman team named ARCA Aeronautics and Cosmonautics Romanian Association (ARCA) is a non-governmental organization, which promotes innovative aerospace projects. Organization's main objectives are to win the Google Lunar X Prize Competition and to send in space the first Romanian rocket. [24]

Danish commercial rocket: a private Danish rocket built by volunteers to launch one person into suborbital space is now slated to launch with a dummy pilot riding aboard. [25] They successfully tested they HEAT 1XP rocket on 2010.05.16. [26][27]

Spanish GLXP group Frednet [28] makes a ball rover which is similar to one of plan of Hungarian Team Puli.

More American teams are in GLXP competition.

THREATS AND CHALLENGES

We must pay attention about newly raised dangers in military context, namely the terror from space.

Because if small private groups all around the world are capable to make powerful and successful space devices, rockets and probes, then similar aggressive devices could be made by other parties and the danger is real and gave a big challenge to avoid from Improvised Space Terror Devices (ISTD). ISTD-s are maybe capable to make dangerous space debris or maybe can pass bombs to anywhere on the Earth.

CONCLUSION

In this article I showed the topic and I briefly described the results of the present world and the availability. I presented the news and ideas of my research, like the “minimal plan” and its modularity.

I talked about expertise, knowledge management and about the education and teaching of young experts and I also reported about results and edification of the “Competition of the Hungarian Applied Engineering Sciences” www.magyarokamarson.hu

I shortly talked about vacuum and climatic test of Hungarian Masat-1 CubeSat program which satellite made from simple commercial parts and devices and developed only by Hungarians and successfully passed all tests.

I have introduced to you the Google Lunar X Prize (GLXP) and the Hungarian GLXP team about attempt to reach the goal and its results and edification of brainstorming and new ideas and about other teams from the World.

At last I summarized new trends of the future. I drew the attention to the newly evolved risks and dangers in military context like terror from direction of space. There are the new challenges and applications which are significant part of NATO research in close connection to NASA and ESA. If small private groups all around the world are capable to make powerful and successful space devices, rockets and probes, then similar aggressive devices could be made by other parties and the danger is real and gave a big challenge to avoid from Improvised Space Terror Devices (ISTD). ISTDs are maybe capable to make dangerous space debris or maybe can pass bombs to anywhere on the Earth.

REFERENCES

1 Sipos Attila: Hungarian Applied Engineering Sciences (Magyar Alkalmazott Mérnöki Tudományok Versenye) magyarokamarson.hu – www.magyarokamarson.hu (2011.01.04)

2 MaSat-1group: MaSat-1 program - http://cubesat.bme.hu/masat-1/?lang=en (2011.01.04.)

3 Google Lunar X PRIZE - http://www.googlelunarxprize.org/lunar/about-the-prize (2011.01.04.)

4 Commercial, off-the-shelf (COTS) - http://en.wikipedia.org/wiki/Commercial_off-the-shelf (2011.01.04.)

5 Saadia M. Pekkanen, Paul Kallender-Umezu: In Defense of Japan, From the Market to the Military in Space Policy. Stanford University Press, 2010.

6 Michael J. Bronikowski [et. al.]: Carbon Nanotubes for Molecular Sensors and Electronic Circuit Elements www.engineerscouncil.org/Conference/2004/Abstracts.doc (2011.01.04.)

7 Po-Hao Adam Huang: Activities and CV http://ho.seas.ucla.edu/members/Adam_CV.pdf (2011.01.04.)

8 Akatsuki (probe) http://en.wikipedia.org/wiki/Akatsuki_(probe) (2011.01.04.)

9 Robotic ants building homes on Mars? – Physorg.com http://www.physorg.com/news143815934.html (2011.01.04.)

10 EADS N.V. group, the European Aeronautic Defence and Space Company http://www.eads-nv.com (2011.01.04.)

11 Hungarian GLXP attempt named Puli Space www.pulispace.com (2011.01.04.)

12 Hunveyor: Hungarian University Surveyor program http://hu.wikipedia.org/wiki/Hunveyor (2011.01.04.)

13 Nanorobotics http://en.wikipedia.org/wiki/Nanorobotics (2011.01.04.)

14 SIPOS, Attila, VIZI, Pál Gábor: Simulated Mars Rover Modell Competition www.lpi.usra.edu/meetings/lpsc2009/pdf/2519.pdf (2011.01.04.)

15 SIPOS, Attila, VIZI, Pál Gábor: Simulated Mars Rover Modell Competition www.lpi.usra.edu/meetings/lpsc2010/pdf/2649.pdf (2011.01.04.)

16 Polaris TV: Summary of Hungarians on Mars Competition (magyarokamarson.hu) http://www.mcse.hu/index.php?option=com_mediatar&task=show&archID=0473&Itemid=338 (2011.01.04.)

17 SIPOS, Attila: Chanel of 'siposattila' - http://www.youtube.com/user/siposattila#p/a (2011.01.04.)

18 Students of the Technical University of Budapest (BME): Masat-1 - The first indigenous Hungarian satellite http://cubesat.bme.hu/masat-1/?lang=en (2011.01.04.)

19 Masat-1 Thermal vacuum test at RMKI http://cubesat.bme.hu/?lang=en (2011.01.04.)

20 P.G. Vizi: Puli Space Concept Video http://www.youtube.com/user/TheUserAZ09 (2011.01.04.)

21 GRENERCZY, Gyula : Introduction of the Differential Synthetic Aperture Radar Interferometry technique in Hungary: Monitoring Land Subsidence with SAR Interferometry and GPS Arrays -http://eopi.esa.int/esa/esa?toprint=-1&id=20700&caller=%252Fesa%252Fesa%253FtopSelectedNavigationNodeId%253DLOGIN%2526sideNavigationType%253DPI%2526piid%253D3140%2526ts%253D1289732774869%2526cmd%253Dpi%2526page%253D1%2526topNavigationDisabled%2

53Dtrue&cmd=project&token=&correspondentid=-1&role=0&header=&topSelectedNavigationNodeId=LOGIN&ts=1289732774869&type=40&sideNavigationType=PI&coordinates=&personid=-1&topNavigationDisabled=true&addattribute=false (2011.01.04.)
22 NASA Surveyor Program http://en.wikipedia.org/wiki/Surveyor_Program (2011.01.04.)
23 Diósy, T. [et. al.]: Hunveyor-1 & -2: Experimental University Lander Developments on the Eötvös (Budapest, Hungary) and JPTE (Pécs, Hungary) Universities in Hungary: New Instrument Assemblages - http://www.lpi.usra.edu/meetings/lpsc2000/pdf/1153.pdf
24 Aeronautics and Cosmonautics Romanian Association (ARCA) https://www.arcaspace.com/ (2011.01.04.)
25 Jeremy Hsu: Private Danish Rocket Aims for Sunday Launch www.space.com/missionlaunches/private-danish-rocket-suborbital-launch-update-100830.html (2010.08.30.)
26 Copenhagen Suborbitals: http://www.copenhagensuborbitals.com/boosters.php
27HEAT 1XP static booster test 16 May 2010 http://www.youtube.com/watch?v=7YX-WzUMGZI
28 Team Frednet concept videos http://wn.com/TeamFrednet

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Bottyán Zsolt
bottyan.zsolt@zmne.hu

Szabadi Vilmos
szabadiv@gmail.com

A METEOROLÓGIAI LÁTÁSTÁVOLSÁG ÉRTÉKÉNEK MEGBÍZHATÓSÁGI VIZSGÁLATA A MAYGAR HONVÉDSÉG ÖSSZHADERŐNEMI PARANCSNOKSÁG HELIKOPTER-SZIMULÁTORÁBAN

Absztrakt

A katonai repülő-hajózó állomány kiképzésében fontos eszköz a MH. ÖHP. helikopter-szimulátora. A szimulátor fejlett meteorológiai alrendszerrel és vizualizációval rendelkezik. Munkánkban a szimulátornak inputként megadott és az általa megjelenített, virtuális repülőtéri környezetben (LHBP) észlelhető meteorológiai látástávolság értékeit hasonlítottuk össze. Az 5000 m-nél kisebb látástávolságokat vizsgálva megállapíthattuk, hogy a szimulátor vizualizációs alrendszerének megadott 3000 m körüli értékek esetén a megjelenített látástávolság csak néhány száz méternél kevesebbel tér el a valóságtól, de 1000 m alatt ez az eltérés kevesebb, mint 200 m. A vizsgált helikopter-szimulátor tehát a fentebb említett pontosságon belül realisztikusnak tekinthető a látástávolság reprezentáció terén.

The helicopter simulator of HDF JFC plays an important role in the military pilot training. The above mentioned simulator has the advanced meteorological and visualisation subsystem. In our work we compared the virtual visualised and the given horizontal visibilities in an artificial airport environment (LHBP). We appointed – in case of the visibility lower than 5000 m – around 3000 m visibility values the difference between visualised and given visibility lower than a few hundred meters but the mentioned difference less than 200 m if the given visibility values were below 1000 m. In the bases of our investigation we can reveals the helicopter simulator can well produce the realistic horizontal visibility inside its virtual airport (LHBP) environment.

Kulcsszavak: *hajózó képzés, helikopter-szimulátor, meteorológiai látástávolság ~ pilot training, helicopter simulator, meteorological visibility*

BEVEZETÉS

Napjainkban a repülő-hajózó személyzet felkészítésében a földi repülésgyakorló eszközök alkalmazása elengedhetetlen. A magyar katonai légijármű-vezetők hazai kiképzését az NFTC programon belül a Magyar Honvédség Összhaderőnemi Parancsnokság, Repülő Felkészítési Osztálya (MH. ÖHP. RFO.) koordinálja és végzi, más intézmények oktatóinak bevonásával. A földi képzés egyik igen fontos eszköze a 2008-ban átadott ROBINSON 2244/IR FNPT I. helikopter-szimulátor rendszer. Az említett szimulátorban a növendékek közel 100 órát dolgoznak, mielőtt megkezdenék a valós repülési feladatok végrehajtását.

A szimulátorban a helikopter és a valóságos repülési környezet modellezése történik, melyben nagy szerepet játszik a meteorológiai feltételek kialakítása, megjelenítése (*Rolfe és Staples, 1988*). Ezt a feladatot a helikopter-szimulátor meteorológiai alrendszere végzi, mely csatolva van a helikopter-modellhez és a vizualizációs alrendszerhez egyaránt (*Bottyán, 2009*). A repülési időjárás állapotának leírásához az egyik legfontosabb paraméter a meteorológiai (horizontális) látástávolság, melyet a valóságban a szakképzett észlelő határoz meg a repülőtéren a meteorológiai észlelések rendjéről szóló szabályzat alapján, vizuálisan (vannak ún. látástávolság mérő automata berendezések is, de az általuk mért adatokat nem tekinthetjük reprezentatívnak a repülőtérre vonatkozóan több ok miatt). A meteorológiai látástávolság meghatározása körkörösen elhelyezkedő, ismert távolságú tereptárgyak láthatóságán alapul.

A meteorológiai látástávolság pontos ismerete egy repülőtéren elengedhetetlenül fontos, hiszen VFR (látva repülés szabályai szerint történő) repülések során a repülőtér végső megközelítését, a látvány alapján történő pozíció-meghatározás alapján végzik, de IFR (műszeres repülés szabályai szerint történő) feladat végrehajtás esetén is - az elhatározási magasságban - szükség van a futópálya szemmel történő azonosítására a biztonságos leszálláshoz. Természetesen a helikopter-szimulátorokban is szükség van a meteorológiai látástávolság pontos értékének megfelelő vizualizációra, a valósághű környezeti modell kialakítása érdekében (*Bottyán, 2009*).

Munkánkban bemutatjuk a fentebb említett helikopter-szimulátorban végzett látástávolságra vonatkozó vizsgálataink eredményét.

A METEOROLÓGIAI LÁTÁSTÁVOLSÁG ELMÉLETI MEGKÖZELÍTÉSE

A meteorológiai látástávolság az a legnagyobb vízszintes távolság, melyről egy megfelelően nagy, a horizonton lévő, meghatározott jellemzőkkel rendelkező, abszolút fekete tárgy még látható és azonosítható (*Johnson, 1954*). A látástávolság értéke függ:

- az észlelő és a tárgy közötti levegő optikai tulajdonságaitól,
- az észlelő szemének érzékenységétől,
- a tárgy és a háttár között kialakult kontraszttól.

A Koschmieder-formula szerint a meteorológiai látástávolság értékét a következőképpen határozhatjuk meg (*Bullrich, 1964*):

$$V = \frac{3{,}912}{(\sigma_R + \sigma_M)}$$

ahol, **V** [m] a látástávolság értéke, σ_R [m^{-1}] levegő molekulái által és σ_M [m^{-1}] az aeroszol részecskék által okozott extinkció értéke. A teljesen tiszta (aeroszol-mentes) légkör extinkciós együtthatóját könnyen számíthatjuk az alábbi összefüggésből (*Johnson, 1954*):

$$\sigma_R = \frac{32\pi^3 (m-1)^2}{3N\lambda^4}$$

ahol, **m** a tiszta levegő törésmutatója, **N** az 1 cm^3-ben lévő molekulák száma, λ [m] a fény hullámhossza. Ha a légkör nem tartalmazna aeroszol részecskéket, a formulával kapott elméleti látástávolság abszolút fekete test esetén 335 km lenne (tisztán Rayleigh szórás)! A valóságban ennél jóval kisebb értékeket tapasztalunk, mert az atmoszféra a valóságban jelentős számban tartalmaz aeroszol részecskéket.

Tekintve, hogy az aeroszol részecskéken történő szóródás (Mie szórás) meghatározása lényegesen bonyolultabb, ezért munkánkban erre nem térünk ki. A műszeres látástávolság-mérő berendezések egy fényforrás intenzitásának egy adott távolságon (kb. 0,5 – 0,8 m) történő gyengülésének mértékéből határozzák meg a $\sigma_R + \sigma_M$ értéket, melyből a Koschmieder-formula alapján, a meteorológiai látástávolság meghatározható az átvilágított légrészre vonatkozóan. A légkörben azonban az aeroszol koncentrációjának és típusának eloszlása rendkívül inhomogén, így a pl. egy repülőtér esetén a domináns látástávolság meghatározását – az esetek döntő többségében – nem lehet műszeresen meghatározni! Ezért történik a meteorológiai látástávolság meghatározása a bevezetőben leírt módon.

A ROBINSON 2244/IR FNPT I. HELIKOPTER-SZIMULÁTOR ÉS A LÁTÁSTÁVOLSÁG ÉRTÉKEK BEÁLLÍTÁSA

A helikopter-szimulátorok installálásának általános szabályai szerint, egy megfelelően elsötétített helyiségben került elhelyezésre a helikopter-szimulátor minden fontosabb eleme (*1. ábra*). A rendszer csaknem teljes körű repülési élményt biztosít, egyetlen hiányossága a teljes helikopter-szimulátorokhoz viszonyítva, hogy nem rendelkezik hidraulikus kabin-mozgatórendszerrel, amely a pilóták egyensúlyérzékére is hatást gyakorolhat. Szoftveres alapja a Microsoft Flight Simulator 2004 módosított verziója, amely rendelkezik a nagyobb magyarországi repülőterek nagy felbontású háromdimenziós virtuális modelljével. A szimulátorban lehetőség van repülési és navigációs eljárások, valamint rádióközlemények végrehajtásának gyakorlására is.

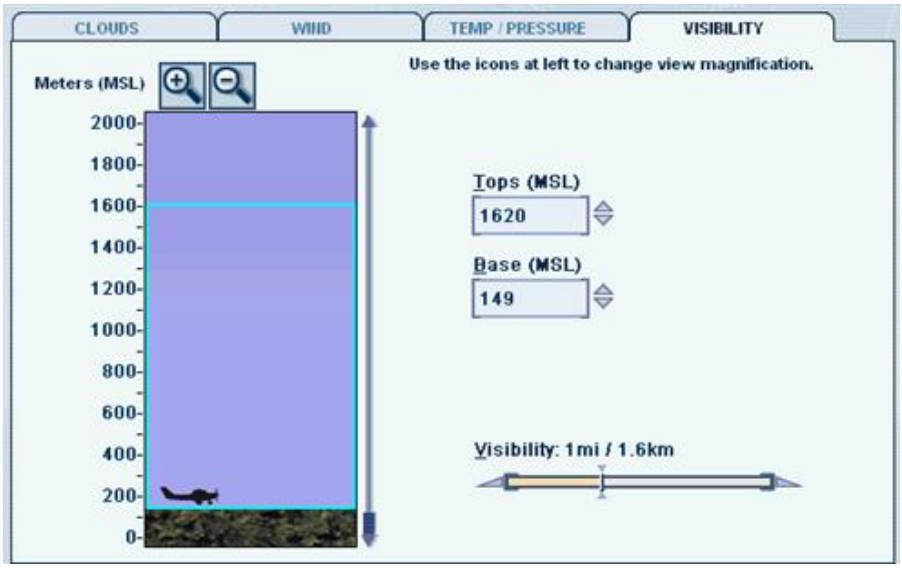


1. ábra. A ROBINSON 2244/IR FNPT I. helikopter-szimulátor átnézeti képe.

A rendszer elhelyezésének, és nagy megjelenítő felületének a célja, hogy a pilóták látóterét minél teljesebben kitöltse, ezáltal növelve a szimuláció valósághűségét. Három video-projektor a pilótakabin előtt-mellett lévő három vászonra vetíti az oktatói vezérlőrendszer számítógépein futó program által alkotott képet, így a látóteret vízszintesen 180°-ban függőlegesen 60°-ban tölti ki (*1. ábra*). Az így kapott, és a repülési helyzet függvényében változó vizualizáció folyamatos, és nagy pontosságú.

Az adott repülésre vonatkozó légköri adatokat, mint a hőmérséklet, szél, felhőzet, turbulencia, jegesedés, látástávolság, légnyomás és csapadék értékeit, a Microsoft Flight Simulator program e célra létrehozott grafikus adatbeviteli felületén lehet inputként megadni. Egy specifikus időjárási központra viszonyítva felvihető egy korlátlan számú, különböző tulajdonságú rétegekből álló vertikális légköri profil (*Williams, 2006; van West és Lee-Cummings, 2007*). A rétegek határai egészen az 50000 m-es maximális tengerszint feletti magasságig 20 m-es függőleges pontossággal meghatározhatóak, meteorológiai tulajdonságaik tetszés szerint alakíthatóak.

A megadható – jelenleg csak minden irányban megegyező – meteorológiai látástávolsággal jellemezhető réteg alsó (base) és felső (tops) határának tengerszint feletti magassága (MSL) tetszőlegesen beállítható. Az adott rétegre jellemző látástávolság értéke egy csúszkával választható meg a következő lehetőségek közül: 100m, 200m, 400m, 800m, 1200m, 1600m, 3200m, 4800m, 8km, 16km, 32km, 48km, 64km, 80km és korlátlan (unlimited) (*2. ábra*). A felsorolt (beállítható) látástávolság értékek jól igazodnak a repülésben alkalmazott fontosabb határértékekhez pl. 5000m, 3000m, 1500m, 800m, mely értékek bekövetkezése esetén a repülőtéri meteorológiai szolgálat ún. SPECI táviratot is köteles kiadni, figyelmeztetve a hajózó személyzetet a szignifikáns határérték átlépésére. Természetesen lehetőség van több repülési szintre vonatkozóan is megadni a látástávolság aktuális értékét, ami a felhőzetben kialakuló látástávolság szimulációjára szolgál (pl. numerikus időjárás előrejelzési produktumok adatai alapján).



2. ábra. A meteorológiai látástávolság (visibility) értékének repülési szintek szerinti beállításának lehetősége a helikopter-szimulátor adatbeviteli felületén.

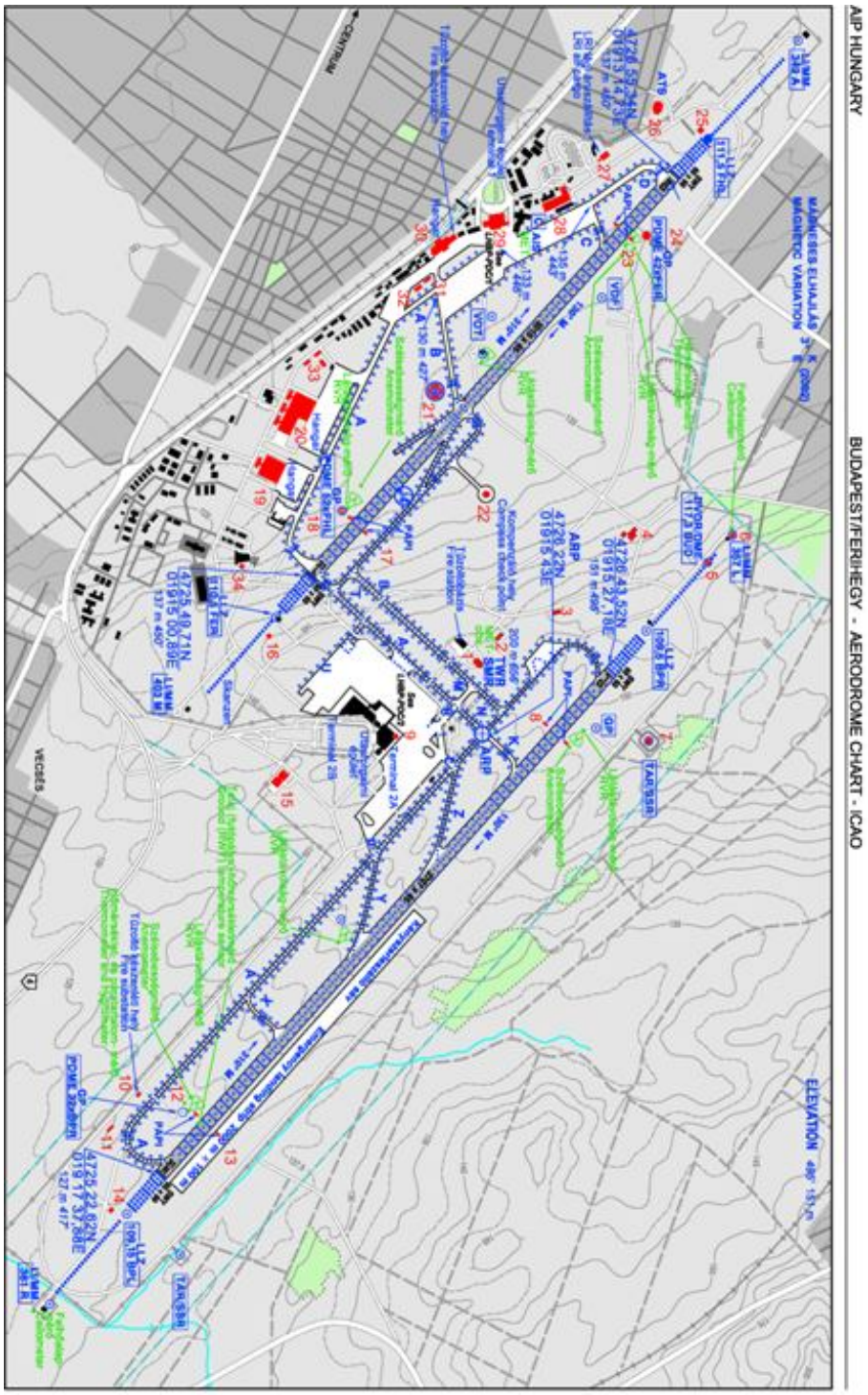
A HELIKOPTER-SZIMULÁTOR LÁTÁSTÁVOLSÁG-VIZUALIZÁCIÓ MEGBÍZHATÓSÁGI VIZSGÁLATÁNAK MÓDSZERE

A helikopter-szimulátor légköri környezet-modelljének megjelenítési pontosságát csak az 5000 m alatti látástávolság értékek esetén vizsgáltuk, hiszen ha a megjelenítés pontossága ebben az intervallumban elfogadható és állandó, akkor feltételezhető a pontosság megtartása a nagyobb látástávolságok esetén is. A szimulátor által megjelenített látástávolság felméréséhez olyan, jól látható, a vizualizációs alrendszer által megjelenített háromdimenziós objektumokra van szükségünk, melyeknek pontos helyzete, és a megfigyelőtől való távolsága ismert, vagy mérhető.

A vizsgálat helyszínként felhasználtuk Budapest Ferihegy (LHBP) nemzetközi repülőtér háromdimenziós modelljét, amely a legrészletesebb vizuális kidolgozottsággal rendelkezik a szimulátorba illesztett magyarországi repülőterek közül. A látástávolság meghatározásának korábban említett módszerének megfelelően, a valóságnak megfelelő helyen elhelyezett, jól felismerhető, háromdimenziós objektumok azonosítására volt szükség a virtuális repülőtér-modellen. Ehhez felhasználtuk az ICAO (International Civil Aviation Organisation) szabvány alapján készített, a Ferihegy (LHBP) repülőteret ábrázoló felszíni térképet, amely a Magyar Légiforgalmi Tájékoztató Kiadványban (AIP HUNGARY – Aeronautical Information Publication) megtalálható. A szimulátorral a virtuális repülőtér-modell felett „felderítő repülést” végeztünk, melynek során a sikeresen azonosított objektumokat a mellékelt térképen piros színnel kiemeltük és sorszámmal láttuk el (3. ábra). A tereptárgyak kiválasztásánál figyelemmel kellett lennünk arra, hogy az 5000 m alatti távolságok esetén – a korábban említett ún. beállítható látástávolságok – jól reprezentáltak legyenek.

Ahhoz, hogy a meteorológiai adatbeviteli felületen beállítható látástávolság értékeket egzakt módon felmérhessük, szükségünk volt az azonosított objektumoktól számított és a korábbi értékeknek megfelelő mérési pozíciókra. A megfigyelési pontoknak a szimulált helikopterrel való leszállásra is alkalmasnak kellett lenniük. Ehhez a repülőtér olyan

nevezetes pontjait jelöltük ki, mint a futópálya-küszöb pontok (13L, 13R, 31L, 31R,) és az ARP (Airport Reference Point).



3. ábra. A Ferihegyi repülőtér digitális modelljében azonosított tereptárgyak jelölése az AIP térképén.

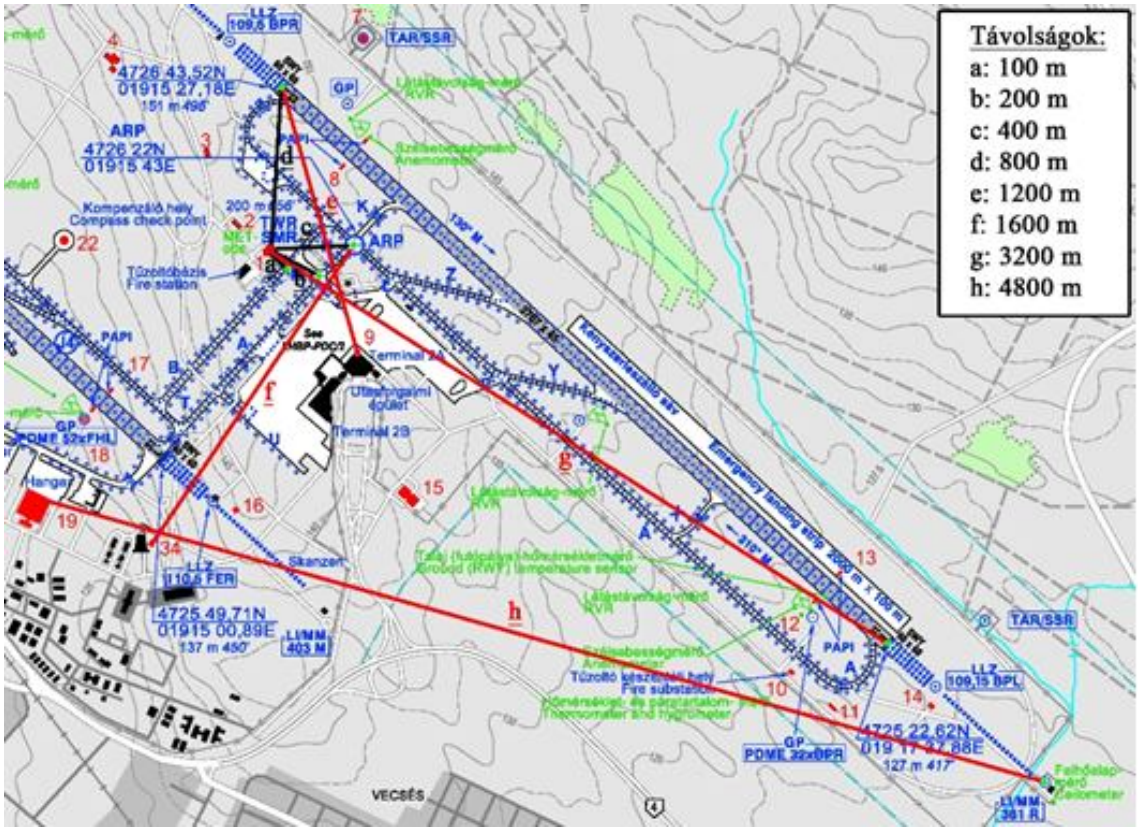
Ezután a Ferihegyi repülőteret ábrázoló AIP térképen felmértük az azonosított objektumok és a megfigyelési pontok valós távolságát a futópálya-küszöbtől illetve az ARP-től egyaránt (1. táblázat).

Sorszám	Objektum megnevezése	Megfigyelési pontok, távolságuk (m)				
		13L	13R	31L	31R	ARP
1	Irányító torony (TWR)	800	3000	1050	3200	400
2	Met-obs	662	2800	1100	3600	550
3	Épület	475	2575	1400	3875	800
4	Épület-együttes	800	2050	1800	4500	1375
5	TVOR/DME	875	2200	2250	4650	1625
6	LI/MM 357L	1050	2050	2400	4850	1800
7	TAR/SSR	450	3225	2100	3700	950
8	13L PAPI	475	3175	1550	3350	350
9	2A Terminál (Északi sarok)	1200	3550	1025	2800	500
10	Tűzoltó készenléti hely	3575	6025	3100	475	2825
11	Épület (31R)	3825	6275	3300	375	3050
12	GP, PDME (31R)	3475	6000	3125	375	2750
13	31R PAPI	3450	5975	3125	400	2700
14	Épület (13L LLZ)	4150	6675	3775	350	3400
15	Épület	1950	4025	3525	2300	1125
16	Objektum	1950	3475	425	3125	1325
17	31L PAPI	1600	2675	425	3800	1325
18	RVR mérő/PDME (31L)	1775	2675	425	3875	1500
19	Hangár	2175	2750	575	3975	1975
20	Hangár	2250	2400	800	4250	2025
21	Helikopter-leszállóhely	1825	800	1175	4650	1900
22	Kompenzálóhely	1200	2050	1050	4225	1325
23	13R PAPI	2450	450	2625	5925	2925
24	GP/PDME (13R)	2475	375	2700	5975	2950
25	Épület	3100	300	3350	6625	3600
26	ATS	3175	450	3275	6650	3550
27	Épület	2850	375	2900	6300	3350
28	„L” Épület	2625	700	2475	5900	3025
29	1 Terminál	2575	1050	2250	5675	2875
30	Hangár	2575	1300	2025	5475	2775
31	Készenléti épület	2425	1500	1775	5275	2625
32	Készenléti épület	2400	1575	1700	5200	2575
33	Épületcsoport	2425	2250	1250	4700	2325
34	Kémény	2225	3150	475	3500	1600

1. táblázat. A Ferihegy repülőtéren azonosított tereptárgyak valós távolságai a vonatkoztatási pontoktól. Pirossal jelölve az ún. beállítható távolságokat jelző értékek.

A fenti táblázatból látható, hogy az azonosított objektumok megfigyelési pontoktól mért távolságértékei egy a 350 m-től 6675 m-ig terjedő skálán oszlanak el, és a beállítható látástávolság értékek egy része is megtalálható közöttük (1. táblázat). Ezek közül kiválasztottuk (és a táblázatban piros színnel kiemeltük) azokat, amelyekre a megfigyelési

pontról való tiszta rálátás biztosított, ezáltal a látástávolság hitelessége felmérhető. A fennmaradó távolságértékek, melyekre még nem állt rendelkezésre optimális rálátási helyzet, de felmérésük a teljesség érdekében szükséges volt, a következőek: 100m, 200m, 4800m. Ezek méréséhez az irányítótornyot (TWR) és a 19. sorszámmal ellátott hangárépületet, mint jól látható objektumokat jelöltük ki. A 100 m-es távolság megfigyelési pontjának a B3 gurulóút irányítótoronnyal szemben lévő távolabbi szegélyét, a 200 m-esnek pedig az A és M gurulóutak kereszteződését választottuk. A 4800 m-es távolság ideális megfigyelési pontja a 31-es jobb futópálya küszöbénél (31R) lévő felhőalap mérő állomás. A látástávolságok felmérésére így rendelkezésünkre álltak az optimális pozíciók, ezeket a következő térkép-kivágaton szemléltetjük (4. ábra). A megfigyelési pontokat zöld színnel jelöltük, a felmérendő távolságokat pirossal, és aláhúzott kisbetűkkel. A jobb láthatóság és elkülöníthetőség kedvéért az 1000m alatti távolságokat fekete színnel húztuk ki (4. ábra).

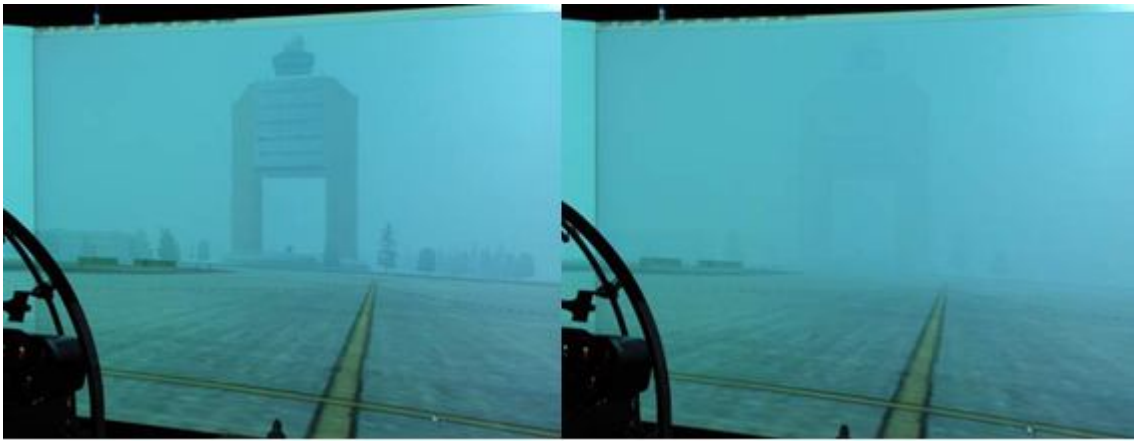


4. ábra. A beállítható távolságok reprezentálására kiválasztott pozíciók a Ferihegyi repülőtér AIP térképén.

AZ ADOTT VIRTUÁLIS KÖRNYEZET FELMÉRÉSE

A látástávolság megjelenítésének felmérését a 4. ábra szerinti sorrendben, tehát a kisebbtől a nagyobb távolság felé haladva, minden esetben legalább kettő (az aktuális és egy szomszédos) beállított értéket megvizsgálva végeztük, hogy a kérdéses látástávolság meghatározható legyen (ezt az elvet használják a repülőtéren dolgozó észlelők is a horizontális látástávolság meghatározásakor). Mindegyik beállítható látástávolság értéket megvizsgáltunk a fentebb leírtaknak megfelelően. Az alábbiakban – terjedelmi okokból adódóan – csak a 200m, 1600m és a 3200m beállítható látástávolság értékhez tartozó vizsgálatot mutatjuk be.

A 200 m-es látástávolság felméréséhez a kijelölt megfigyelési pontra repültük a helikoptert, amely jelen esetben az A és M gurulóutak kereszteződése. Ebben a pozícióban a távolságunk a szemben lévő irányítótoronytól 200 m volt. A látástávolságot 400 m-re állítva rögtön körvonalazódik az irányítótorony. Méretéből és távolságából adódóan teljes egészében megjelenik előttünk a projekciós felületen, továbbá pozíciónk bizonyítékaként a gurulóutakat jelölő sárga vonalak kereszteződése is látható, közvetlenül előttünk (5. ábra). Ugyanezen megfigyelési pozícióból 200 m-re állított látástávolság mellett – az első esethez hasonlóan – csak a torony körvonalai láthatóak, és az ugyan még látható, de már nem válik ki olyan egyértelműen környezetéből. A körülötte lévő fák, és a tűzoltóbázis teljesen elhalványultak. Ebben az esetben a meteorológiai látástávolság ténylegesen 200 m körül van.



5. ábra. A 200 m-re lévő irányítótorony látványa a 400 m-es (bal oldali kép) és a 200 m-es (jobb oldali kép) beállított látástávolságnál.



6. ábra. Az 1600 m-re lévő kémény megjelenítése 1600 m-es (bal oldali kép) és 1200 m-es (jobb oldali kép) beállított látástávolságnál.

A következő objektum, amely segítségünkre volt, a 31-es bal futópálya küszöbétől 400 m-re déli irányban kimagasló, 34-es sorszámmal ellátott piros-fehér színű kémény. A megfigyeléséhez ismét a repülőtér vonatkoztatási pontra (ARP) repültük a helikoptert, innen a kémény távolsága 1600 m, és délnyugati irányra fordulva pontosan előttünk látható. A láthatóság kedvéért a keresett objektumokat piros körrel megjelöltük, és a képek jobb felső sarkában felnagyítottuk. Mindkét képen közvetlenül előttünk láthatóak az A, K, és a N

gurulóutak egymást keresztező középvonal-jelzései. Az 1600 m-re beállított látástávolságnál a kémény és a közeli fák is körvonalazódnak. Jól megfigyelve, még a kémény feltűnő csíkozott festése is kivehető. Azonban a látóhatárt 1200 m-es távolságra csökkentve teljesen eltűnik a szemünk elől, már felnagyítva sem látható (6. ábra). A reprezentált látástávolság tehát 1300 m és 1600 m között van (közelebb az 1600 m-hez)!

Végül a 3200 m-es látástávolság vizsgálatához a helikoptert a 31-es jobb futópálya küszöbéhez állítottuk. A távolban északnyugati irányban kimagaslik az irányítótorony (TWR). 3200 m-es látástávolságot beállítva, az objektum még jól látható. Azonban, ha a látóhatárt a torony távolságánál kevesebbre, a szomszédos 1600 m-es beállítható értékre állítom, az épület már szabad szemmel nem fedezhető fel, sőt, nagyítás mellett sem rajzolódik ki (7. ábra). Ekkor tehát a megjelenített látástávolság 3200 m és 1600 m közötti értéket mutat.



7. ábra. A 3200 m-re lévő irányítótorony megjelenítése 3200 m-es (bal oldali kép) és 1600 m-es (jobb oldali kép) beállított látástávolságnál.

EREDMÉNYEK

Az elvégzett teljes felméréssorozattal sikeresen teszteltük – és egyben be is mutattuk – szimulátor meteorológiai alrendszerének a környezeti modellre gyakorolt hatását a meteorológiai látástávolság tekintetében. A repülőtér méreteiből, a megjelenítés/képrögzítés minőségéből fakadó korlátokat figyelembe véve, az 5000 m-nél kisebb látástávolságokat mértük fel, melyek kialakulása repülésbiztonsági szempontból a leginkább fontosak. A felmérés folyamán láthattuk, hogy a látóhatáron belül elhelyezkedő objektumok tökéletesen azonosíthatók, az azon kívül lévők, pedig nem láthatók. A látóhatáron lévő tárgyak, épületek kissé nehezebben, de felismerhetőek, körvonalaik még megjelennek. Ezek alapján joggal állíthatjuk, hogy a látástávolság ily módon szemléltetett megjelenítési pontossága az 5000 m-nél nagyobb távolságok esetében is fennáll, hiszen a látvány előállításához használt – a meteorológiai alrendszerben beállítható – légkörfizikai összefüggéseken alapuló látvány-generáló eljárások ugyanúgy működnek nagyobb látástávolság értékek esetén is.

Fontos azonban megjegyeznünk, hogy a konkrét helikopter-szimulátorban installált meteorológiai alrendszerben csak a korábban említett néhány látástávolság érték állítható be (nagyléptékű diszkretizáció). Éppen ezért, a tesztelés során is csak a legközelebbi értékek alkalmazásával tudtuk a konkrét látástávolságok értékeit vizsgálni, melyek azonban – a nagyobb látástávolságok esetén – jóval messzebb estek a kiválasztott értéktől (pl. 3200 m esetében 1600 m volt a legközelebbi kisebb beállítható érték). Ebből adódik, hogy a 3000 m

körüli látástávolság tartományban csak azt tudjuk megállapítani, hogy a megjelenítés hibája nagyságrendben kisebb, mint néhány 100 m. Az 1000 m-nél kisebb látástávolságok esetén ez a hiba biztosan kisebb, mint 200 m.

Mindezek alapján megállapítható, hogy a helikopter-szimulátor virtuális környezetének megjelenítése a meteorológiai (vízszintes) látástávolság esetében – az adott pontosságra vonatkozó megjegyzések mellett – realisztikus és megbízható.

IRODALOM

Bottyán Zs. (2009): Gondolatok a repülőgép-szimulátorok meteorológiai alrendszerének szerepéről. Repüléstudományi Közlemények.

Bullrich K. (1964): Scattered radiation int he atmosphere and the natural aerosol. Advance in Geophysics. Vol 10. 99-260.

Johnson J., C. (1954): Physical Meteorology. John Wiley and Sons, New York

Rolfe J., M. and Staples K., J.(1988): Flight Simulation. Cambridge University Press.

van West, J. and Lane-Cummings, K. (2007): Microsoft Flight Simulator X for Pilots: Chapter 13: Weather 2007.
Forrás: http://www.avweb.com/news/avtraining/flight_simulator_x_for_pilots-chapter_13-weather_196384-1.html

Williams B. (2006): Microsoft Flight Simulator as a Training Aid, Aviation Supplies & Academics Inc. Newcastle, Washington.

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Gőcze István
gocze.istvan@zmne.hu

THE WAR OF FUTURE – THE FUTURE OF WAR
Views held by the United States on 21st Century armed combat and USA's novelties in military techniques and technologies – Part 2

Absztrakt/Abstract

A szerző cikke második részében a hagyományos haderőnemeknél bekövetkezett illetve folyamatban lévő haditechnikai fejlesztéseket vizsgálja meg. Továbbá azt kutatja, hogy e szervezetek estében, miként alakul a 21. századi hadviselés, illetve hogyan vélekednek erről a különböző amerikai szakértők

In this second part of the article, the author examines the development in military techniques which occurred, or are in process to take place in branches of traditional armed forces. Furthermore, he explores the ways in which, 21st Century warfare takes shape within these organizations and what are the opinions of different American specialists about this process.

Kulcsszavak/keywords: *háború, hadviselés, jövő ~ war, warfare, future*

LAND FORCES

First of all, let's look at how do US specialists see the future's armed combats in case of land forces.

A pilotless robot plane (UAV) provides the location of the enemy base and this report is sent to the forward combat positions. The armed intervention is directed by the commander from 30 kms distance, through satellites. At this point, the human factor enters the forestage. Troops advance to viewing distance, the strike team occupies its position, based on exact GPS coordinates, then it encircles the enemy base. Robots and UAVs approach the target and the attacking infantry's armoured fighting vehicles' cannons open fire.

According to Popps, the future's combat systems is a leap forward in precision weapons, vehicles with human and automatic control, operator-provided modern artillery, unmanned aerial vehicles and such weapons, which enable combat even beyond viewing distance. (2008)

The commanders of tomorrow will have to bring the troops out to the field of combat through new means. Such is, for instance, the Stryker. In case of the Stryker, we can see that the debate about caterpillar versus wheel-based drives was settled, given that this combat vehicle possesses eight rubber-clad wheels. According to "end-users", the vehicle is extraordinarily mobile and quiet. Troops are comfortably seated in it, being the most up-to-date armoured troop carrier vehicle. It is equally quick and quiet on both paved and poor quality roads. With the help of the Sryker, solders are able to strike upon the enemy vanguards as much as 100 kms away, where these do not even expect them.

„The combat vehicle has two main varieties, which are the Stryker IPC (a transport vehicle) and the Stryker MGS (gun tower- equipped) vehicle versions. In addition, eight sub-versions exist for the Stryker IPC. These are: the Nuclear, Biological and Chemical Recon Vehicle (NBC RV), Anti Tank Guided Missile equipped vehicle (ATGM), Medical Evacuation Vehicle (MEV), Mortar Carrier Vehicle (MC), Engineer Support Vehicle (ESV), Commander's Vehicle (CV), Fire Support Vehicle (FSV), and the Reconnaissance Vehicle (RV).

The crew of Stryker ICV is made up of 11 people (commander, driver and 9 crewmen). Its armament consists in the Protector Remote Weapon System. Contents: 1 pc M2 machine gun, 1 pc MK19 40 mm grenade launcher, or 1 pc MK240 7,62 mm machine gun and 4 pc M6 smoke grenade launchers.



Fig.1. Stryker ICV
(Source: http://www.haborumuveszete.hu/rovatok/fegyverek/pancelosok/stryker_pszh/)
(28. 10. 2010)

The Stryker MGS' crew is made up of 3 people (commander, driver and gunner). Its armament consists in a 105 mm cannon with autoloader, which can fire 10 shots per minute." (Art of War, 2006)



Fig. 2. Stryker MGS
(Source: http://www.haborumuveszete.hu/rovatok/fegyverek/pancelosok/stryker_pszh/)
(28. 10. 2010)

Within the land forces arm, the Stryker is only one element in the future combat. As future combat vehicles enter deployment, commanders also have to lead and direct their units and sub-units with different methods. Own forces can be continually tracked through the army's new recon-tracking system. Every vehicle is equipped with a GPS locator, while own forces are displayed on digital maps with blue identification symbols. By clicking with the mouse on the icon, numerous information appear about the given asset or person. The position of every single combat vehicle is known, vehicle identifiers making possible the determination of their exact position. During combat, this provides a considerable advantage and support, as up to now, connection was only maintained through radio, which was the only way to get to know the position of troops. These days, the terrain, as well as the position of own units can all be seen through a map displayed on a screen. IT provides connection between all fighting vehicles, combat systems and soldiers. However, the successful land combat needs air support, as well.

THE AIR FORCE

The F-16, the new F-22, and moreover, the newest F-35 fighter jets are able to fly at sea level, reaching twice the speed of sound, with a speed of more than 2000 kms per hour.



Fig. 3. F-35 fighter jets
(28. 10. 2010)

Nevertheless, a new technology exists, which may make these planes obsolete. This is the Scramjet[1]. The Scramjet is a supersonic combustion ramjet engine[2], operating with traditional fuel, at speeds of 4-7 Mach. By using hydrogen as fuel, its top speed may be increased to up to 14 Mach. At a speed of 5 Mach, meaning above 6000 km/h, the supersonic flights become hypersonic. The key factor to achieve this top speed is the Scramjet engine's airflow intake and blow-out. Compressed air arriving into the burn-chamber is not slowed down to subsonic speed, as the process created this way provides a larger thrust power and much higher speed. The Scramjet can not only operate on fighter jets. Hypersonic airplanes ensure higher speed and efficiency. Having a greater speed, one can strike deeper and more efficiently into enemy territory. The essence of this system is that the attacking aircraft can cover 1200 kms in 10 minutes, meaning that, a robot airplane can make it from Chicago to Washington DC in this short time. Let's see an example from a present day fighting scene: in Afghanistan, this technology allows to attack a marked target without the need to fly with our fighter jets into a hostile nation's airspace.

The hypersonic jets fly with Mach 10; however, one of the most important technological breakthroughs consists in the development of the slow, unmanned aerial vehicles, the UAVs. Their shape is strange, they are slow and do not have their own weapons yet, but it is highly likely, that these airplanes will serve as the core of tomorrow's aerial arsenal. Coalition forces in Afghanistan use UAVs to recon the enemy positions, and launch attacks from them, mainly with Hellfire missiles. The great advantage of UAVs is that these can fly anywhere and can stay in the given airspace for a prolonged time, while no pilot is endangered. The "electronic eyes" (cameras) monitor the landscape, track the target and warn the navy ships and coastal forces about the potentially hostile activity. UAVs are also capable to escort the fleet, watch for terrorist actions, or perchance, the enemy's landing. According to Leahy, it was the development of IT that brought along the huge advancements. Onboard sensors and other equipment made possible the first informatics revolution, which brought to life the Predator and the Global Hawk, as bases from which, even better such contrivances can take off. (2005).

The pilotless combat airplane (UCAV) will be among the new generation of UAVs also and it will even fly in formation. It doesn't look like any of its pilot flown buddies; it will be smaller and it will be able to put up with stresses which are beyond human endurance.

[1] HTKA: The hypersonic aircraft and their hearths – the Scramjet (http://htka.hu/2009/11/06/a-hiperszonikus-repulogepek-es-szivuk-%E2%80%93-a-scramjet/)

[2] http://hu.wikipedia.org/wiki/Torl%C3%B3sug%C3%A1r-hajt%C3%B3m%C5%B1



Fig. 4. The X-47A UACV
(Source: http://www.jp-petit.org/Disclosure/disclosure_a_doubt.htm)
(28. 10. 2010)

The flight systems and weapons of today's UAVs are still commanded remotely, by an operator, but in the future, these will run automatically, according to a programmed flight plan. In the future, different UAVs will cooperate with each other, based on shared intelligence (reckoning) and decision making, in order to strike a target, while the observing person does not even have to intervene at all. We can state, according to Leahy's opinion, again, that within ten years, one-third of all combat airplanes will be unmanned. Given the integration of arms, the role of traditional airplanes will be to transport the troops to and from the combat zone. The future combat system is expected to ensure fast deployment (dispersion) of the troops. (2007)

These days, a ship-based unit can board a smaller transport plane, which will take it to the marked area, then return to the base. "But we already have such sensors, which will signal us that, at precisely this or that place, there is an almost 600 metre-long open place, which is proper for landing, the ground is solid and there are no enemies nearby. Once the defence is organized, the plane can enter the area and land under any meteorological conditions. What can we do without sensors? The airplane picks up the first platoon, flies over the target area and then, it returns for another load, which it might drop at a much further location. Today, we can't talk about fast and precise aerial troop transports". (Leahy, 2009)

The new technologies revolutionize the land-based and aerial combat of the future, but there are changes in the making at the navy, as well.

THE NAVY

These days, the navy fleet is radically changing. The new navy ships have to execute novel assignments. Furthermore, these vehicles move and fight in ways differing from their predecessors. In the past, navy ships were tasked to fight in open sea combat and to cover with artillery fire the

enemy coast from afar. Nowadays however, there is a need for faster and more expandable ships. Some of these do not even look like ships as we knew them. The FSF1 SeaFighter[3] is a vehicle which was developed by the Naval Research Office.



Fig. 5. The FSF1 SeaFighter
(Source: http://www.ifish.net/gallery/data/500/medium/Sea_Fighter_FSF1.jpg)
(28. 10. 2010)

The aluminium-bodied catamaran was designed for fast actions in shallow coastal waters. It is capable to manoeuvre in as much as 3.5 metres of water depth. It is basically a multipurpose vehicle. Numerous, so called deployment modules were designed into the ship's body, so that it is capable for mine-sweeping, anti-submarine combat, amphibious operations or humanitarian help support. On its right side, or at the back, it can receive or deploy inflatable rafts and remotely controlled boats. The flight deck was constructed for helicopters and vertical landing and takeoff UAVs. Regarding its stealth properties, the inner areas within the hull were coated with such materials, which decrease escaping vibrations and noise by 70%. It is indeed faster and more mobile then racing boats, as its top speed can reach up to 90 kms/hr. Its excellent manoeuvrability is ensured by the two Rolls Royce water jet engines, which can also be operated individually from each other.

In case of traditional combat ships and other fighting vehicles, the propulsion is separated from the weapon system, meaning that the propulsion force is not appropriate for enemy detection, or in the combat against it. However, this principle is to be modified, as well. The new, electric navy ships and fighting vehicles are already on the designers' board.

With the large amounts of generated electric power they can even operate sensors or weapons. The designing process of vehicles is undergoing a change, as more efficient integrated vehicles are in the making, with higher survivability capacity. The generator-produced electricity feeds the propulsion, as well as the radar, sonar, missile launching system, or provides energy for the electronic weapons. The DDG-1000 integrated supply destroyer, which was already presented in the first part of the article, is equipped with the newest traditional weaponry, planned to be updated with even more state-of-the-art weapons during an upcoming stage. The directed energy weapons operate with microwaves, electric impulses and laser beams. Their energy paralyzes or destroys

[3] Strategy Page: Sea Fighter (http://www.strategypage.com/military_photos/military_photos_20052816.aspx)

the enemy's ships and shots down its missiles or aircraft. The new weapon featured on the new ships is the electric cannon, being under development over the last 75 years.[4]

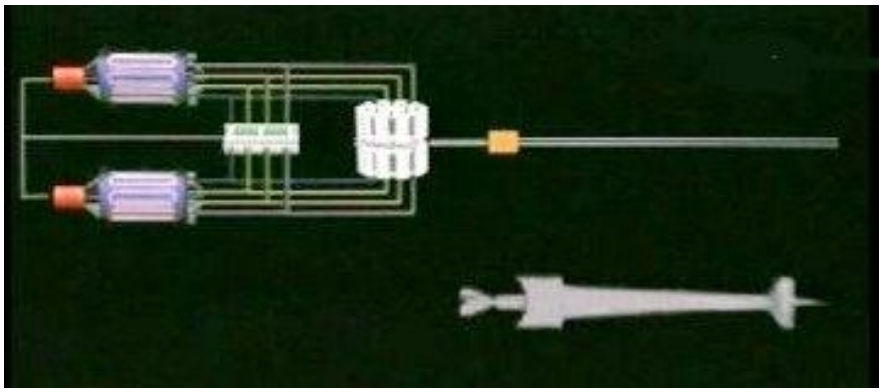


Fig. 6. The electric cannon
(www.wikipedia.org)
(28. 10. 2010)

They send electric current through two parallel sliding rails, which induces an electromagnetic field. The projectile, which is made of a conducting material, is placed between the two rails, closing the circuit. The propulsion energy starts up the process, based on the Lorenz-effect, shoots the projectile out towards the target. The operation principle of the electric weapon is as follows: an electromagnetic field is generated and using the electromagnetic field's reciprocal effect, the projectile moves along the two rails at a speed of 6-7 kms/second. This is 5-6 times faster then the customary speed of traditionally charged weapons. The grenade moves so fast, with such a kinetic energy, that there is no need for a warhead. During testing, the Wolfram bar used as a projectile penetrated through the armour plate of a tank.

Its other considerable advantage is the firing range. The Navy plans to deploy into combat electromagnetic cannon with a firing range of 400 km.

The projectile covers 80% of its 500 km trajectory in outer space. During its return, the atmospheric drag slows it down a bit, but even this way, it is much faster then the grenade of any of today's weapons.

CONCLUSION

As a conclusion, we can assess that, in all three combat arms of the USA, such techniques and technological developments are under way, which, according to my own judgement, are far exceeding the framework of anti-terrorism combat and are maximally appropriate for deployment in conventional armed combat, if the nation's interests dictate it so.

[4] „During the 1920's, the Norwegian Birkeland already developed an electric cannon, based on his patent registered in 1902. During the 2nd World War, the Germans also did experiment with such a weapon, but the technology of that time was not yet appropriate. The USA started experimenting 20 years ago, at smaller scales and they arrived here through a process full of hurdles" (Twentieth Century: The Electric Cannon http://www.huszadikszazad.hu/index.php?apps=cikk&cikk=5055)

REFERENCES

Art of War (2006): *The Stryker combat vehicle*
http://www.haborumuveszete.hu/rovatok/fegyverek/pancelosok/stryker_pszh/
(Download date: 14. 08. 2010)

LEAHY, M. B. (2005): *Structural Challenges for the Next Century of Flight*
http://www.asipcon.com/2006/images/proceeding05/pdf%20files/Thurs/1200_Leahy.pdf
(Download date: 21. 10. 2009)

LEAHY, M. B. (2007): *Microsystems Technology Office (MTO) Unmanned Combat Air Vehicle (UCAV)*
http://www.darpa.mil/darpatech2002/presentations/tto_pdf/speeches/LEAHY.pdf
(Download date: 21.10. 2009.)

LEAHY, M. B. (2009*): The Wartime technology of the Future*
www.Spektrumtv.hu
(Download date: 05. 06. 2010)

POPPS, D. (2008): *Congressional Black Associates Welcomed to DoD by Army's Acquisition Executive*
https://www.alt.army.mil/portal/page/portal/oasaalt/Bio_PRINCIPAL_DEP
(Download date: 12. 03. 2010)

SPEKTRUM TV, February 19, 2009.

www.wikipedia.org

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Miskolczi Ildikó
miskolczi.ildiko@gmail.com

EDUCATION IN THE XXITH CENTURY: TEACH OR HELP TO LEARN?

THE ASSIMILATION OF THE PRESENCE EDUCATION AND MODERN DISTANCE LEARNING, WITH SPECIAL REFERENCE TO THE ELECTRONIC DISTANCE LEARNING

Absztrakt/ Abstract

A cikk bemutatja a köznyelvben hagyományosnak nevezett jelenléti oktatás, és a XXI. század technikai, illetve világháló adta lehetőségeit kihasználó legmodernebb oktatási forma, az elektronikus tanulás közti különbségeket. Az alapfogalmak meghatározása után az előadó beszél a modern IKT eszközök alkalmazásáról napjaink oktatásában. Kitér a jelenléti oktatás során történő alkalmazási lehetőségekre (blended learning) csakúgy, mint a távoktatásban történő felhasználás igényére. Bemutatja az elektronikus oktatás jelentőségét korunk digitális világában. Megfogalmazza az oktatásmódszertan változásának, változtatásának igényét az IKT eszközök adta lehetőségek tükrében.
Az internet, a digitális technológiák használata, a hálózatos tanulás lehetősége az oktatásban tegnap lehetőség volt, ma szükségszerű, holnap kötelező lesz. Az oktatásban Gutenberg kora lejárt. Az oktató szerepe átalakul(t). Nem a tudás átadása, hanem a tudás megszerzésének lehetővé tétele, segítése (lesz) a feladata.

The paper presents the differences between the traditional education and the modern forms of eLearning, which use the most modern forms of education for example World Wide Web. After defining the basic concepts, the artist talks about the application of modern ICT tools in education today. Refers about using these tools in the presence education, the employment opportunities during the training (blended learning) the possibilities of use in distance learning. It illustrates the importance of today's digital world in electronic education. It refers about the methodology of education. The Internet, digital technologies and online learning opportunity in education was possible yesterday today necessary and tomorrow will be mandatory. Gutenberg in education is over. The instructor's role is transformed. Task of teacher is not to transfer the knowledge, but to help the students to learn, to earn the knowledge.

Kulcsszavak/Keywords: *távoktatás, távtanulás, elektronikus tanulás, IKT eszközök, felhő-technológia, felhőtanulás, felhőpedagógia ~ distance education, distance learning, eLearning, ICT tools, cloud technology, cloud learning*

INTRODUCTION

The methodology of education in the 21st century goes through a significant transformation when the tools of modern ICT appear into the education independently we are talking about presence or distance education. Currently grown up the „digital generation" or as Tapscott [1] says „n-generation" (net generation). The net generation grew up with internet. The most prominent feature of this generation is to learn with incredible efficiency and speed. For management of relations and getting informations they use hyperspace unwavering certainty. Regardless of what ICT tools available for information and/or (knowledge) acquisition, a fraction of a moment they share the connections through the virtual space, while reinterpreting their own thoughts and emotions of adding. This is born of knowledge, and such way we create the meaning. This generation expects the usage of these applications from the trainer, because usages of these applications are natural to them.

However, the needs of the lifelong learning (LLL), in the 21st century is basic both for economy and society too. To become a good technician and potential worker is not enough to learn a job when we are young. All life we have to learn that can be professionally recognized. The economic and financial crisises in the world, the changes in societies are demand not to know only one thing, but we are able to stand other areas of life. This is the concept of the whole life learning, covering the all territory of life (life wide learning, LWL). The interpretation of Bertalan Komenczi the LLL is at the same time, and the contents of the LWL (width) are determined by the content of the thinking (life-wide learning) in the 21st century. [2] We can see the contents of throughout the life-wide learning (LLL and LWL) context on the Figure 1.

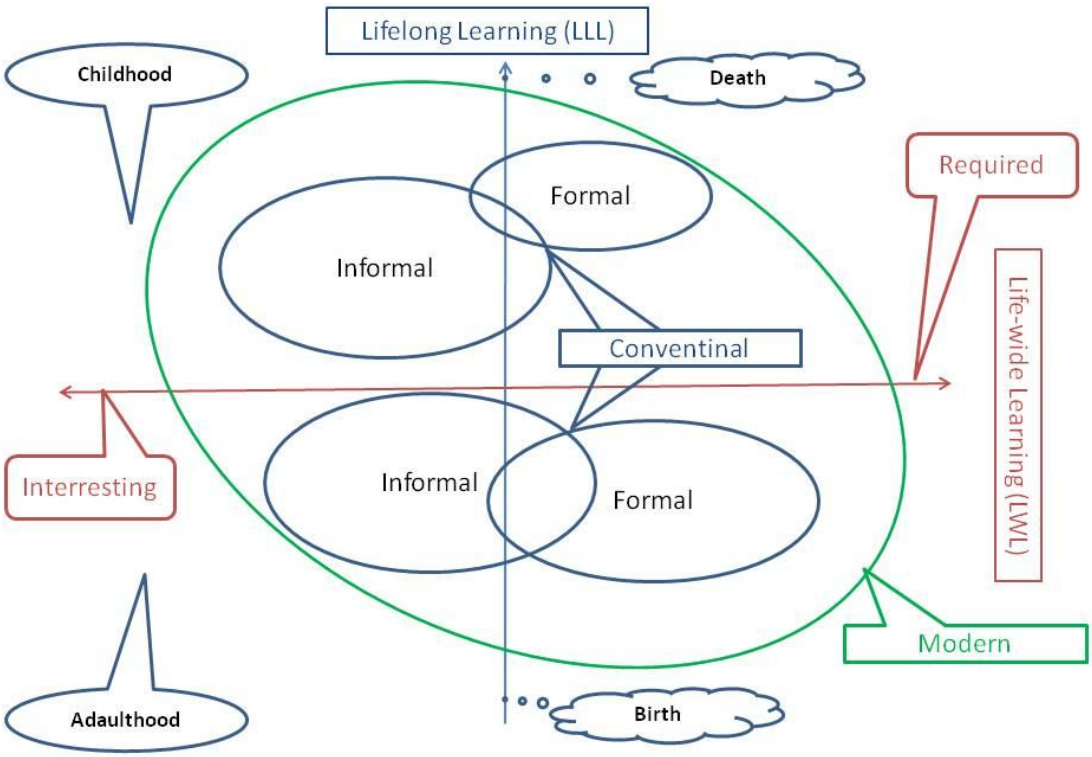


Figure 1. The whole life-wide learning model
(By: Ildikó Miskolczi)

In the 21st century there is more and more knowledge. This is increasingly more difficult to make the process of reception and processing for the users. However, the knowledge becomes the very quickly obsolete, so the renewal time of the knowledge is less and less. We want to know more and more in less time. In a specific field of knowledge „up-to-date", complex way, however, many-to-know knowledge applied, which means the significantly increased the length of time in learning.

THE CHANGE OF FACTORS OF LEARNING

Technical development

However strange it may seem, but if we research on the development and the appearance of distance learning, we have to search for its roots in the correspondence course. To do this, we must put the clock back. According to some researchers, the founder of the correspondent education was St. Paul, [3] who has made his clerks write his doctrines and made his messengers spread his teachings. The papyrus was massive product so it could take the long-distance transport well. St. Paul has also used a certain degree of "interactive" items in his written messages to ensure that his words get into the thought of the followers. He put rhetorical questions in his texts (and even he replied to them). So he has broken the monotonous tune of the written text. These questions-answers had claimed to continue the thinking of the raised thoughts.

With a big jump forward, most of the researchers profess that the first true e-mail type of education is related to Isaac Pitman. Pitman was the person, who taught shorthand in 1840 in Great Britain this way. He was in communication with his students through postcards and he sent the exercises them through postcards too. Thus, the claim to communicate with the pupils has already appeared in the early monuments. In 1856, the first correspondent school has been founded in Berlin, where Toussaint taught languages in the form of correspondence. At the end of the 19th century - with the exception of Africa - maybe in almost each continents correspondence school appeared. The schools were excellent which worked in Australia, America (since 1891) and England (1856), and France (since 1877). At the beginning of the 20th century, in 1905, was the first correspondence school established in Baltimore, and in 1914 in Australia, and in 1919 in Canada were also founded this kind of schools. [4]

György Seres and his colleagues have presented in their article [5], how the electronics, the appearance and application of information and communication tools became the instrument of the education from the subject of it. „*In the 1920s and 1930s, popular public radio and public television broadcasts have started, and they have made the electronics the major and new parts of the education. The school-radios (1940s) and school-televisions (1950-60s) have already made the electronic the part of tools in the community education. In the 1970s the magnetic recording and in the 1980s video recorders and personal computers have been produced, and because of these the new device has already been in school education initiated. The great breakthrough was brought in the 1990s by the widespread use of the Internet, and in the first decade of the new millennium, by the spreading of the broadband data transmission, the quick Internet access. With the help of the digital data-, audio- and video record, as well as the transmission of data by using a broadband data transmission, via the Internet, any kind of syllabuses may be made available for* ***anybody****,* ***anywhere****, and may at* ***any time*** *within a* ***realistic time****. This is the point where the electronics has been become from the subject and tool of the education to the scene of the learning.*

Increasingly complex user programs to run, the increasingly larger data files to store and move, the more data processing and data transfer speed to achieve a stronger and more expensive hardware and software requirements for the users of the site.

Recognizing this, in the second decade of the 21st century, a service was born, that is called Cloud Computing. With this service, the data storage and data movement, as well as the large computing tasks cannot be carried out by the users on their own computers, but also by a means of a simple Internet browser free of charge, or, when creating your own resources and the operation is substantially less in return for a rent service, these tasks are provided by service that are worked in cloud computing.
The thought, of course, is not new. To find a data source via the Internet jungle, we haven't searched through our own computer on the World Wide Web for a long time. This task has been making by searching services that maintain enormous resources (Yahoo, Google, etc.).
The modern, cost-effective, interactive knowledge transfer cannot be resolved using only their own resources. In this area, you can also use the services of Cloud Computing." [5]

Changes in the needs of society

„In the second half of the 20th century, however not only *science, technology,* but *society*, and the economy have *also begun a fast development and because of this, the knowledge that we obtain in the schools become obsolete in our active life many times, so that we have to start to learn again and again if we want to save our competitiveness on the labour market. At the end of the 20th century, it has been born the concept of „lifelong learning" (LLL).*
Traditional school education system, of course is not capable of giving satisfaction this claim. Therefore large companies, by following the millennial traditions of armies, the regular training of the employees are organized themselves, and for the smaller ones professional training enterprises ensure the regular trainings." [6], [7]

The development of ICT technology and in the third part of the last century significantly changing social needs have effected together on the attitude of the people to the knowledge and learning.

Today there is no doubt that the lifelong learning more specifically, the extending of it to each part of our life is the necessary coefficient of our life. Essential in the sense that in the globalised world, we have to always renew our knowledge to adapt to the evolving and changing economic conditions, social expectations. Beyond the individual personal demands, the constraint is often the reason for a continuous learning process, as it is, in the 21st century's accumulated knowledge that are produced by hyper society, information has increased almost exponentially from hour to hour. However, a factual knowledge can very quickly become obsolete on any territory/special field of life.

In our time the need for continuous learning is required, however it not only means that the knowledge acquired at an early age, constantly updated to keep it fresh and save it's marketable. Today the economic and social crises and changes require that the people learn other disciplines and get new knowledge in other professions they gain modern, applicable, new knowledge, with which they will be able to occupy other jobs/posts. But if someone deal with a particular profession, lifelong on a high level, in other fields of application, the emphasis will also be required, on a certain level. Thus, a change in the methodology of education is required by increasingly emerging approach that use instead of the whole concept of lifelong learning, a more modern concept and it has a better reflects the reality of the whole life (in all areas), covering concept of learning. The concept of life-wide learning was used in the Hungarian pedagogy by Bertalan Komenczi. [8]

Changes in the methodology of education

The eLearning

In the second half of the 21st century, at the end of the 1960s, the beginnings of eLearning were appeared. In the 1970s were already operating networks specifically for higher education (PLATO, TICCIT). From the end of the 1980s, has been developed a modern ICT tools supported education, that means of a form of eLearning, what can change fundamentally the learning process and the methodology of teaching.
„The nice new world of eLearning is just virtual, so it's only an opportunity, potential a reality. In order to become a reality, in each educational institutions and, usually in those institutions that organize teaching services, we claim another thinking, to learn new things, and a lot of resources and a very serious, thoughtful and disciplined work are needed. It is distributed virtuality, from which will be always formed the reality in the learning environment while we develop the specific programme, which may be either Didactica Magna. It is the virtual reality of pedagogy." [9], written by Bertalan Komenczi[1] in 2004. Today, probably he thinks otherwise these words or a part of them. Today eLearning is not only a possibility, not only virtuality. Here it is, it is an integral part of our everyday life. *„Virtual reality of the pedagogy"*-type Komenczi [9]. So I would say: the reality the virtual world of pedagogy.

The opportunities of eLearning make today's pedagogical practices wider and more colorful. More and more elements of it are displayed and continuously incorporated into the training attendance (blended learning), as well as in a large part of the distance learning. In the regular training and in non-formal education systems both, the application of it spread quickly. Today grown up the N-generation (net-generation), in other word the digital generation. In their life there was not a section, when they have no a computer or internet, take for granted and require the application of modern techniques, technologies in the field of education too.

The dominance and spread of electronic devices in the education means that we won't talk about *„learning"* and *„eLearning"*. The *"e"* prefix will disappear quickly from this form of education, because the electronic education, e-learning, as a form of learning will become usual, natural.
Of course, to this, we need not only equipments, tools and technology, but specially-written and specially-developed „eEnvironment" teachings. Today it has already been.

The networked learning

The development of networked learning practices in some ways is necessary to the eLearning. According to Ilma Kovács, [10] we can speak about the concept of e-learning more than one level. Thus, in the strict sense, only the network's training courses are organized in this way, but if the conceptual series are made wider, this includes any form of education, which builds on any kind of electronic technology, or a device in the education. In my opinion, this latter approach is being widespread in the eLearning system. Of course on the basics of this conceptual circle it means those eLearning processes, what are organized and carried through closed, internal, corporate, school intranets, more widely, those which are organized by the world wide web, or with modern ICT tools using learning processes.

[1] Translated by author.

The networked learning as a technique is significant because with the help of the specially technically developed electronic learning curriculum, the students don't need to go ahead in the curricula in a linear way. The construction of the digital curriculum allows that students explore the existing context independently.

However, the networked learning not only means the structure of the curriculum, but the possibility (and need) to advance knowledge can be reached, not only from the syllabus but with the using of additional resources (which are attached to it), and which are found somewhere in the virtual space. A closed virtual learning environment or the World Wide Web can be the stage of this network.

The cloud learning

The formation of a cloud learning practice is the past two years - a revolutionary new opportunity for education-methodological issues. It is a major station of the distance learning not only from the perspective of the technical development. From education-technical point of view, I see the importance of it that can allow eliminating the space and time limits and the lack of the presence of personal trainers in the educational system. Virtual consultations, virtual conferences, can be created by the Internet service providers. Thus, the learning support will be not only modern, but also interactive. The services of the cloud learning-system support not only the learning of individual student, but it also give help to the teacher and student connections. In addition to the individual learning, group learning can also be taking shape.

Learning in a connectivity way

The principle and practice of networked learning (connectivity), is the new way in distance education. This new paradigm in the distance learning can change the method of teaching in the eLearning in base. Some researchers [11], [12] call this revolutionary new method in learning the fourth teaching paradigm (over behaviorism, constructivism and cognitivism), and they profess, that it will change our whole pedagogical practices fundamentally.

The fundamental principle of connectivism means that we view the knowledge, as a network. The least elements are the nodes in our network. These could be the conceptual definitions, phrases, any elementary knowledge. The chords among them are the relationships, with which we connect the nodes. In this sense, learning may mean two things:

- new nodes to be connected to the fabric
- reordering the net connections.

The high-profile (connecting with many chords to other nodes) nodes determine our thinking. The connectivity-view determines the learning process and its relevance in the opportunity of the construction of the knowledge network and its restructure on demand. Thus, our knowledge increases changes constantly through the established network connections. The network research deals with the examination of this new paradigm, which are also a method and an approach. The network research examines the relationships between things on a micro level, and samples on a macro level, that drawn by the connections. [13]

THE ELEARNING, DEFINITIONS AND CHARACTERISTICS OF ELEARNING

We cannot find the definition of eLearning in the „Act of the Higher Education"[2] thus it has been defined by the research.

[2] 2005. CXXXIX. Act about Higher Education

The eLearning means a new learning environment what is completely different from the presence of the traditional training. It means the application of new techniques, and technologies. It means the usage of ICT technology in the learning process. It's the mode, method and tool of educational form at the same time. By the formulation of Bertalan Komenczi: *„eLearning is the general definition of the education-development efforts that are based on electronical information and communication technology."*[3] [14] However, in the opinion of Ilma Kovács [15] the conception of eLearning can be interpreted on multiple levels, depending on we keep decisive the technology and the learning tool in the learning or only the construction mode, form.

The eLearning concentrates not to the teaching, but to the process of learning, in focus the students, and (apparently) it gives new tasks to the educator. He will help the learners from the background. In this way, the traditional educational structure overturns, and the central idea of this technology will be not the teaching, but helping the students in learning. So this method is primarily characteristic of those educational institutions, which accept and use the constructivist learning model. Institutions where education is considered as a service activity by the school. Where the educational philosophy is not to give the systematized knowledge by the teacher, but to help to the students to learn to coordinate and direct them in the learning process. The teacher's role is primarily helping in this form of learning. Its task is transformed compared to the traditional educational tasks, and this role requires other types of activity.

The eLearning is an educational form what is able to apply in a very wide circle, in the formal, non-formal and informal education too. You can apply it in the distance education and in the presence education too. In the latter case, we speak about blended learning or mixed educational model.

The eLearning eliminates the border-lines in the learning process, because the education becomes independent in space and time too. Today, in the 21st century the learning content will become available *anywhere*, *anytime*, for *anyone* with the application of eLearning, and with it these contents will be acquirable *within a reasonable period*. György Seres analyzed full-size of the conditions in his researches [6], [7], when he created the first distance learning and e-course[4]. I tried it myself as a student, and I have collected my personal experiences about the learning with eLearning and the function of the virtual Intranet. [16]

A further characteristic of the eLearning, that it helps not only the individual learning, but learning of the small or large groups at the same time and it isn't demand on the students are close or far from each other in the space. It is able to learn big masses although, but it also supports the individual training.

In conclusion, we can declare, that the eLearning is a new educational environment, which requires different teaching-learning style from the traditional education modes, and it has new strategies in its method. In addition, the entire learning process that based on eLearning has to be organized in a new way, and a new pedagogical method has to be applied. It has new, growing, ever-changing toolbar. The application of information and communication technologies (ICT) in education is a challenge and an opportunity at the same time for both the teacher and the student.

[3] Translated by author

[4] http://drseres.com/elearning/

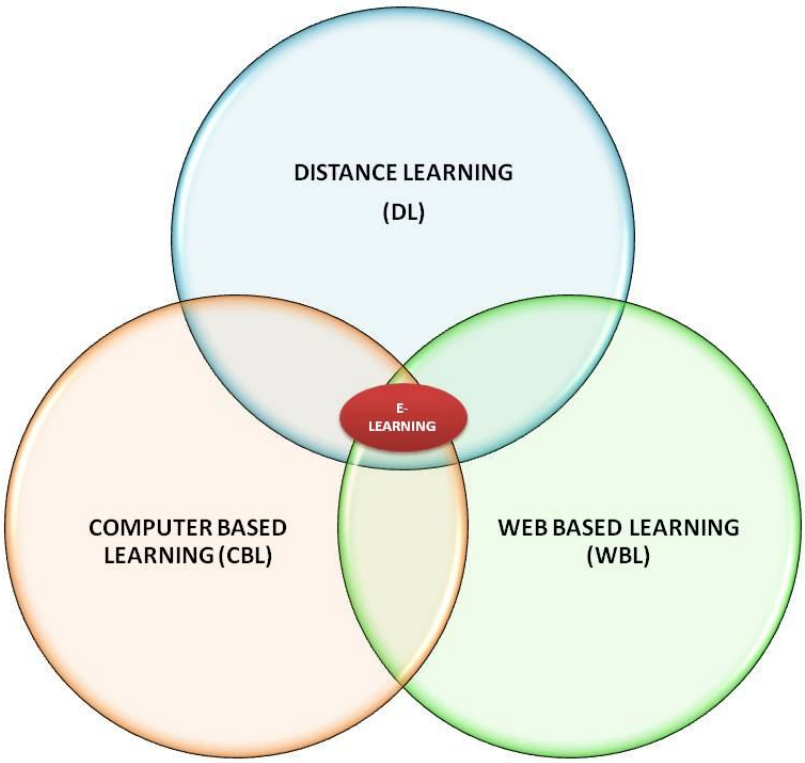


Figure 2. The eLearning model
(In the wake of Komenczi [17] by: Ildikó Miskolczi)

The role of man (instructor) won't decrease, but change. To adopt to the method of learning, virtual mentors will be established (Virtual Mentor-VM), who help students with interactive instructions in a well structured and synchronized multimedia-based eLearning environment. The main properties of the virtual mentors are the support of the multimedia, interactivity, real-time availability, management, flexibility, intelligence. [18]
Ilma Kovács [19] give great importance to the student and learning centralization, the system-view and process organization, to the point of contact and the presence of the framework, and external-internal marketing, the convergence of the old and the new elements. According to Ilma Kovács the eLearning [20]: *„... the term e-learning covers complex content, because it contains complex processes, which on the one hand learning, on the other hand teaching, and the third hand mean organization/organizational problems, and which can be realized only by informational and communicational technologies. On the one hand the e-learning is a new form of learning-teaching, which is able to included in the organized educational system, on the other hand, is a new mode and tool of teaching/learning, which can serve individual needs through the new e-learning environment – compared to traditional learning environment that is implemented by conventional means – because of its specificity. The latter, we also call non-formal, independent, personal discoverer learning."*[5]

THE NEWEST E-LEARNING OPPORTUNITIES OF DISTANCE LEARNING IN THE 21ST CENTURY

At the beginning of the 21st century, the platform of e-learning is the web, the World Wide Web. The World Wide Web, as the biggest, the world surrounding network and application of services, is now natural and accepted in the process of learning. With this the personal

[5] Translated by author.

learning environment (PLE) expands significantly, because we can use modern web-tools and services in the learning, with the help of that the applicable knowledge (but often quickly become obsolete) can be reached in a short time.



Figure 3. Determining factors of learning environment in the 21st century [6]



Figure 4. The learning process of the factors affecting[7]

The cloud technology, as a revolutionary new opportunity in the education, uses these options and factors. But what is the cloud technology? According to The National Institute of Standards and Technology (NIST):

[6] Picture from http://www.articulate.com/rapid-elearning/3-things-to-consider-when-building-your-e-learning-courses/
[7] Picture from http://langwitches.org/blog/2009/04/21/connecting-colaboracion-kommunikation-across-languages-cultures/

„A comfortable model, which allows you to use network access through a shared computer store of source or energy, and the fast using of the applications with minimum costs." [21]
What is the cloud? The cloud helps to construct, synchronization, update the web connections, and it helps to extend the boundaries of our capabilities. It can operate as a virtual storey, automate the processing. In a technical sense it is not other than servers, links, software, and networks.

In the course of this, the various tools and applications on the web, you can use so, that you need not download to your own computers, so you don't burden your own resources. The required applications can be used in the virtual space (on the web) for a small rental fee or free, that is provided by service providers.

Using this opportunity, the new method was born in higher education with the name of *cloud pedagogy*. The main characteristic of it that we can use the performance of computers, (we call cloud) and a part of them can be reached in the virtual space, while we release our own resources. In this way, the cloud technology can help to increase the efficiency in the field of education too. (Just think that when in the 21st century, we set our own portfolio, it is nonsense to collect on a sheet and represent all our activities in today's digital world.) Specially this is true in the case of a teacher, because he can refer to the digital formed syllabuses only, if the link their availability via the Internet. In life, this means that we mark and collect every platform, where our manifestations are present.

According to Cohen, there are more types of the educational clouds: [22]

- Public cloud
  - An open, publicly accessible cloud computing environment
  - Free of charge or in return for rent can be used
  - Individuals and organizations may use
- Your own cloud
  - Custom-designed and crafted cloud environment
  - Closed, the network is protected by an internal firewall
  - Highly reliable
  - Can be operated with high costs
- A hybrid cloud
  - A combination of the positive technology of the previous two
  - The basis of the formation of industry standards

The development of the cloud services can be isolated in three major sections, which make up models on the basis of their services. On the basis of these, the services of the cloud can be listed into three major models: [23]

- IaaS (Infrastructure as the service)
  - The most basic model
  - Users in the end work in a network
  - The server, operating system will be the mover of the cloud (network)
- Paas (Platform as a service)
  - The next level of development, when the application environment provides the cloud for the user
  - It's advantage, that a functional environment can be construct with the help of it
- Saas (Software as a Service,)
  - Currently the highest level of technology
  - It means the using of task- and job applications

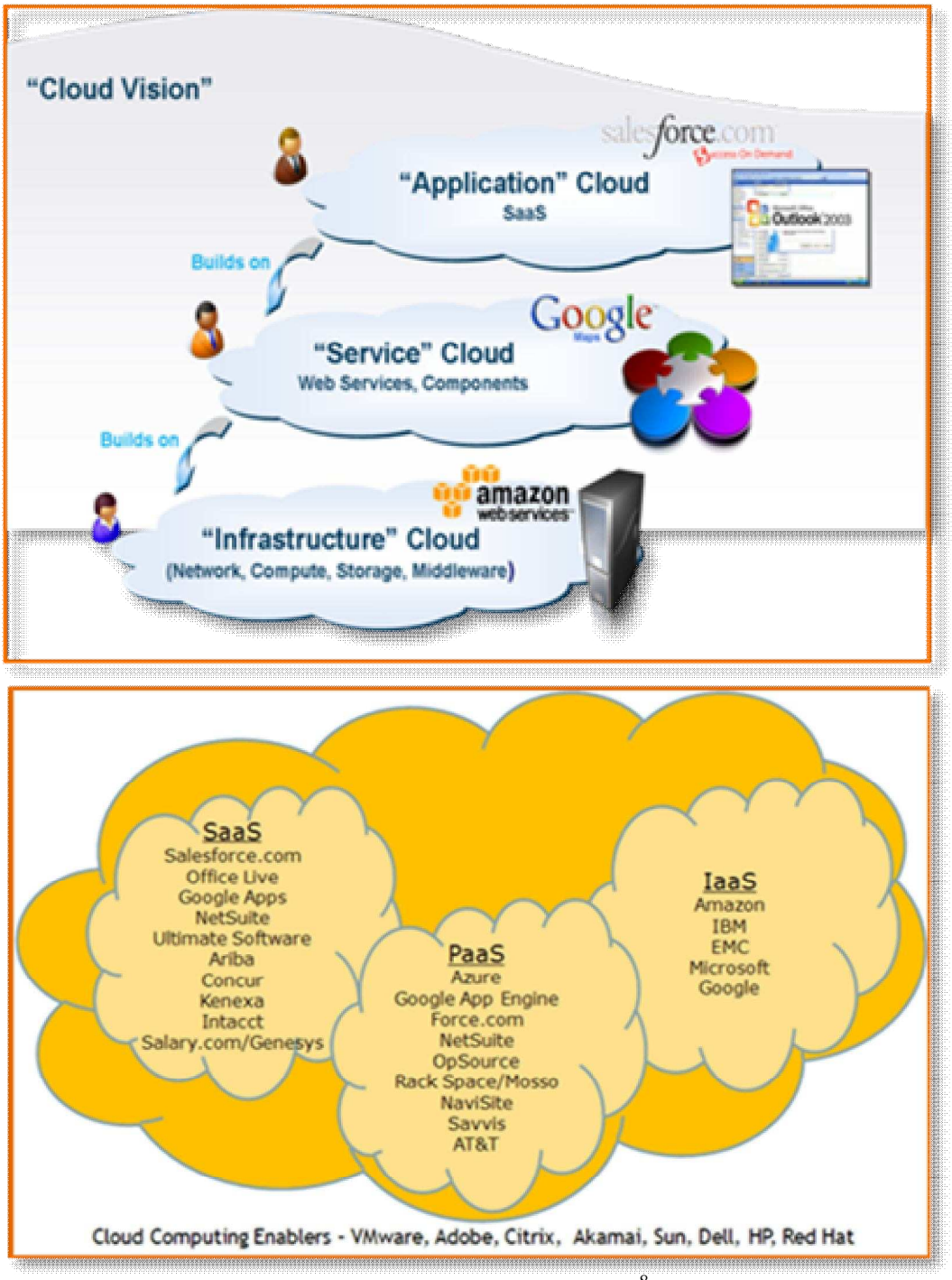


Figure 5. The cloud services[8]

The cloud computing technology, such as the complex entirety of web-based set of services, has only a couple of years old history. The appearance and the application in the education is only option today, but tomorrow will be mandatory. Not only the use of the technology extends rapidly on the different fields of life and in the education too, but it is also developing, changing, expanding with more and more services and applications. This makes it

[8] Pictures from: http://kasunpanorama.blogspot.com/2010/07/understanding-cloud-computing-feel-easy.html and http://www.trigent.com/technology/cloud.htm

necessary to examine, what kind of advantages and disadvantages this drawbacks of this technology is involved in education (too).

The advantages of the cloud technology: [24]

- Reduce costs (the programs are running in the cloud and not on your computer)
- Better performance (less memory consumption, the programs operate more efficiently)
- Reduced software costs
- Update of SaaS software is now no problem (usually automated)
- Virtually unlimited storage capacity
- Secure data storage (the collapse of the "computer" doesn't compromise the availability of data)
- Document access (we don't have to carry on with us, only have to sit down by a machine at anytime, anywhere)
- Not computer addicted applications and services

Disadvantages of the cloud computing technology: [24]

- We need internet connection to access the cloud
- Some softwares and software applications don't run in cloud (compatibility issue)

Although the cloud technology itself is a very young methodology in the history of eLearning, but many providers provide opportunities through their applications to use. Such service providers are for example Yahoo, Amazon, Microsoft, Hotmail, or Google. On the following pictures can be shown the cloud of the Google, which can be used free of charge and the services, applications that are provided by the cloud.



Figure 6. The "older" Google services[9]

[9] Picture from http://indolaw.alafghani.info/2010/05/6-free-collaboration-tools-for-lawyers.html

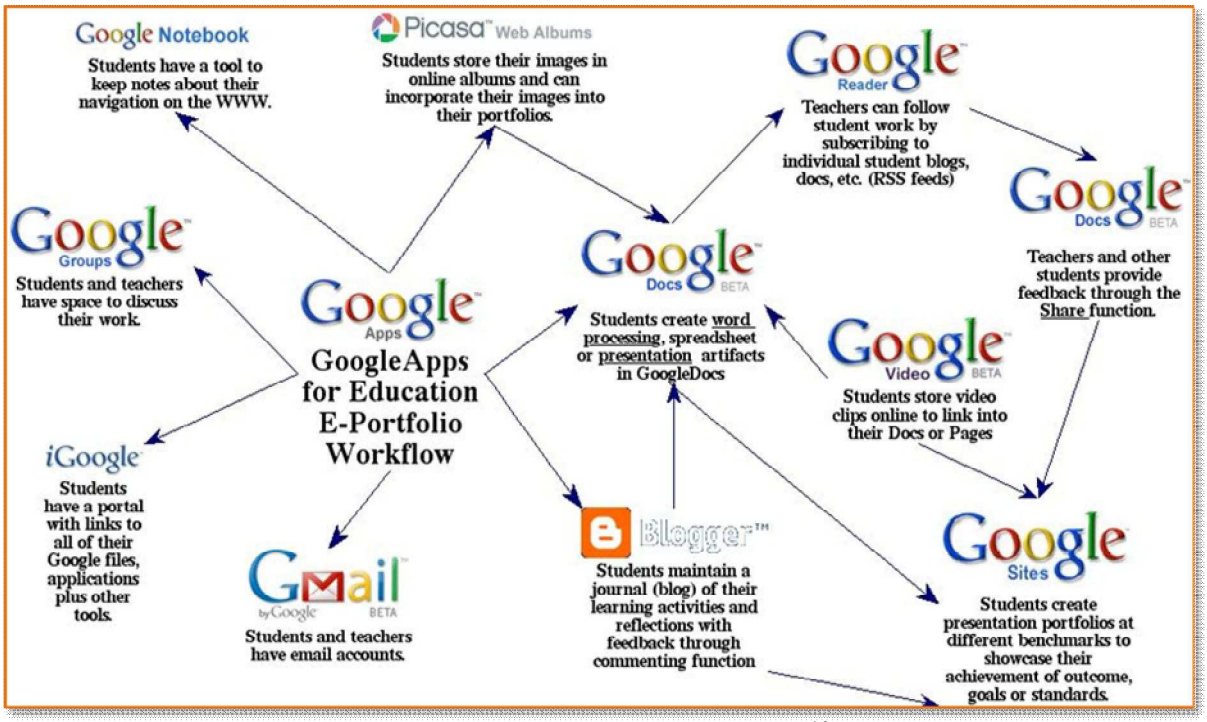


Figure 7. The great Google cloud[10]

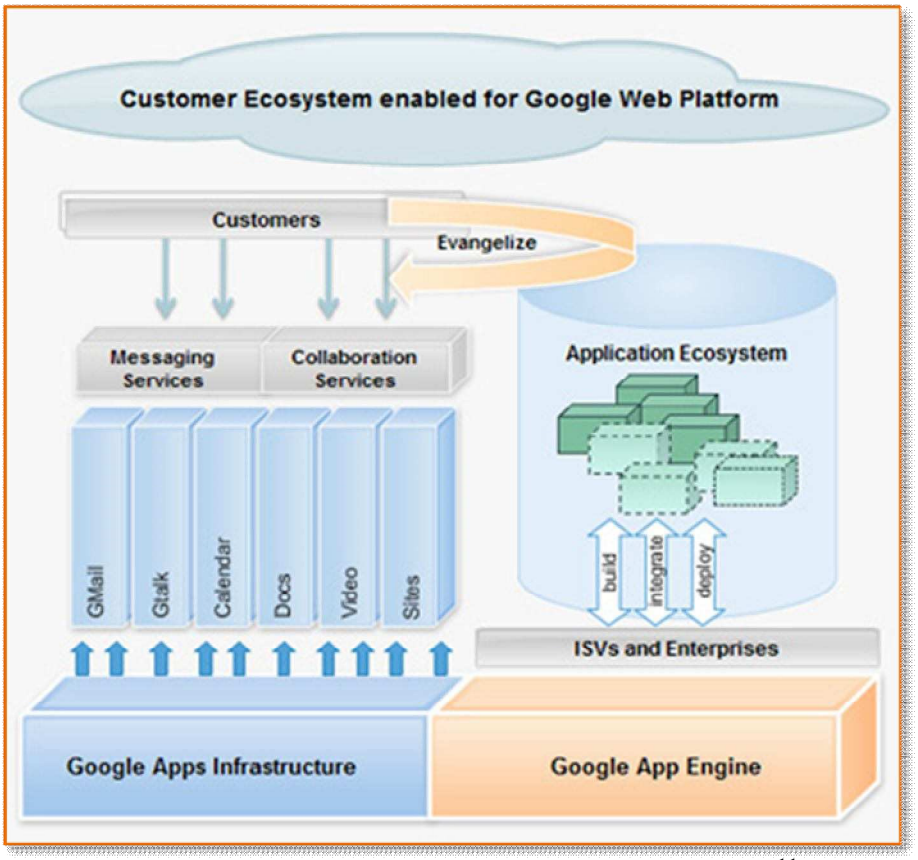


Figure 8. The web-platform of Google Apps Cloud[11]

[10] Picture from http://www.hwsw.hu/hirek/37167/google_microsoft_office_apps_wahington_online_irodai_szoftver.html
[11] Picture from http://www.persistentsys.com/Offerings/SaasCloudComputing/GooglePlatformServices/tabid/454/Default.aspx

SUMMARY

In the societies, the explosion of the informational revolution has brought with itself the development of the ICT tools at the end of the last century. In almost all segments of our lives have developed the e-technologies, so that the eLearning in the field of the education. This modern method of distance learning is now makes the education possible to be independent from space and time. At the dawn of the 21st century, the concept of distance learning has undergone and it is passing through important content changes, its conceptual class is continuously changing and expanding. The eLearning has been published and it's now an integral part of the distance learning. Virtually all of us use the eLearning every day, even if we aren't aware of this. Today, there is almost nobody, who does not use a computer daily, or iPod, or the I Phone to the working process or obtain information. Of course, the high-skilled computer use is an essential element of this process, and it is called digital literacy. For the young "digital" generation, this is not a problem, because a generation has been grown up to the higher education system, whose life there wasn't a period when they didn't have computer and Internet. The existence and application of these tools is natural for them. However, the older generations necessarily use ICT tools too, even through the daily working process or their everyday life.

Distance learning is an important part of the educational structure of our world and its importance and weight will grow in the near future. Modern distance education allows you to apply the totally new method of education (eLearning), with the using of the acquits of the age. We can speak about the eLearning, as one of the most modern type of learning, in more than one sense (mode, design, methodology, technique). Today, the distance learning is inspired by a new spirituality, the *constructivist and connectivist approach*. The *network-based learning* is emphasized, which main pillar is, that the content of the education and the participants are present (locally) in the various spaces, and they meet with each other and they carry out their views to each other, opinions about some of the topics in the virtual space. The students don't learn in an isolated way, but in close relationship with each other, and from each other. The tutor's role has been slightly changed, and he doesn't direct, but also coordinate the learning process. He doesn't provide the knowledge, but also he shows how to get the knowledge. He coordinates how we can build up applicable, on fresh results of research based knowledge from much information. The connectivist distance learning considers the elements cornerstones in the educational system, such as: [25]

- real-time broadcast; picture and sound
- online common document-editing;
- opportunity of common Web date talks with calendar function;
- using of Web document library;
- using of Web syllabus wall;
- operation of Web Whiteboard;
- construction and operation of student forums;
- chat "rooms";
- online exam;
- online presentations;
- online teaching, consultations;
- wiki;
- feedback;
- community tasks;
- blog;
- games…

Today is published and rapidly spreading – not only in the field of education – the *cloud computing technology* (cloud, cloud computing technology), which build on the largest network on the Web. Thus, the electronical education is also changing, and the web1.0 technology is replaced by the revolution of web2.0 technology. Now we don't read the digital contents only, but we are also involved in the creation of them. We create virtual communities, change opinion, make contents, share, reconstruct, reunderstand the knowledge. Thus we, students create the knowledge.

On the next step of the development, we will connect the various services of the cloud. A wide range of diverse data service providers will share informations with each other, creating a strong platform, which may be the basic of a totally cloud-based service, service executes. This is called *Rainbow Computing*, *Rainbow technology*. This requires a higher level of the communication, Internet culture and relations, which may called simply a NetIQ.

Age of Gutenberg is over in the education.

Bibliography

1. TAPSCOTT, Don. Grown Up Digital: How the Net Generation is Changing Your World. USA: McGraw-Hill Companies, 2008. ISBN: 9780071508636.

2. Bertalan, KOMENCZI. Az E-learning lehetséges szerepe a magyarországi felnőttképzésben (The possible role of E-learning in adult education in Hungary) (research). www. nive. com [Online], 2006. [Reference: 10 August 2010.] https://www.nive.hu/konyvtar/content/edoc/files/03_komenczi.pdf .

3. John TIFFIN, Lalita RAJASINGHAM. Education in an Information Society. London, New York, 1995, Search Of The Virtual Class, p. 88.

4. Ilma, KOVACS. Új út az oktatásban? (New way in education? The distance learning.) Budapest, Budapest University of Economics Academic Coordination Office, 1996. ISBN: 159 503 9 963.

5. George SERES, and less. Hipermédia az oktatásban – avagy felhőpedagógia. Hogyan vált az elektronika az oktatás tárgyából annak színterévé? (Hypermedia in education – cluod learning. How to become the subject of education electronics to provide?) www.hadmernok.hu [Online], June 2010. [Reference:18 September 2010.] http://hadmernok.hu/2010_2_seres_etal.pdf. ISSN 1788-1919

6. George SERES, George KENDE, Ildikó MISKOLCZI. Tanuljunk könnyen, gyorsan, élethosszig, bárhol, bármikor (Let's learn easily and quickly-anytime, anywhere, in the area). Jampaper. [Online], 2008. [Reference: 16 September 2010.] http://www.jampaper.eu/jampaper_h-arc/2008._iii._3.sz._files/jam080302e.pdf . 3./III./2008. ISSN 1789-6967.

7. György SERES, György KENDE, Ildikó MISKOLCZI. Let's learn easily and quickly-anytime, anywhere, in the area. Jampaper. [Online], 2008. III. class 3. number.

[Reference: 16 September 2010.] http://www.jampaper.eu/jampaper_e-arc/no.3_iii._2008_files/jam080302e.pdf . ISSN 1789-6967.

8. Bertalan, KOMENCZI. Az E-learning lehetséges szerepe a magyarországi felnőttképzésben (The possible role of E-learning in adult education in Hungary) (research). www. nive. com. [Online], 2006. [Reference: 10 August 2010.] pp. 15-16. https://www.nive.hu/konyvtar/content/edoc/files/03_komenczi.pdf .

9. Bertalan, KOMENCZI. Didaktika elektromagna? Az e-learning virtuális valóságai (Didaktica electromagna? The e-learning virtual realities). 2004. 11. a new Pedagogy, Inspection, pp. 31-49.

10. Ilma, KOVÁCS. “Mesterségek” és elvárások" – elektronikus tanulás (Crafts" and expectations (electronic learning)). www.epa.oszk.hu. [Online], 2009. november. [Reference: 7 September 2010.] http://epa.oszk.hu/01200/01251/00003/pdf/fef_szemle_200901_149-160.pdf . III. class 1. number.

11. Zsolt, KULCSÁR. Hálózati tanulás (Network learning). Inforrmatics-Education. [Online], 2009. 1. number, pp. 4-16. [Reference: 20 July 2010.] http://www.oktatas-informatika.hu/20091szam-online.html . ISSN 2061-1870.

12. Zsolt, KULCSÁR. A negyedik oktatáspardigma. (The fourth learning-paradigm). Slideshare. [Online], 2009. [Reference: 26 March 2010.] http://www.slideshare.net/kulcsi/a-negyedik-oktatasparadigma .

13. Viktor, BEDŐ. Magyar Virtuális enciklopedia (Hungarian Virtual Encyclopedia). [document] Budapest: MTA, 2009. on 17 March. http://www.enc.hu/1enciklopedia/fogalmi/inf/halozatkutatas.htm .

14. Bertalan, KOMENCZI. Elektronikus tanulási környezet. (Electronic learning environment. An attempt to analyse the phenomenon didactica). Habilitant treatise. Debrecen, 2007.

15. Ilma, KOVÁCS. “Mesterségek” és elvárások, - bővített változat ("Jobs" expectations and e-learning). in: Electronic Periodical archive on adult education (I) Survey, pp. 141-160. [Online], 2009. november. [On August 25, 2010.] http://epa.oszk.hu/01200/01251/00003/pdf/fef_szemle_200901_149-160.pdf .

16. Ildikó, MISKOLCZI. Egy interaktív e-learning portál első tapasztalatai egy e-diák szemszögéből (The experience of an eLearning course) presentation and performance of the MTA and the Committee of the School of management, knowledge management Sub-Committee on 2008. workshop per year. [Online], 2008. March. [Reference: szetember 10 2010...] http://vati.szie.hu/node/161

17. Bertalan, KOMENCZI. Az információs társadalom iskolájának jellemzői (The characteristics of the schools of the information society). Institute of educational research and development. [Online], [By: 20 June 2010.]

http://www.oki.hu/oldal.php?tipus=cikk&kod=informatika-komenczi-informacioshttp://www.oki.hu/oldal.php?tipus=cikk&kod=informatika-komenczi-informacios

18. DONGSONG Zhang Zhao, j. LEON Zhou, Lina, NUNAMAKER, Jay f., Jr. Can replace e-Learning classroom learning? Communication of the ACM. [Online], vol. 47, no. 5. pp. 75-79, 2004. in May. [Reference: 1 October 2010.] www.portal.acm.org. http://210.240.189.212/dctelearning/type_resources/01_papers/9612_digital_papers/2_english/bit095110/can%20e-learning%20replace%20classroom%20learning.pdf .

19. Ilma, KOVÁCS. Távoktatás és hozzáférés (Distance learning and access. Adult education inspection), pp. 9-120. [Online], 2008. March. II. class 1. number. [Reference: 10 September 2010.] http://epa.oszk.hu/01200/01251/00002/pdf/fef_szemle_200801_096-120.pdf .

20. Electronic learning, 274 p. 74 p.. Budapest: tomorrow's Publisher.

21. Agatha, GILMORE. Learning in The cloud site. : Chief Learning Officer, from EBSCO www.clomedia.com database. Feb2010, Vol. 9 Issue 2, p32-35, ISSN: 1935-8148

22. Erica, ORANGE. Mining information from the Data clouds. Bethesda, USA: World Society, 2009 Fututre. July-August. The futurist. from EBSCO database www.wfs.org. Jul/Aug2009, Vol. 43 Issue 4, p17-21, ISSN:00163317

23. Dave, BURKEE. Why cloud computing will never be free? site: queue.acm.org, communications of the acm, 2010. 05. Practice, 5. volume. from EBSCO database. May2010, Vol. 53 Issue 5, p62-69, ISSN:00010782

24. Doron, KAMINSKI. A walk in the clouds. Canada: CMA Management, from EBSCO database. Apr2010, Vol. 84 Issue 2, p41-42, ISSN:14904225

25. George, KENDE - George, SERES - Ildikó,MISKOLCZI - Christina, FÓRIKA - Gábor HANGYA. Virtuális campus - az e-tanulás lehetőségei a külszolgálatot teljesítő katonák képzésében (Virtual Campus - opportunities of e-learning for the training of soldiers). Szolnok: in the scientific magazine online, Communications of science of fly, 2008. ZMNE. http://www.szrfk.hu/rtk/kulonszamok/2009_cikkek/kende_gyorgy-miskolczi_ildiko_stb.pdf . ISSN 1417-0604

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Seres György
drseres@drseres.com

FENNTARTHATÓ FEJLŐDÉS – FENNTARTHATÓ NEMZETVÉDELEM

Absztrakt

A tanulmány a fenntartható fejlődés és a fenntartható nemzetvédelem fogalmát, rendszerelméleti eszközökkel elemzi és definiálja: „A veszélyeztetettséggel arányos nemzetvédelmi rendszer létrehozása a veszélyeztetettség növelésének kiprovokálása, illetve a gazdasági, a társadalmi és a természeti környezet károsítása, valamint fenntartható fejlődésének megakadályozása nélkül."

The study analyzes notion of sustainable development and sustainable national defense with tools of system theory, and define it: "Create a national defense system which is proportional to dimension of endangerment, without increasing of endangerment, or damaging of economical, social and natural environment."

Kulcsszavak: *fenntartható fejlődés, fenntartható nemzetvédelem, rendszerelmélet, katonai rendszerek modellezése ~ sustainable development, sustainable national defense, system theory, modeling of military systems.*

A „VALÓSÁG” című folyóiratban egy rendkívül érdekes tanulmány jelent meg 2004-ben, Turchany Guy és professzortársai tollából: „A fenntartható fejlődés: mítosz vagy valóság?” címmel [1]. A szerzők újszerűen közelítik meg a fenntartható fejlődés – manapság rendkívül divatos – fogalmát. Különösen figyelemreméltó a kultúra és civilizáció fejlődése és növekedése közti összefüggések elemzése, illetve a vizsgálat dimenzióinak kiterjesztése a fejlődés és a növekedés negatív tartományaira.

A FENNTARTHATÓ FEJLŐDÉS ÉS A HÁBORÚK

A fenntartható fejlődésnek van egy olyan aspektusa, amelyre a tanulmány csak utalást tartalmaz: *„Vagy létezünk, s akkor magasra törekszünk, vagy nem törekedhetünk magasra — mert például katonai vagy gazdasági kényszerek merő vegetatív szintre korlátoznak bennünket —, s akkor létezésünk azonnal kérdésessé válik.”*

Igen! A háború és a hadsereg – bármennyire is szeretnénk ezt elfelejteni – elválaszthatatlan részét képezi a kultúrának és a civilizációnak, amióta az ősember először használta a kőbaltát a szomszéd törzs területének vagy vadászzsákmányának megszerzésére.

Az emberi kultúra és a civilizáció a területileg, vagy etnikailag elkülönült embercsoportok – államok, népek, vallási csoportok – kultúrájának és civilizációjának egymásra épüléséből és keveredéséből alakult ki. A történelem során egy-egy kultúra és a civilizáció *fejlődésének fenntarthatóságát* – azt, hogy hogyan, és milyen mértékben épült be az egyetemes kultúrába és civilizációba – igen gyakran éppen a háború és a hadsereg döntötte el.

Néhány kiragadott példa.

Gondoljunk csak a háborúk által elpusztított ókori városállamokra, vagy a spanyol hódítók által feldúlt délamerikai indián birodalmakra, melyek kulturális és civilizációs eredményeiről jószerint csak a régészeti feltárások eredményeként szerezhettünk tudomást.

Az, hogy a modern Európa elsősorban a római kultúra és civilizáció hagyományain alapszik, és nem a jóval korábbi görög, vagy egyiptomi mintákon, (például, az európai egyetemeken ma is alaptárgy a római jog), az a római légiók hadjárataival is nagymértékben összefügg.

De az Európai Unió létrejöttének előzményei között is jelentős szerep jutott a napóleoni háborúknak, illetve a francia-német szembenállás – az első és a második világháborúban kicsúcsosodó – tragikus következményeinek.

A növekedés korlátait szemléletesen mutatja meg az Egyesült Államok és a Szovjetunió között folyó fegyverkezési verseny „eredménye” – a reageni „csillagháborús” program csúcspontja után a szovjet birodalom összeomlott.

Végül, a fenntartható fejlődés érdekében létrejövő világméretű nemzetközi összefogásnak – így az Agenda 21-nek is – mintául szolgált a Hirosima emlékét nem feledő nagyhatalmak kezdeményezésére született atomcsend egyezmény.

Több kutató is felhívja a figyelmet a háború, a béke és a fenntartható fejlődés szoros kapcsolatára.

David Krieger, például ezt írja: *„Ahhoz, hogy felmérhessük a béke és a fenntartható fejlődés kilátásait, figyelembe kell vennünk korunk politikai, gazdasági, katonai és kulturális irányzatait”*[1] [2]

Tobias Damjanov így fogalmaz: *„Ha fenntartható fejlődést akarunk megvalósítani, akkor a biztonság kérdését feltétlenül számításba kell vennünk. Ha kifejezetten a biztonság ha-*

[1] "In order to assess the prospects for both peace and sustainable development, we must take into account the broad global trends of our time: political, economic, military and cultural.”(a szerző fordítása)

gyományos értelmezésére koncentrálunk – ez a katonai meghatározás –, azt kell megvizsgálnunk, hogy a hadsereg összeegyeztethető-e a fenntarthatósággal."[2] [3]

Az ENSZ 1992-es rio-i konferenciája jegyzőkönyvének [4] 24. alapelve pedig kimondja: *„A háború önmagában rombolja a fenntartható fejlődést. Ezért az államok a fegyveres konfliktusok alkalmával figyelembe fogják venni a környezetvédelemre vonatkozó nemzetközi jogi előírásokat, és ha szükséges, együttműködnek annak továbbfejlesztésében."*[3]

Mindezek ellenére, a fenntartható fejlődés elemzéséhez az ENSZ által ajánlott „indikátorok" között [5, 6] a nemzetvédelemmel kapcsolatos mutatóval nem találkoztunk.

Úgy gondolom, ezek az argumentumok kellően alátámasztják azt az igényt, hogy a fenntartható fejlődés kutatásánál a *fenntartható nemzetvédelem* kérdései is szerepeljenek.

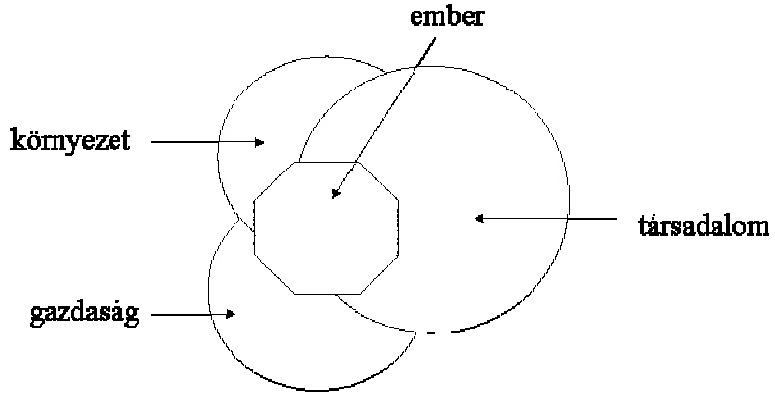
Ezt indokolja a „VALÓSÁG"-ban megjelent tanulmány egy másik megállapítása is: *„Mivel minden egyes jelenségcsoport több kontextusban vizsgálható, ugyanannak a jelenségcsoportnak annyi meghatározása lehet, ahány összefüggésben tanulmányozzuk."*

A FENNTARTHATÓ NEMZETVÉDELEM

A fenntartható nemzetvédelem kutatását azzal kell kezdenünk, amivel minden új terület feltárását. Tisztáznunk kell, hogy mivel is akarunk foglalkozni – fel kell állítanunk egy munkadefiníciót. Ahogyan a Turchany tanulmány fogalmaz: *„... a kutatásra kiválasztott kontextushoz tudatosan kapcsolt hipotetikus definíciót nevezzük munkadefiníciónak. A munkadefiníció sem egyetemesen, hanem viszonylagosan (kontextushoz kötötten) és feltevésszerűen körvonalazza a bennünket érdeklő jelenséghalmazt."*

Először néhány fogalmi pontosítást fogunk bevezetni, hogy a kutatás végén – remélhetőleg – eljuthassunk az egzakt matematikai modellek megalkotásáig.

Az idézett tanulmány 3. ábráján az embert három rendszer veszi körül: a társadalom, a gazdaság és a környezet (1. ábra):

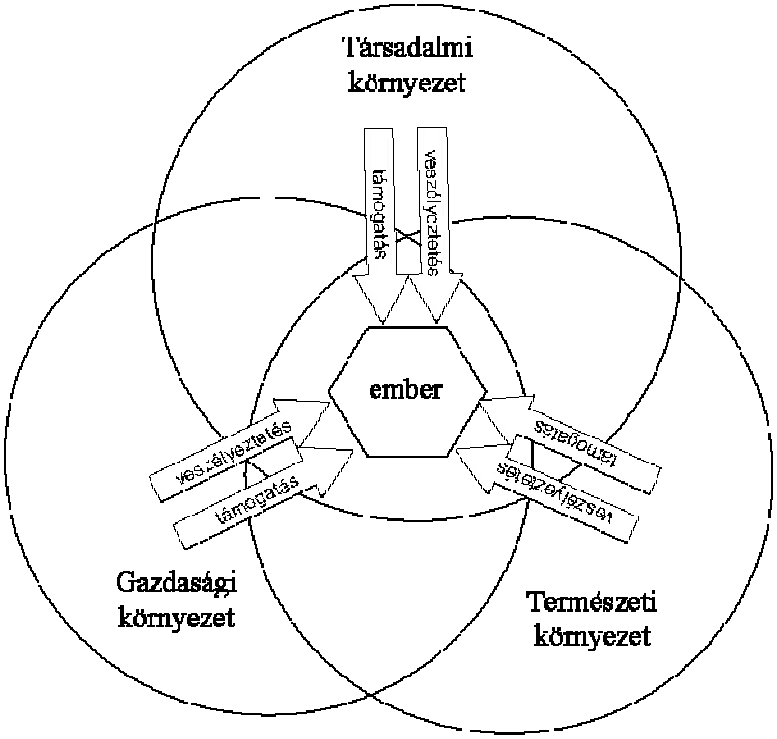


1. ábra

Ebben a megközelítésben – és a manapság általánosan alkalmazott terminológiákban – környezet alatt mindig a természeti környezetet értik. Ez a terminológia a kutatásunk alapvető módszerének választandó rendszerszemlélet szempontjából félreérthető lenne, ezért kiindulásként a 2. ábrán vázolt modellt választjuk.

[2] „If you want to implement sustainable development, the question of security is certainly on the agenda. Focusing more specifically on the traditional understanding of security – that is the military definition – it has to be examined whether or not the military complies with sustainability." (a szerző fordítása)

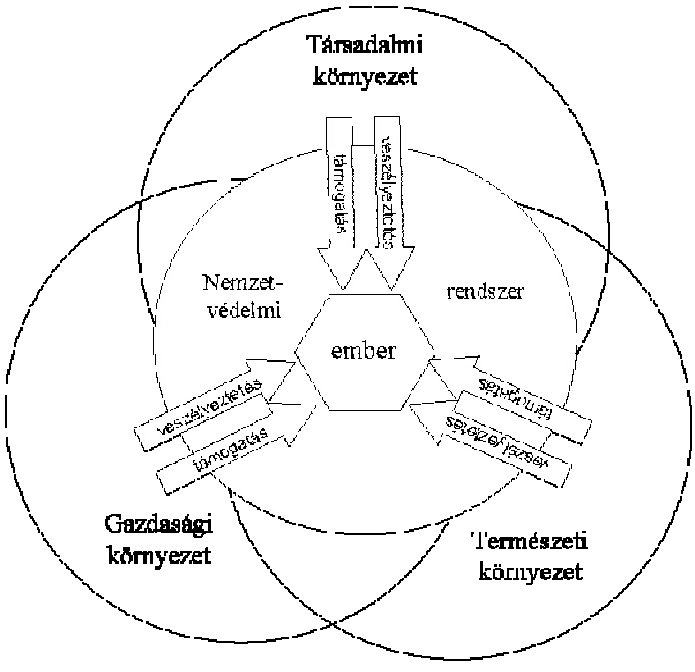
[3] "Warfare is inherently destructive of sustainable development. States shall therefore respect international law providing protection for the environment in times of armed conflict and cooperate in its further development, as necessary." (a szerző fordítása)



2. ábra

Az általános rendszerelmélet szerint egy rendszer környezete minden, ami a rendszeren kívül van. Mivel az ember része mindhárom, őt körülvevő rendszernek része, ezért mindhármat környezetnek – társadalmi, gazdasági, illetve természeti környezetnek – tekintjük. Ennek megfelelően, az embert mindhárom környezete részéről alapvetően kétféle hatás éri: a támogatás pozitív, és a veszélyeztetés negatív hatása.

A vizsgálni kívánt rendszerünket, a nemzetvédelmet, ebben a modellben a 3. ábrának megfelelően helyezhetjük el.



3. ábra

A nemzetvédelmi rendszer célja az ember és környezete közti kapcsolat biztosítása olymódon, hogy a támogatással szemben transzparens legyen – ne csökkentse azok pozitív hatását, ugyanakkor a negatív hatásokat – a veszélyeztetést – a lehető legjobban mérsékelje.

Ezt a célt a nemzetvédelmi rendszer akkor tudja elérni, ha magába integrálja a legkülönbözőbb negatív hatásokkal szembeni védelmi rendszereket – a hadsereget, a nemzetbiztonsági szolgálatokat, a határőrséget, a rendőrséget, az igazságszolgáltatást, a katasztrófa-elhárítást, stb.

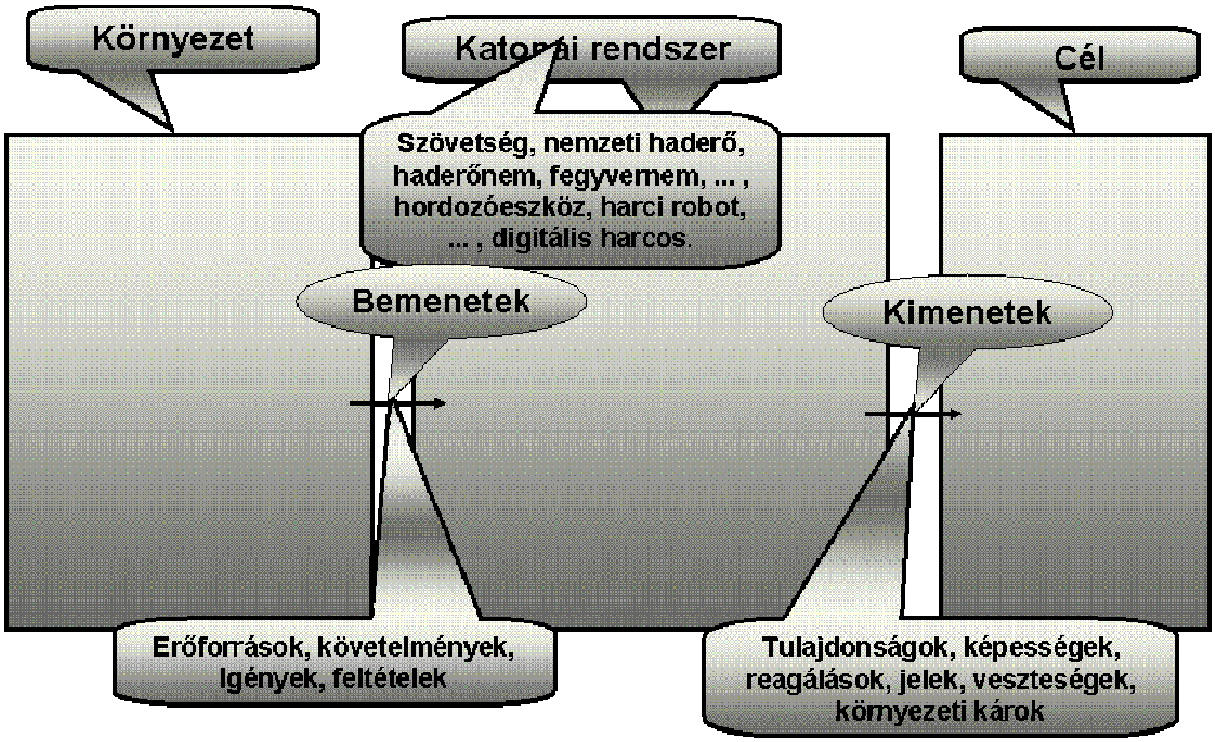
Ha a nemzetvédelmi rendszert a fenntartható fejlődés szempontjából kívánjuk vizsgálni, akkor meg kell határoznunk, mit értünk a fenntartható nemzetvédelem fogalma alatt. Első közelítésben a fenntartható nemzetvédelem munkadefiníciójaként az alábbit ajánljuk:

A veszélyeztetettséggel arányos nemzetvédelmi rendszer létrehozása a veszélyeztetettség növelésének kiprovokálása, illetve a gazdasági, a társadalmi és a természeti környezet károsítása, valamint fenntartható fejlődésének megakadályozása nélkül.

A nemzetvédelmi rendszer alrendszerei – a hadsereg, a nemzetbiztonsági szolgálatok, a határőrség, a rendőrség, az igazságszolgáltatás, a katasztrófa-elhárítás, stb. – más-más szerepet töltenek be az EMBER veszélyeztetettségének csökkentésében, és tevékenységük eltérő mértékben befolyásolja a fenntartható fejlődést. Ezért a fenntartható nemzetvédelem kutatása az egyes alrendszerek esetében különböző modelleket igényel. E tanulmány keretében a katonai alrendszer vizsgálatához ajánlunk egy modellt, melynek analógiájára – reményeink szerint – kidolgozhatók a többi alrendszer vizsgálatára alkalmas modellek is [7,8].

Egy rendszermodell a fenntartható nemzetvédelem katonai alrendszerének kutatásához

Annak érdekében, hogy a fenntartható nemzetvédelem katonai alrendszerének feladatait és folyamatait elemezni tudjuk, bemutatunk egy általános modellt (4. ábra).



4. ábra

A katonai rendszer fogalma

A modellben *katonai rendszer* alatt értünk minden szervezett erőt – szövetségi, nemzeti, haderőnemi, fegyvernemi szinttől a hordozóeszközökön és a robotokon keresztül az egyes fegyveres harcosig – amely adott *környezetben* katonai tevékenységet hajt végre meghatározott *cél(ok)* elérése érdekében.

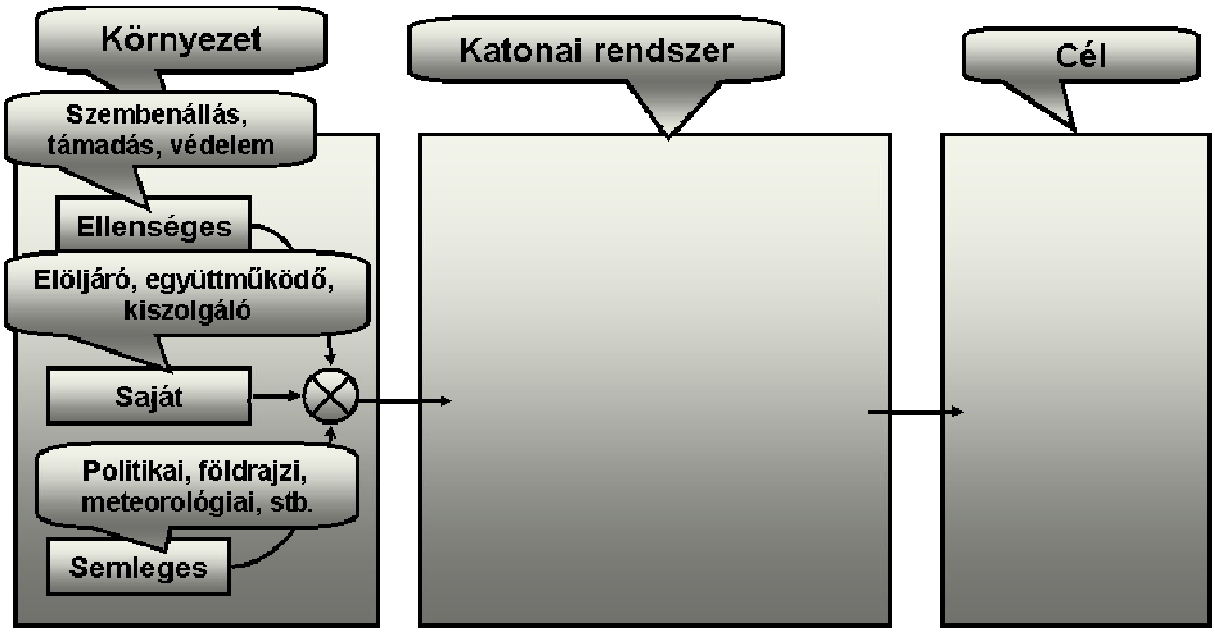
A rendszer bemeneteit a környezetéből érkező *erőforrások, követelmények, igények, és feltételek*, kimeneteit pedig a céljai elérését biztosítani hivatott *tulajdonságok, képességek, reagálások és jelek,* illetve a tevékenység során elszenvedett *veszteségek,* valamint a környezetnek okozott *károk* alkotják.

A katonai rendszer környezete

Egy rendszer vizsgálatát a környezetének leírásával kell kezdeni, mivel ez jelöli ki – határozza meg, vagy kényszeríti ki – az elérendő célokat.

Gondoljunk csak Napóleon és Hitler Oroszországi hadjárataira, a franciák és az amerikaiak vietnami kalandjára, vagy az arab államok Izrael elleni háborújára. Ezek kimenetele nem tükrözte a katonai erőviszonyokat, mivel a támadók figyelmen kívül hagyták a környezet hatásait – az orosz telet, a vietnami dzsungelt, a patriotizmust, illetve a diaszpóra segítségét.

A katonai rendszer környezete a tevékenység során *saját, ellenséges* és *semleges* elemeket foglal magába (5. ábra).



5. ábra

A *saját* környezetet az *elöljáró*, az *együttműködő* és a *kiszolgáló* rendszerek alkotják.

Ezek *követelményeket* illetve *igényeket* támasztanak a katonai rendszerrel szemben, valamint információk és technikai, illetve humán *erőforrások* formájában biztosítják a működéshez szükséges *feltételeket*.

Az *ellenséges* környezet lehet *szembenálló*, *támadó* és *védelmi*, a katonai rendszer tevékenységének jellegétől függően.

A katonai rendszerek *semleges* környezete a harctevékenység *politikai, földrajzi, meteorológiai, klimatikus, évszak, napszak, stb.* feltételeit határozza meg.

A katonai rendszer célja

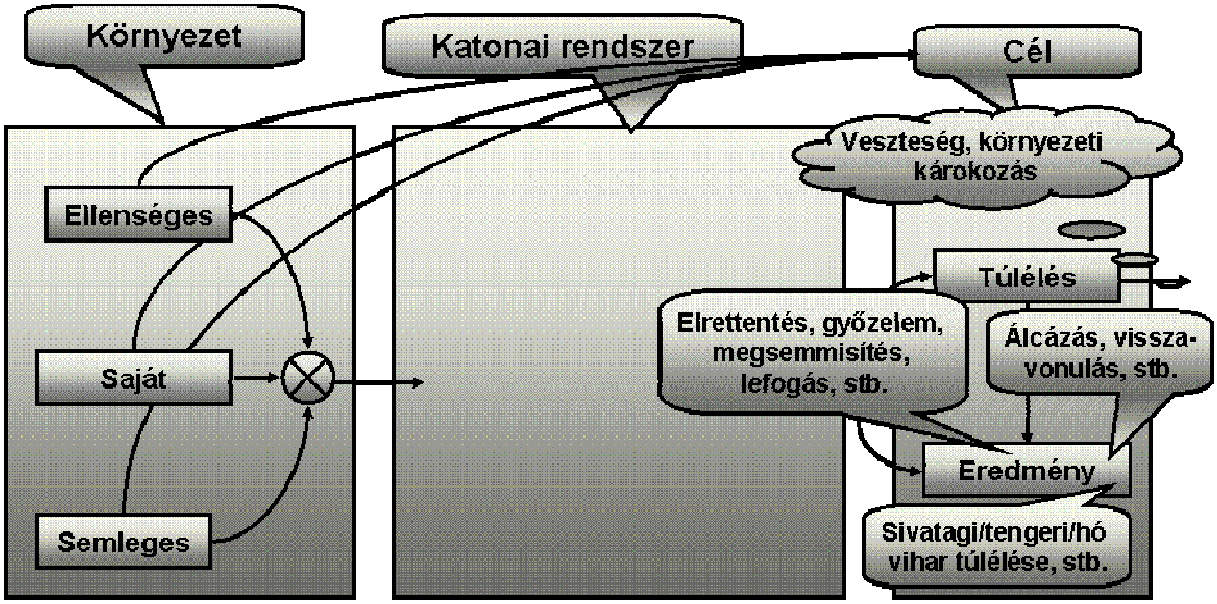
A rendszer vizsgálatának második szakaszában a környezete által meghatározott – kitűzött, illetve kikényszerített – célokat kell leírni (6. ábra).

Emlékezzünk az idősebb és az ifjabb Bush elnök Irak elleni háborújára. Az utóbbi céljának meghatározásakor az Egyesült Államok nem vette figyelembe a politikai környezet hatásait – az Európai Unió meghatározó hatalmai, Oroszország és a környező iszlám országok reakcióit, illetve az iraki vallási és etnikai közösségek erőviszonyait.

A katonai rendszer céljait alapvetően a környezete határozza meg (kivéve a katonai puccs esetét, amikor a rendszer egyes elemei önállósítják magukat, és céljaikat saját maguk határozzák meg). A *cél* mindig valamilyen *eredmény* elérése és - egyes kivételektől eltekintve - a rendszer *túlélésének* biztosítása a *veszteségek* és a környezetnek okozott *károk* minimalizálásával.

A *saját* – elsősorban az elöljáró, vagy együttműködő – környezet által kitűzött célok, a katonai rendszer szintjének megfelelően, olyan *eredmények* lehetnek, mint például: *az elrettentés, a győzelem, a megsemmisítés, a lefogás, katasztrófa-elhárítás,* stb.

Az *ellenséges* környezet is rákényszerítheti – a túlélés érdekében – a katonai rendszereket olyan célok elérésére, mint például: *az álcázás, a sugármentesítés, a visszavonulás*, stb.



6. ábra

A *semleges* környezet is határozhat meg olyan célokat a katonai rendszerek számára, mint például: *sivatagi, tengeri, vagy hóvihar túlélése*, stb.

A katonai rendszernek a céljai elérését biztosítani hivatott *tulajdonságok, képességek*, *reagálások és jelek* mellett a tevékenység során elszenvedett *veszteségek,* valamint a környezetnek okozott *károk* a rendszer nemkívánatos *kimeneteit* alkotják, amelyek csökkentik a *túlélés* esélyeit, illetve az *eredmény* értékét.

A katonai rendszer struktúrája

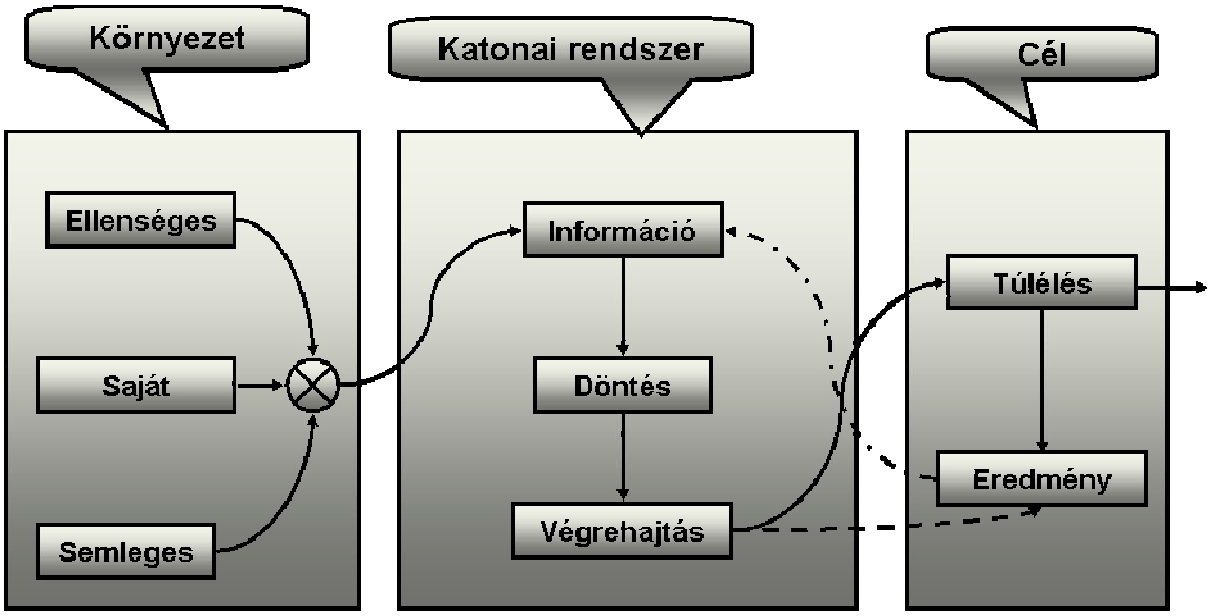
Egy katonai rendszer struktúrája alatt, a hagyományos megközelítés szerint általában az alrendszereket, azok elemeit és a köztük, illetve a környezetével fennálló kapcsolataik felépítését értjük. Egy nagy katonai rendszer vizsgálatához ezek szerint nem kellene mást tennünk,

mint az *információszerző*, a *döntési* és a *végrehajtó* alrendszereket elemeikre bontanunk és leírni az alrendszeren belüli, illetve a környezettel fennálló kapcsolataikat. Ez a megközelítés azonban nem adna teljes képet a katonai rendszer működéséről, mivel az ilyen funkcionális modell nem, vagy csak felszínesen, mutatja meg a rendszeren belül megoldandó feladatok egymásra épülését és kapcsolatait, illetve elfedi azok szervezési rendjét. Egy bonyolult katonai rendszerben egy-egy alrendszerre, illetve elemre többféle funkcionális feladat megoldása is hárul, egy-egy feladat megoldása pedig megoszlik az egyes elemek között.

Például, ha egy légvédelmi rakéta alegységet a légvédelmi rendszer elemének tekintünk - márpedig annak kell tekintenünk -, nehéz eldönteni, hogy a légvédelmi rendszer melyik alrendszerébe soroljuk be. Első közelítésben azt mondhatnánk, hogy természetesen a végrehajtó alrendszerbe tartozik. Egy légvédelmi rakéta alegység azonban maga is egy bonyolult rendszert alkot. Az alegység felderítő és célmegjelölő radarja információszerzési, harcálláspontja döntési feladatokat old meg, rakéta rávezető rendszere pedig a légvédelmi beavatkozás végrehajtását végzi. Ez utóbbi, emellett, maga is megold információszerzési és döntési feladatokat.

A rendszerben lévő emberek helyzete még bonyolultabb, hiszen még egy radarkezelő is legalább két alrendszer feladataival foglalkozik, egy repülőgép-vezető pedig betölthet információszerzési, döntési és végrehajtó funkciót is.

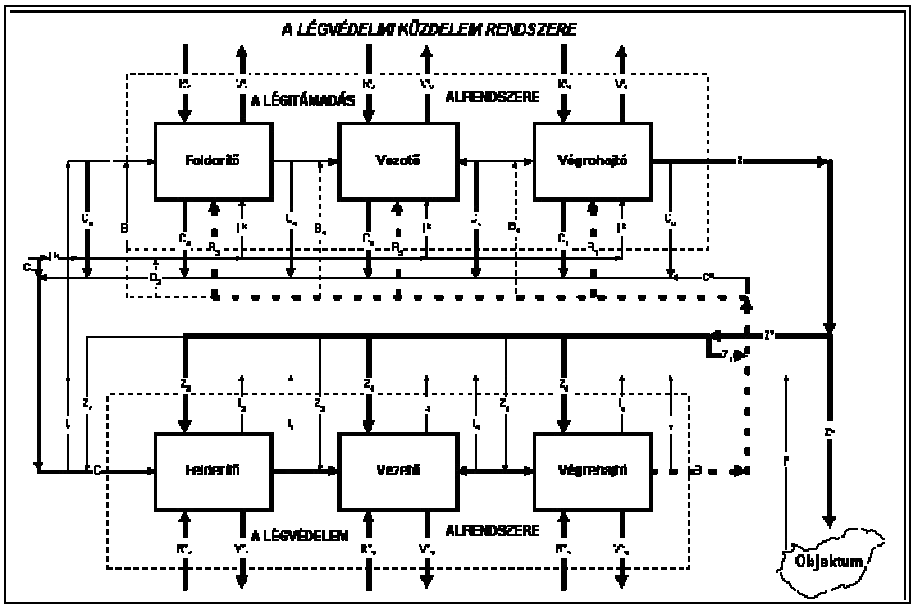
A katonai rendszerek tényleges funkcionális modelljében (7. ábra.) a környezetből érkező bemenetek mindhárom alrendszerre hatnak, és a kimeneteket valamennyi alrendszer befolyásolja. Ez könnyen belátható, ha a katonai rendszert "természetes" közegében, a fegyveres küzdelemben vizsgáljuk.



7. ábra

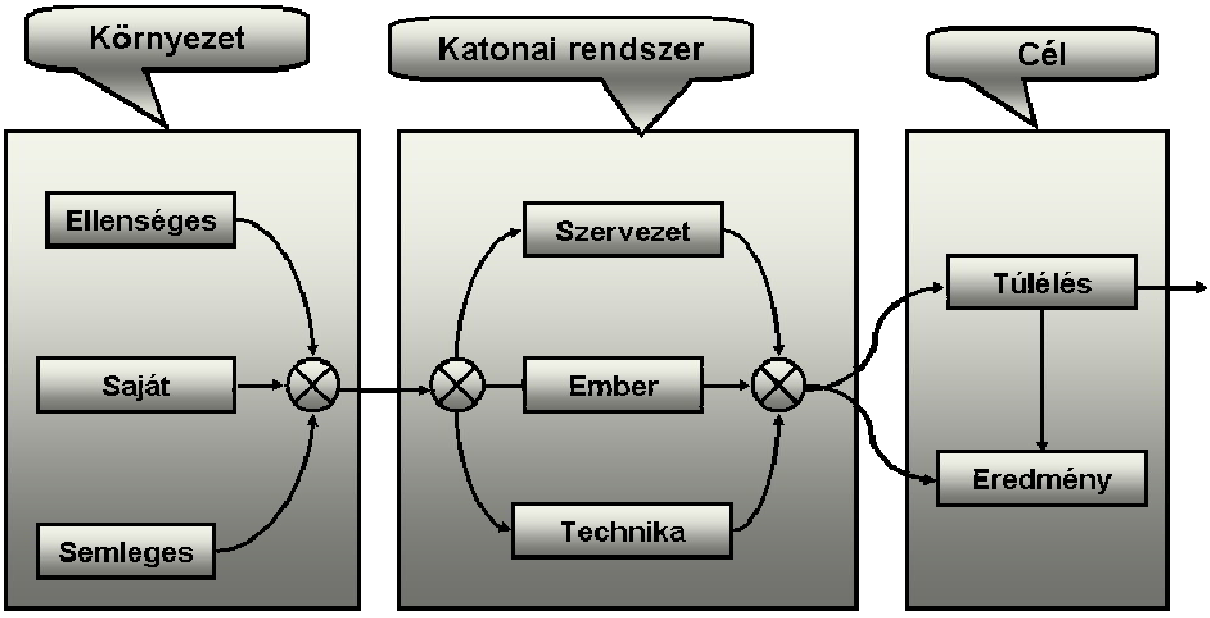
Az ellentmondás feloldására két lehetőség kínálkozik. Az egyik, ha katonai rendszer "fekete dobozait" olyan mélységig bontjuk ki, hogy ott az elemek már valóban elemek, mivel egyértelműen besorolhatók valamelyik al-al-alrendszerbe. Ez a megközelítés oda vezetne, hogy egyértelmű struktúrát csak az egyes alkatrészek szintjén találnánk.

Ezen az úton járva, az elemek funkcionális hovatartozásának bizonytalansága miatt, vagy csak ellentmondásos, vagy, ha a felbontás már elég mély, még a korszerű számítás-tudomány felhasználásával is csak nehezen kezelhető modellt kapnánk (például, a légvédelmi küzdelem esetében a 8. ábra).



8. ábra

Az ellentmondás feloldására - a különböző szintű katonai rendszerek, különböző alkalmazási feltételek közötti vizsgálatára - a másik lehetőség a katonai rendszer strukturális modelljének alkalmazása. E modell szerint a katonai rendszer a *környezet* saját, ellenséges és semleges elemei által meghatározott *követelmények, igények* és *feltételek* között integrálja három alrendszere – az *ember,* a *technika* és a *szervezet – tulajdonságait, képességeit* a rendszer – a környezet által kitűzött, illetve kikényszerített - *céljának (eredmény, túlélés, illetve a veszteségek és a környezeti károkozás minimalizálása*) – elérése érdekében (9. ábra).



9. ábra

A katonai rendszerek egy speciális változata a harci robot

A haditechnikai kutatás-fejlesztés célja, hogy a saját katonai rendszerünk minden szintjén, a harc megvívása során a *haditechnika* egyre több funkció megvalósítását vegye át az *embertől,* illetve növelje annak túlélési esélyeit. E cél elérésének három útját vizsgáljuk meg.

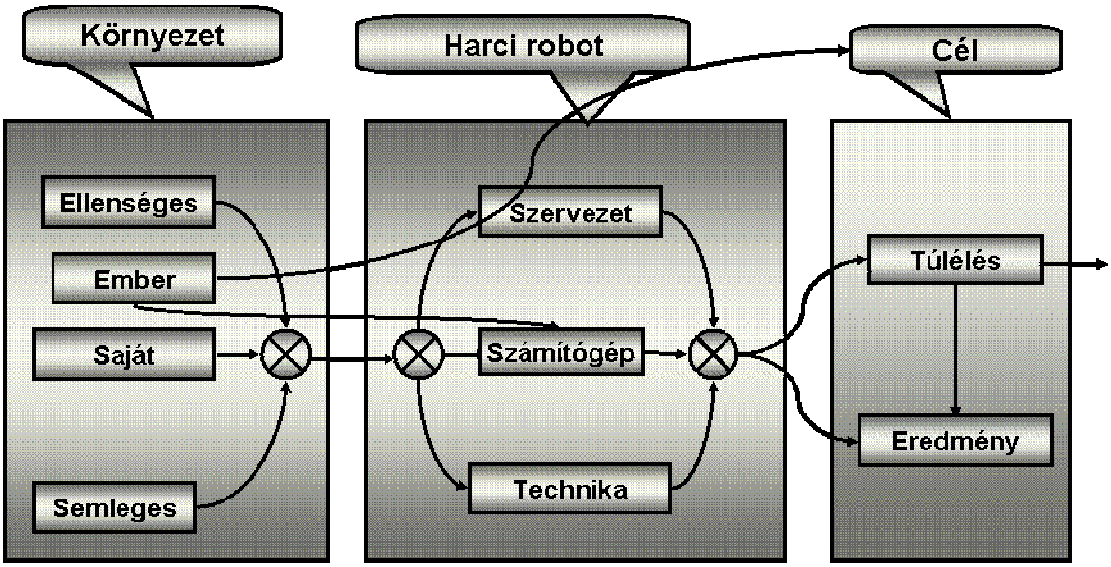
Az első, legkézenfekvőbb út a *támadóeszközök hatótávolságának és pusztítóerejének növelése,* ami elvezetett a parittyától az interkontinentális, nukleáris ballisztikus rakétákig, amelyekkel a pusztító eszközöket a föld bármely pontjára el lehet juttatni.

A második út az *egyéni és kollektív védőeszközök* fejlesztése a pajzstól, az egyéni védőeszközökön át az atombunkerekig tartott. Az egyre biztonságosabb védőeszközök javítják ugyan az ember és a haditechnika túlélési esélyeit a harcban, azonban csökkentik a hatékonyságot.

A haditechnikai kutatás-fejlesztés legígéretesebb útját a huszadik században – a *számítógépek* megjelenésével – megkezdődött *automatizálás* nyitotta meg. A – kezdetben mechanikus, majd elektromechanikus, később elektronikus analóg és digitális – számítógépek katonai alkalmazása a reakcióidők csökkentésével és a döntések megbízhatóságának növelésével biztosították a támadó és a védelmi eszközök hatékonyságának javítását, és a túlélési esélyek emelkedését.

A huszadik század második felében a haditechnikai eszközök és a számítógépek drasztikus miniatürizálása, az információtechnológia rohamos fejlődése, és a mesterséges intelligenciakutatás eredményei lehetővé tették, hogy a fegyveres küzdelemben ne csak egyes funkciók, hanem komplex harcfeladatok végrehajtása is automatizálható legyen. A haditechnikai K+F eredményeként megjelentek - az önálló *rendszernek* tekinthető - földfelszíni, légi és vízi (víz alatti), *felderítő, támadó és védő robotok.*

Ezekben a *rendszerekben* az *ember* szerepét a *számítógép* veszi át. Az ember e rendszer *környezetének* elemeként a rendszer céljának meghatározását – és az előre nem látott esetekben a számítógép programjának módosítását – végzi (10. ábra).



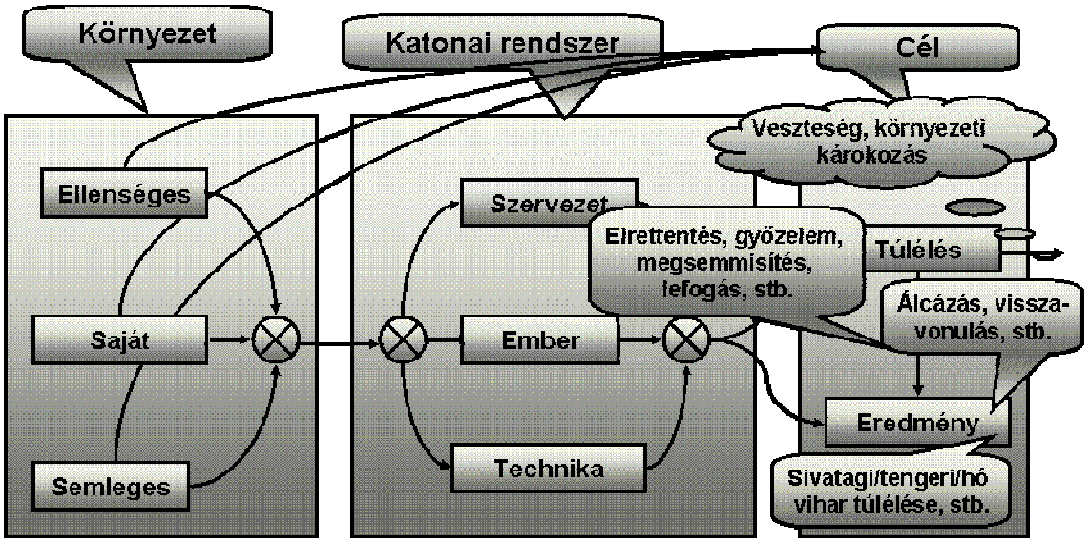
10. ábra

A harci robotok alkalmazása nemcsak jelentősen csökkenti az emberi veszteségeket és – a pontosabb hatáskifejtés eredményeképpen – a környezeti károkozást, de ez utóbbiak felszámolásában is szerepet játszhat – például, aknakutatásban, szennyezett terepszakaszok semlegesítésében.

Első következtetés

A modell feladata olyan fenntartható katonai rendszer elemzése, amely biztosítja, hogy a rendszer bármely szintje, valamennyi – a környezet minden eleme által kitűzött, illetve

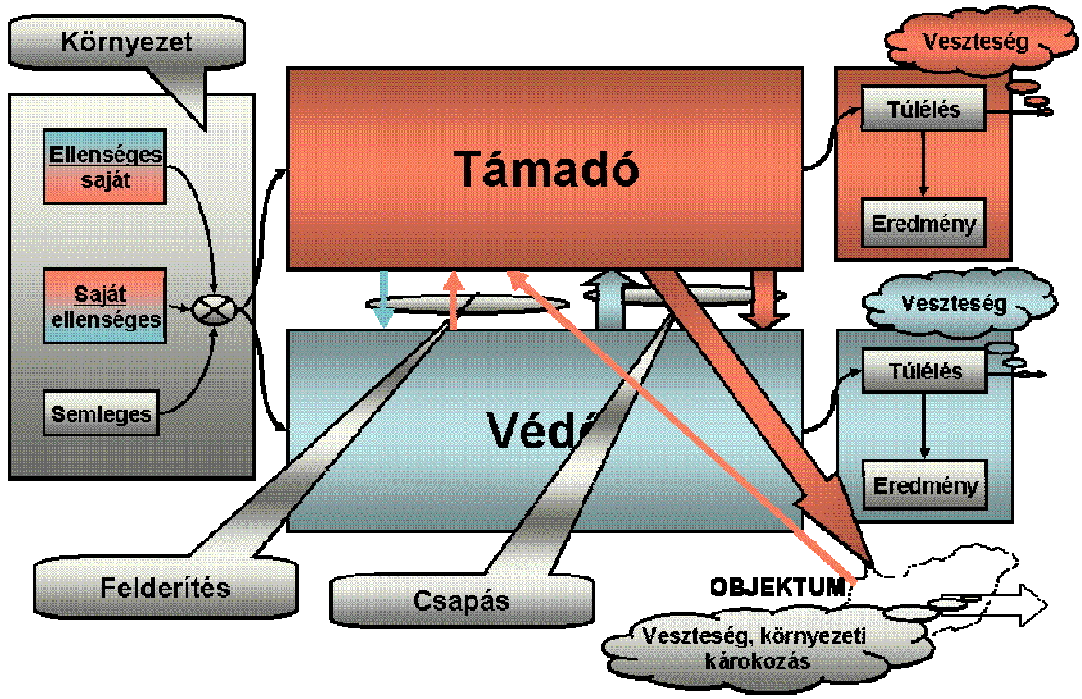
kikényszerített – célját képes legyen elérni a veszteségek és a környezeti károkozás minimalizálásával (11. ábra).



11. ábra

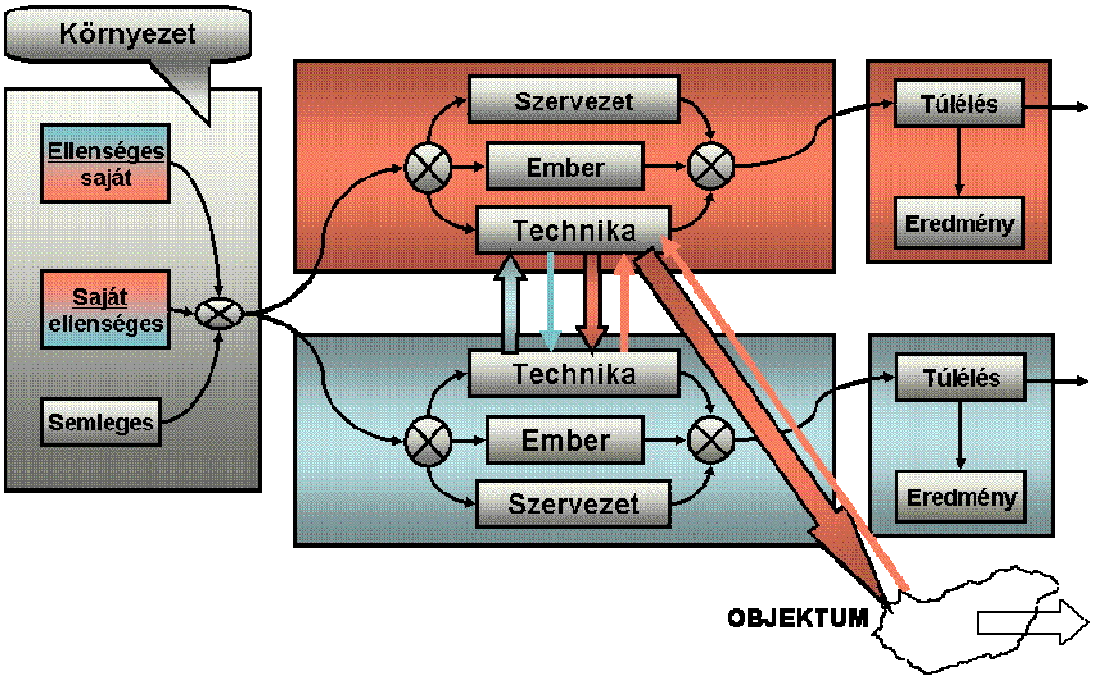
A technika szerepe a fegyveres küzdelemben

A katonai rendszerek céljaikat a fegyveres szembenállás, illetve a fegyveres küzdelem keretében érhetik el (12. ábra).



12. ábra

A katonai rendszerek közvetlenül mindig a „technikai oldalukat” fordítják szembe egymással. A haditechnikai eszközök és rendszerek biztosítják mindkét oldal számára a felderítési információkat, a csapásmérést, illetve a saját emberi és szervezeti elemek védelmét (13. ábra).



13. ábra

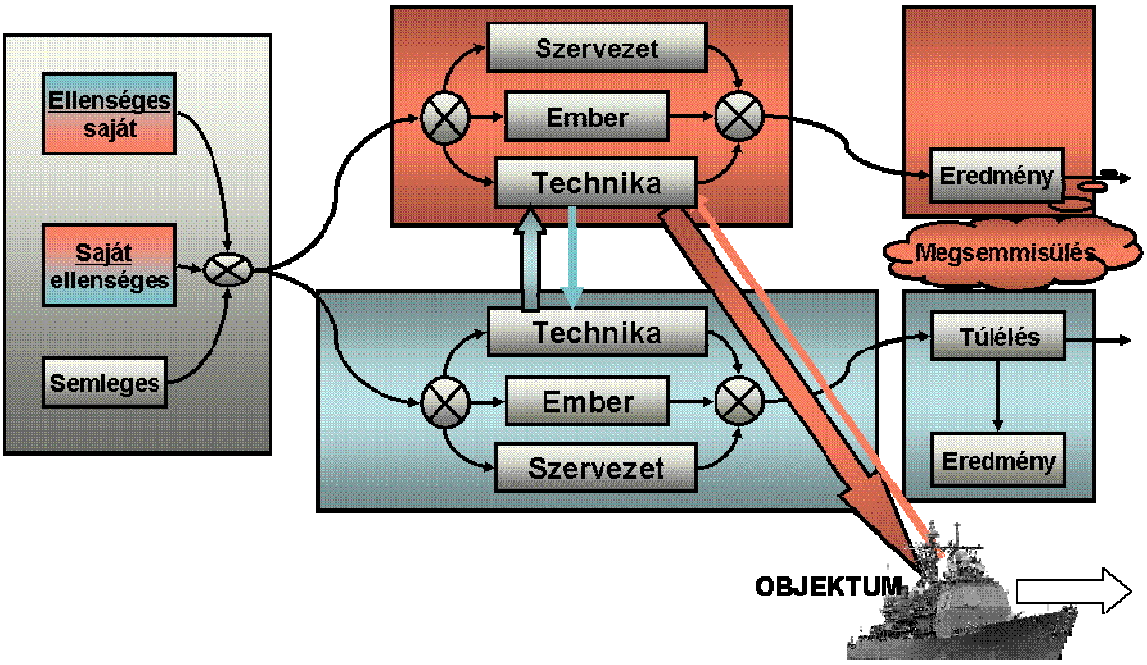
Katonai rendszerek szembenállása esetén mindkét félnek el kell dönteni, hogy elrettentéssel, vagy fegyveres küzdelemben akarja a saját elöljáró, vagy együttműködő környezete által kitűzött céljának elérését. A döntést – a politikai motívumok mellett – tervezési modellkísérletekkel lehet megalapozni. A haditechnika szerepének növekedésével a fegyveres küzdelem modellezése is egyre bonyolultabbá vált. A nagyteljesítményű számítógépek megjelenése lehetővé – és a hadtudomány fontos feladatává – tette a fegyveres küzdelem komplex matematikai modelljeinek kidolgozását.

Az *összemérhető* haditechnikai fejlettségi színvonalú, katonai szövetség, vagy nemzeti hadsereg szintű katonai rendszerek szembenállása esetében az elrettentés fenntartására vonatkozó döntés minden esetben új hadtudományi kutatási feladatokat eredményez.

A szembenálló katonai rendszerek haditechnikai fejlettségi szintjének jelentős eltérése esetén a fegyveres küzdelem modellje – az alapvető összefüggések fennmaradása mellett – eltérhet a bemutatott modelltől.

A fegyveres küzdelmet a haditechnikai fejlettségi szintjének jelentős eltérése esetén három jellegzetes modell alapján vizsgálhatjuk.

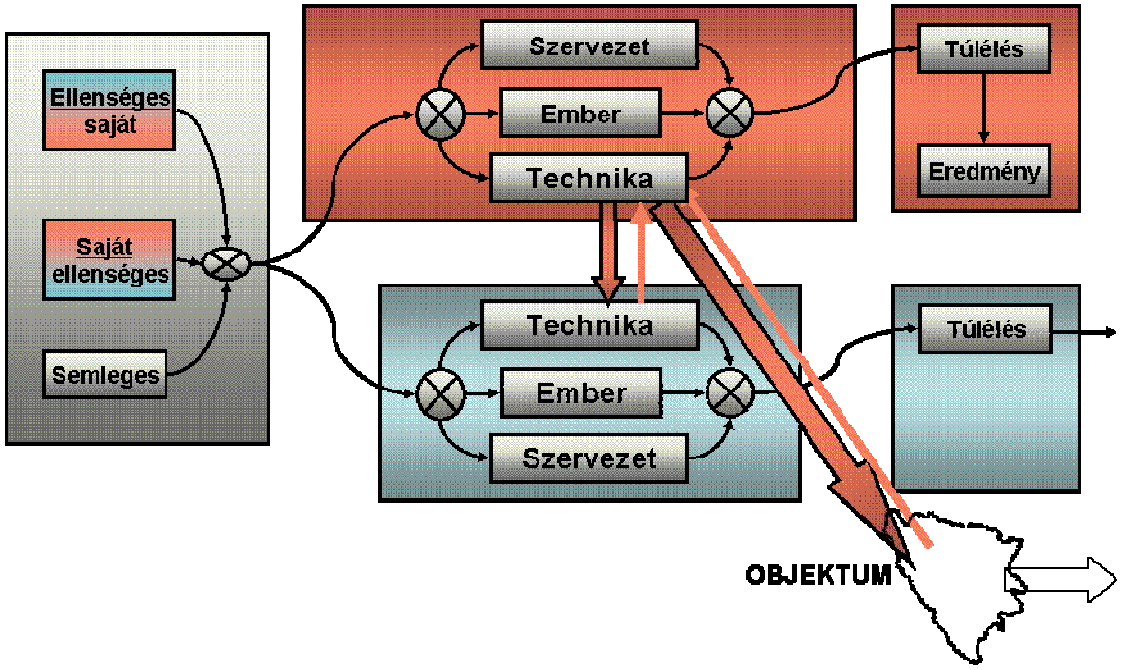
A *„kamikáze” modell* a második világháborúban a japán öngyilkos pilóták „technológiáját” szemlélteti, amikor a *túlélés* kikerült a katonai rendszer céljai közül (14. ábra).



14. ábra

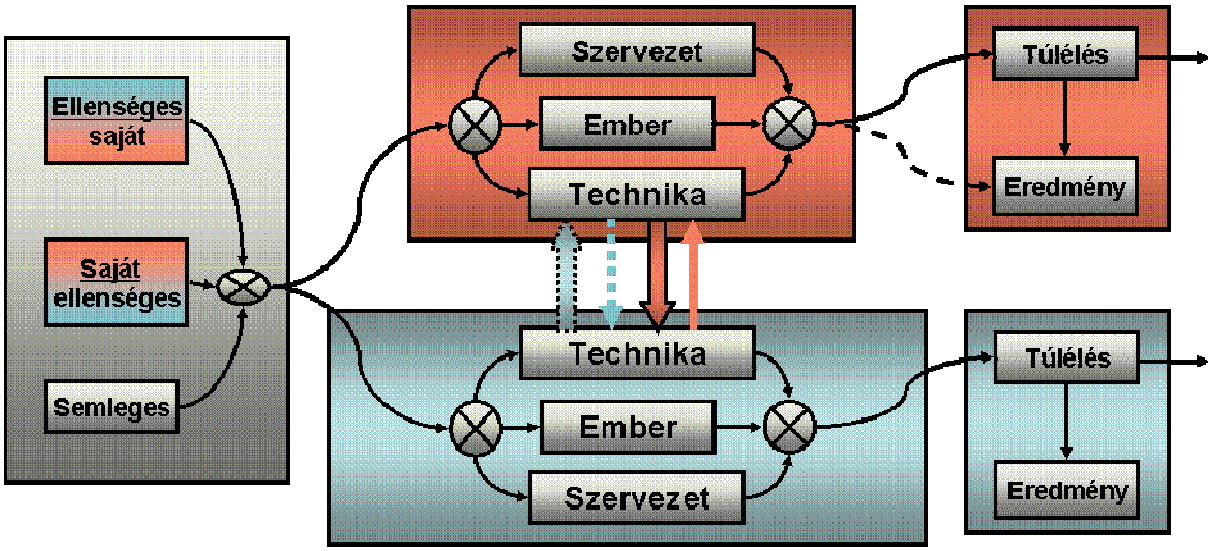
Amikor a Csendes-óceáni hadszíntéren folyó japán-amerikai összecsapások során kiderült, hogy a japán hadiipari rendszer már nem képes időben megfelelő hatósugarú, és pontos célzóberendezéssel ellátott repülőgépeket kifejleszteni a radarberendezésekkel és lőelemképzőkkel felszerelt amerikai hadiflotta elleni bevetésekhez, akkor a bombázógépekre egyszerűen rácsavarozták a kabinfedelet. A fanatizált pilóták pedig élő bombaként vezették rá repülőgépeiket az amerikai hadihajókra.

A *„délszláv" modell* szerint a támadó fél olyan mértékű haditechnikai fölénnyel rendelkezik, hogy az első – a kommunikációs kapcsolatokat és a vezetési rendszert, valamint a légvédelmet megbénító elektronikai, és nagypontosságú romboló – csapások után a védelem céljai között már gyakorlatilag csak a *túlélés* maradhat meg (15. ábra).



15. ábra

A *„gerilla” modell* a fegyveres küzdelemnek azt az esetét szemlélteti, amikor a döntő haditechnikai fölénnyel rendelkező fél egy *idegen állam területén* már elérte a katonai rendszere elé kitűzött célt, azonban nem tudta teljesen felszámolni a szembenálló fél katonai rendszerét. Ebben az esetben a legyőzöttnek tekintett fél, a helyi földrajzi, klimatikus és meteorológiai – valamint nem utolsósorban a politikai – *környezet ismeretében*, egyoldalú felderítési adatok birtokában, képes hatékony csapásokat mérni a „győztes” félre, úgy, hogy az, használható információk hiányában, sokszor képtelen az eredményes válaszcsapásokra (16. ábra).



16. ábra

A gerilla hadviselésre sok esetben jellemző a kamikáze jellegű, öngyilkos fanatizmus, vagyis az eredmény kierőszakolása a túlélés esélye nélkül.

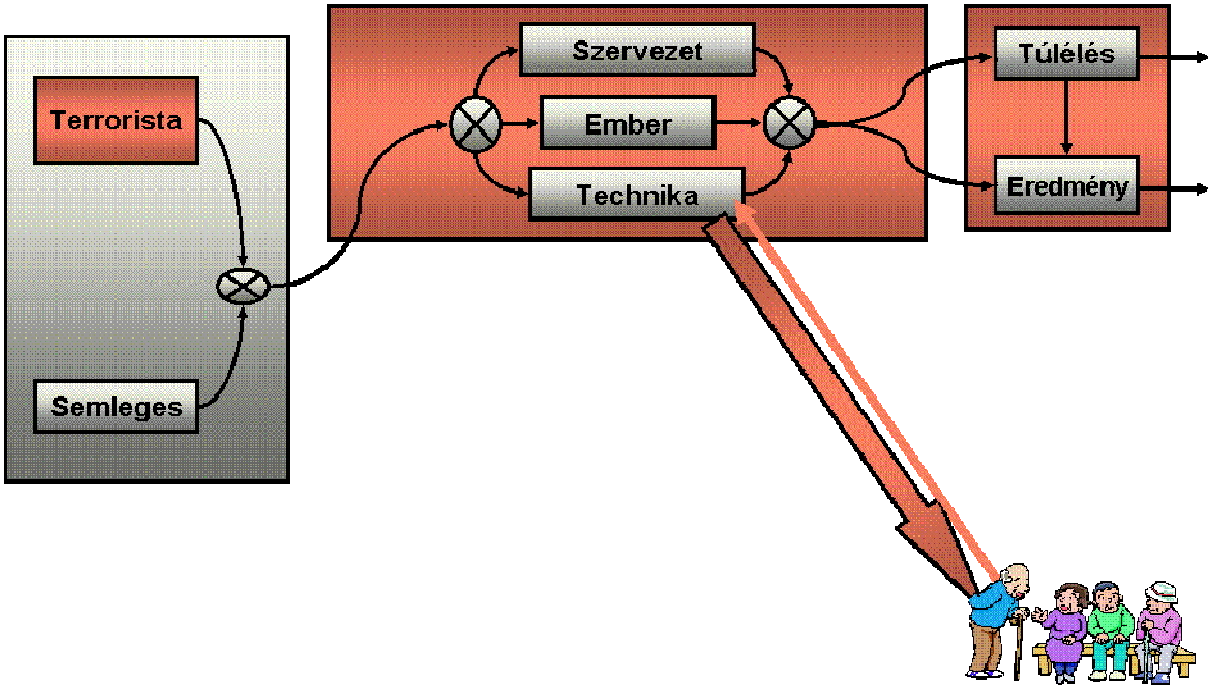
Második következtetés

A fegyveres szembenállás és a fegyveres küzdelem során a katonai rendszereket haditechnika kapcsolja össze, azonban annak fejlettségi szintje nem garantálja egyértelműen a harc kimenetelét.

A technika szerepe a terrorista rendszerekben

A fenntartható nemzetvédelem kutatása során nem tekinthetünk el a terrorizmus elleni küzdelem vizsgálatától. Ezért szükséges áttekinteni a katonai célokból létrehozott haditechnikai eszközök terrorista célú alkalmazásának lehetőségeit is.

A haditechnikai K+F tevékenység során, általában abból indulunk ki, hogy a létrehozandó, új haditechnikai eszközöket egy másik katonai rendszerrel szemben fogjuk alkalmazni, amely eszközeinek paraméterei a sajátunkhoz hasonló anyagi és erkölcsi értékek alapján meghatározhatóak. A terrorista katonai és félkatonai rendszerek esetében ezek az értékek teljesen más dimenzióban jelentkeznek. Ezek a rendszerek haditechnikai eszközeiket – szinte kizárólag – a technikai és szervezeti védelem nélküli EMBEREKKEL szemben alkalmazzák (17. ábra).



17. ábra

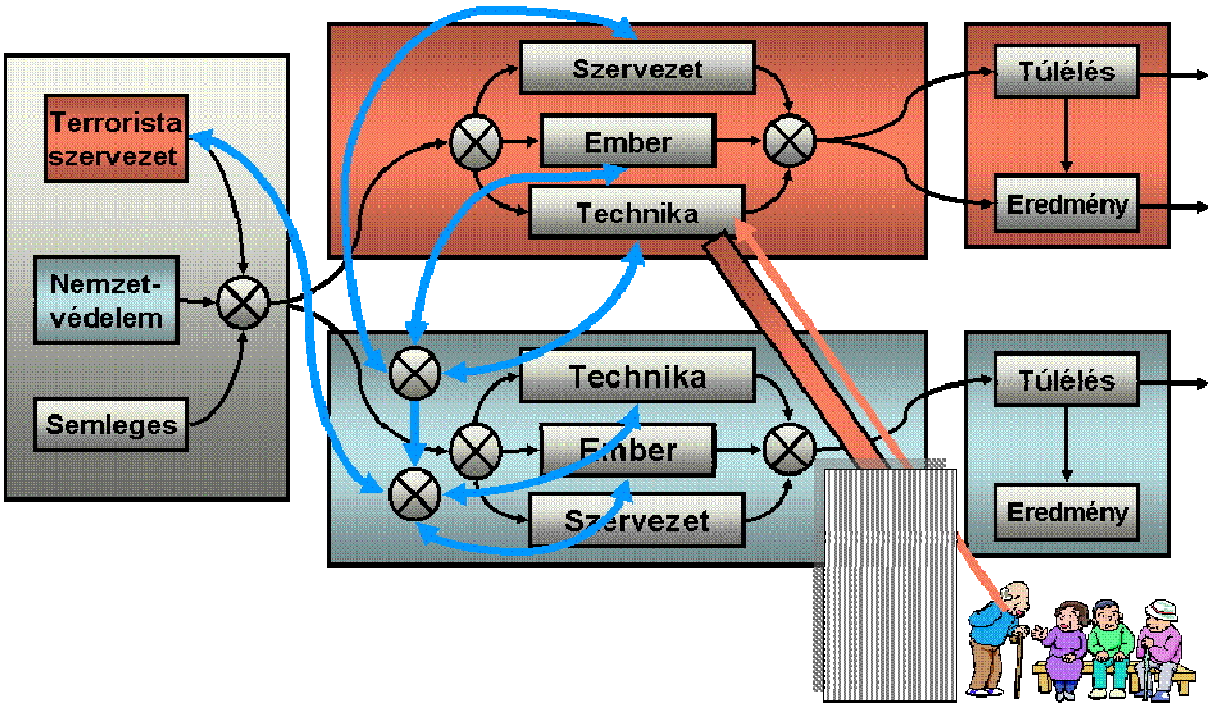
Az *„állami” terrorizmus* a totalitárius rendszerekre és a katonai puccsok szervezőire jellemző, amely a katonai rendszerek elleni fegyveres küzdelem céljaira kifejlesztett haditechnikai eszközöket alkalmazza a védelemre képtelen polgári lakosság ellen.

A *„törvényen kívüli” terrorizmust,* általában államokhoz közvetlenül nem köthető, katonai és félkatonai szervezetek alkalmazzák. Ezek jelentős részében a túlélés nem tartozik az elérendő célok közé. A terroristák általában a „hivatalos” haditechnikai K+F keretében kifejlesztett eszközöket alkalmazzák, de a pusztító eszközök célbajuttatására gyakran alkalmazzák az „emberi” hordozóeszközöket, vagy a polgári célú földi, vízi és légi szállítóeszközöket. A K+F tevékenységnek a haditechnikai eszközök méretének és súlyának csökkentését célzó eredményei jelentősen megnövelték annak lehetőségét, hogy a terrorista szervezetek birtokába egyre pusztítóbb eszközök kerüljenek.

A katonai rendszerek antiterrorista alkalmazásakor a szervezetek és az emberek nem csak a haditechnika támogatásával, vagy annak védelme alatt kerülnek szembe egymással, hanem a szembenálló rendszerek minden alrendszere közvetlenül kapcsolatba is kerülhet egymással (18. ábra).

A terrorista szervezetek katonai rendszereivel szemben a technikai felderítőeszközök bármilyen fejlettsége mellett sem nélkülözhető a hírszerző tevékenység, és a terrorista szervezetek politikai, vagy pénzügyi befolyásolása sem.

Ezért, ha az állam, vagy valamely nemzetközi szervezet saját katonai rendszerével akarja megvédeni polgárait a terroristatámadások ellen, az a hagyományostól eltérő jellegű eszközök és módszerek alkalmazását – a nemzetvédelmi rendszerek szinte valamennyi alrendszerének szoros együttműködését – követeli meg.



18. ábra

Harmadik következtetés

A terrorista szervezetek katonai és félkatonai rendszerei a haditechnikai K+F eredményeit is alkalmazzák a védelemre felkészületlen és alkalmatlan EMBEREK ellen, ezért a fenntartható nemzetvédelem vizsgálata során fokozott figyelmet kell fordítani az a egyes nemzetvédelmi alrendszerek szoros együttműködésére a terrorista támadások megelőzésében, az ellenük való védekezésben, illetve az általuk okozott károk felszámolásában.

ÖSSZEFOGLALÁS

A katonai rendszerek bemutatott modellje univerzális jellegű, mert alkalmas:

- a katonai rendszerek bármely szintjének;
- az ember, a technika és a szervezet alrendszerek koherenciájának;
- az egyes környezeti elemek által meghatározott célok befolyásának;
- az eltérő technikai színvonalú katonai rendszerek közötti harc változatainak;
- a terrorista jellegű rendszerek működésének, illetve a nemzetvédelmi alrendszerek ellenük alkalmazandó együttműködésének tanulmányozására.

Hogyan tovább?

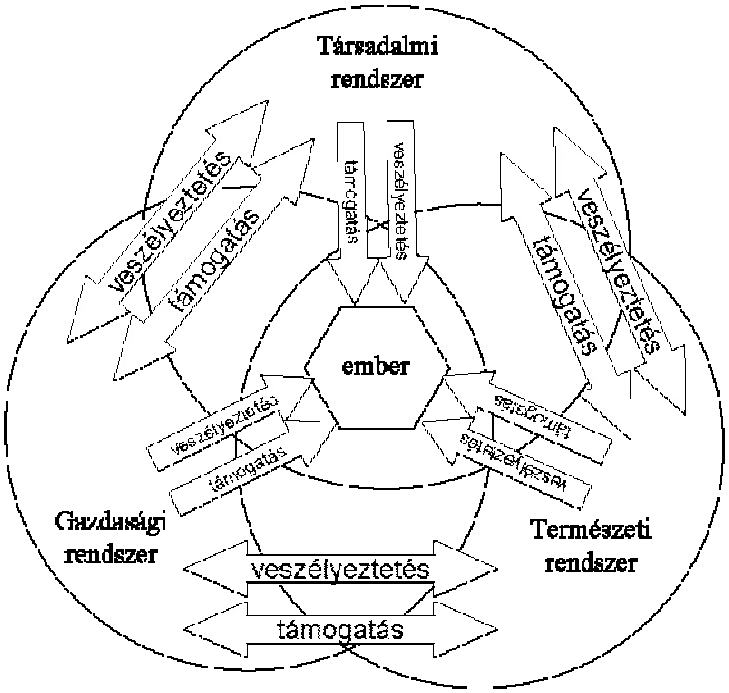
A Turchany tanulmány igen pesszimista következtetéssel zárul:

„Mi a teendő? Mit kellene tennünk ahhoz, hogy az európai kultúrkör… virágzása fenntartható legyen? ... a hangsúlyt a kultúrára indokolt visszahelyezni, új alapot teremtve ezzel egy egészen új civilizáció számára... Így az ember végre az állandó minőségi javulás és a felemelkedés útját fogja járni. Talán még odáig is eljut, hogy a benne működő destruktív erőket is szabályozni fogja. ... Ha ellenben ez a program nem sikerül, nincs más hátra, le kell tenni a

fegyvert, s egy, a jelen problémáit tekintve tehetségesebb kultúrának kell átadni a történelmi stafétabotot."

Valóban, írhatjuk már az európai civilizáció nekrológját?

Nem hiszem. Ha Európa képes volt néhány évtized alatt olyan politikai kultúrát kialakítani, amely több évezredes, szinte folyamatos háborúskodás után megteremtette a *fenntartható béke* feltételeit, akkor arra is képes lehet, hogy megtalálja a *fenntartható fejlődés* útját is.



19. ábra

Ennek az útkeresésnek egyik módszere lehet a rendszerszemlélet alkalmazása az embert körülvevő rendszerek – fenntartható ipari rendszer, fenntartható mezőgazdasági rendszer, fenntartható politikai rendszer, stb. – vizsgálatára, illetve a társadalmi, a gazdasági és a természeti környezet rendszerként való definiálása (19. ábra).

Ehhez az útkereséshez kívántam hozzájárulni egy, a példarendszer vizsgálatára alkalmazható modell felvázolásával.

Irodalom

[1.] Turchany Guy – Beranek László – Füleky György – Turcsányi Károly:
A fenntartható fejlődés: mítosz vagy valóság? *VALÓSÁG 2004. június XLVII. évfolyam 6. szám. 3. oldal.*
(http://www.valosagonline.hu/index.php?oldal=cikk&cazon=163&lap=0)

[2.] David Krieger: Peace and Sustainable Development Will Rise or Fall Together
Published on Thursday, August 15, 2002 by CommonDreams.org, p.1
http://www.commondreams.org/cgi-bin/print.cgi?file=/views02/0815-08.htm

[3.] Tobias Damjanov: NATO, Security and Sustainable Development
Paper presented at the "No NATO" Conference of Alba Kör, Budapest, Hungary, Nov. 1997

[4.] Report of the united nations conference on environment and development *(Rio de Janeiro, 3-14 June 1992, Principle 24)*
http://www.un.org/documents/ga/conf151/aconf15126-1annex1.htm

[5.] Indicators of sustainable development: guidelines and methodologies
http://www.ff3.hu/upload/indisd-mg2001.pdf

[6.]Sustainable development indicators in your pocket 2004
http://www.sustainable-development.gov.uk/indicators/sdiyp/sdiyp04a4.pdf

[7.] Kende György – Seres György: Haditechnikai kutatás-fejlesztés**,** *multimédiás egyetemi tananyag,* ZMNE, 2005.
http://drseres.com/tavoktatas/fejezetek/01/kpluszf_01.htm

[8.] György Seres: Bases of military system modeling, *multimédiás egyetemi tananyag*
http://drseres.com/ceepus/

HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Szegediné Lengyel Piroska
l.piroska@t-online.hu

AN INNOVATIVE METHODOLOGY IN COMPILING DISTANCE LEARNING MATERIALS

Absztrakt/Abstract

Jelen cikk bemutatja, hogyan lehet növelni a tanulók motivációját, a kötelezettségvállalások fejlesztését, a pozitív hozzáállást, valamint a személyiségüket a legmodernebb interaktív tananyagok használatával. A szerző a virtuális oktatást vizsgálja a személyiség-központú pedagógia tükrében. A cikk célja bemutatni, hogy a szerző által kifejlesztett elektronikus tananyagok (e-könyvek) a hallgatók saját személyes tanulási módszerek megerősítésében, az öntudat és a pozitív gondolkodás növelésében milyen szerepet játszanak.

The article is to present how to increase the students' motivation for learning, to develop their commitments, their positive attitudes, their personalities by compiling and using state-of-the-art interactive teaching materials. The author approaches the effectiveness of virtual teaching through the mirror of personality-focused pedagogy. The article is to describe how the electronic learning materials (e-books), developed by the author, might support students for elaborating their own personal learning methods, strengthening their self-consciousness, their positive thinking.

Kulcsszavak/Keywords: *e-tanulás, e-tanár, kognitív tudás, kompetencia-motiváció, módszertan ~ e-learning, e-teacher, cognitive knowledge, competence-motivation, 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, the socialization of the "lifelong learning" has become a primary task, i. e. a piece of the 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 its relevant methodology – the further key elements: the student, the teacher and the teaching-learning environment.

On the basis of the above "premissa" I developed four e-books (Accounting of Subsidies, Introduction to the Accountancy, General Accounting, Taxation), available on the Moodle-portal of my home page (http://www.lengyelpiroska.hu/elkonyv.html). [1]

When compiling the learning materials, I have relied on my pedagogic principle: the main aim lies, to a great extent more, at forming personalities in an appropriate way and developing the abilities in an adequate way, than at increasing the quantity of the knowledge, as basically the former factors may guide the students to convertible knowledge. The methodology of the e-books are 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 has to be continuously learned by them. The methodology of the e-books 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.

The e-books have been available since October, 2009 and mainly used by high school student teams, as an additional learning source to the traditional ones and, despite the relatively short time elapsed, can show a considerable success achieved. The number of visitors of the homepage has exceeded 16,000, in the first eleven months.



Figure 1. Electronic books compiled by the author
http://www.lengyelpiroska.hu/elkonyv.html

When writing the e-books, the basic principle was that the transfer of knowledge should serve, on the one hand, for the self-reliance, the self-development, the freedom in the education, and on the other hand, for educating the sense of responsibility, the respect of others, cognition and recognition of others. The methodological structure of the modules in the e-books reflects my hypothesis, that several types/devices of learning sources should be offered to the student, and then, it is to be left on their own, without any external pressure, to choose between them.

The e-books are inducing the students to accomplish a self-organised learning, supported by the Internet, however they are obliged to follow a disciplined and linear progress in the learning material. Due to the specificities of the learning material, the students, for the sake of the successful accomplishment, have to respect the offered order of progress:

- learning on their own, using "The learning material" module which is easily readable and rich in multimedia devices,
- deepening the acquired knowledge by using the "Lectures" module,
- checking the knowledge by using the "Practices" module which offers practice-oriented examples,
- the "Stage" module, as the "level of action", serves for trying the practical application of the knowledge.

Due to the systematic order of modules, the message, the content of the e-books will become interesting, enjoyable and effective to learn "…..The secret and basic element of the success of an e-learning system is to see the consecutive educational phases and the related modules clearly and to separate them carefully when planning the modules." [2]

In the course of planning the single modules and the learning environment, I put major emphasis on the clear-cut structuring in order to provide an easy "look-through", a "sense of safety" for the students, as they will be able to select the devices, modes for acquiring and practicing a given lesson, a homework. In a well-structured learning material the chance for the self-relied progress is better, the derivation of consecutive new items is simpler, the manageability of the material is better. [3]



Figure 2. The four modules of the e-book: Introduction to the Accountancy (Learning material, Lectures, Practices, Stage)

http://www.lengyelpiroska.hu/szamvitele/konyv/Tartalomjegyzek.html

THE FIRST LEVEL OF THE LEARNING PROCESS, THE "LEARNING MATERIAL" MODULE

The "Learning material" level, i. e. the level of acquiring information, serves for a self-relied acquisition of the knowledge for the student, i. e. learning on his own. The module uses passive and active elements, supported by multimedia devices, for presenting the topics, illustrated by pictures, figures. The content, being split into information units, will form an organic whole, thus supporting the structuring of the acquired knowledge.

The built-in guiding elements and feedbacks are encouraging the students for active learning and are, at the same time, directing, optimizing the learning process, adapting to the learning styles and mental standards of the students.

When compiling the "learning materials" of the e-books, I was searching for methods, through the application of which the "closing up" of students with lower status can be solved, their participation will be more active in the learning process and their study performance improves.

"All that, in which we are progressing well, will keep our interest alive, while, on the contrary, an activity, in which we do not reach certain level of the competence, will, in general, raise our interest for a long-lasting period, rarely." [4] Positive feedbacks, received from the partner students and the teacher will strengthen the competence, the self-confidence and, in this way, will give further motivation for continuing the activity and will induce students to meet the requirements.

In the closing section of each major chapter of the learning material, I inserted project works, which are to prefer working in teams, to get acquainted with partner students, to emphasize the importance of community-building, thus the requirements which are relevant for the e-learning, as well. It is offered to the students, every of them can measure the level of the knowledge, acquired through the self-relied learning through the solution of the project works of practical nature, working together with other partner students, in the framework of on-line sessions.

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 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 that everybody possess important intellectual abilities, even though unique ones, through which he 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 work, so, in this way, a relation-net of mutual interdependence will be formed between them. [5]

The most important aspect is that for the successful solution of the team work, it is inevitable to mobilize the students' colourful abilities and through this way – in addition to the advantage that every student, irrespective from his own intellectual abilities, contributes to the successful solution of the team work – the teacher, as an observer, has a possibility for studying and "mapping" the individual capacities and capabilities of the students.

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 lower status students' being switched on into the team work.

THE SECOND LEVEL OF THE LEARNING PROCESS, THE "LECTURES" MODULE

The "Lectures" module is the second level of the learning process, the level of deepening the knowledge, learning with interaction and learning with teacher's cooperation. The lectures are



Figure 3. The Lecture
http://www.lengyelpiroska.hu/szamvitele/konyv/Eloadas.html

fundamentally being relied on an illustrative-explanatory method. The essence of this method lies in visually presenting, modelling the topic, 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. The progress made on his own, the self-relied development, is able to multiply the efficiency of the learning process. The activity and progress on his own is a real, natural learning action (it is not artificial, directed from outside, as in case of "old traditional" school learning) it is being fed by the student's curiosity and manifested in increasing desire for learning (observing, appraising etc.). One's knowledge, acquired in this way, can be recalled even in many years later. As an example, let's take the railway models or car models collection hobby of the children: they remember the mechanical-technical data of the models even in their adult age, since the knowledge was made on their own in the course of a natural, active process.

The learning plan should, in each subject, put a weight on the active "discovery", which is to be acquired throughout specific experiences. [6]

In the course of compiling the lectures, the fundamental idea was that the experience-like learning leads to a better than average motivation and results in a long lasting learning spirit. The simple passive reception of the learning material through eyesight and listening (visual/auditive learning styles) will not be sufficient, one can notice, in this way, the half of the content only, at most, while throughout an active, contributory participation (chinesthetic learning style) this proportion can be increased even to 80- 90 %. [7]

There is a reward, built in to the learning material, offered for the successful acquisition of the knowledge, namely a reward presentation, playing, an active relaxation during the learning process. The playing is able to increase the efficiency of the learning in a considerable measure due to the fact that in the course of studying by playing the affirmation of the knowledge acquisition process with emotional experiences is exceptionally intensive. A learning activity like this is much more enjoyable, has an entertainment-like character: the students are playing in the course of the learning, they are learning by way of playing.

The closer the playing to the reality stands, the better the intensity of the knowledge acquisition will be. The playing (reward lesson), based on a real situation, built-in to learning material (see accounting in the small enterprises' practice, as an example, in the Introduction to the Accountancy), due to its experience-like character, will, on the one hand, increase the inner motivation of the students, and has, on the other hand, a specific beneficial effect, as the participants will, in the course of playing, experience the contexts of the real practice. The students have possibilities to shape the playing and in this way a team work will be emerged which mobilizes the knowledge of every participant and creates an opportunity for learning and changing each others' thoughts and opinions.

The learning material, having been played, will better be stored in the one's brain, as if it would have been heard, only. Both the intuitive vision, the several-sided observation of the facts and the free fantasy activity will help to store the knowledge and the experiences.

The condition to take part in the reward lesson, thus accomplishing a simple, playing-like task, selected out of the "Practices" (e. g. a crossword) provides an opportunity for acknowledging the results achieved by the students and this feedback influences the inner motivation positively. If the informational aspect of the reward is dominant, it confirms the student in his competence and self-determination which maintains his further interest. [8]

THE THIRD LEVEL OF THE LEARNING PROCESS, THE "PRACTICES" MODULE

The Practices module serves to measure the level of acquisition of the knowledge. Both the teacher and the student receive a feedback on how and to what extent the latter has managed to acquire the learning material.

The assessment plays an important role in shaping the attitudes to the learning process, in framing the learning motivation. [9] In order that the assessment can be able to fulfil its motivating function, the teacher has to analyze – based on results of the students in solving the works of the Practices – the students' difficulties in learning, continuously. The serial failures shape an aversion in the student in relation either with the learning process in general, or with a given subject and, as a consequence, his intellectual abilities will be blocked [10]

The Practices module serves for strengthening self-confidence of the students. Every student may choose out of the works with different difficulty level of the Practices, in accordance with his own assessment regarding the level of knowledge acquired by himself. The position of having an opportunity of the choice increases the student's autonomy sensation in the learning process [3]

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. A built-in program of the module evaluates the student's results promptly, thus the immediate feedback can contribute to confirm himself in his personality and to

respect himself for his result achieved. From learning efficiency's point of view, it is exceptionally important for the student to release his own negative attitudes against himself, to have a healthy self-confidence and to realize, he is a valuable man.



Figure 4. Practices

http://www.lengyelpiroska.hu/szamvitele/konyv/jutalom_eloadas.html

When developing the Practices module, the guiding idea of the process was that the acknowledgement of the results releases the student's inner insecurity, the success motivates him positively and he needs an intense motivation to achieve the success. The works, the tests have to possess such contents that the students can look forward to go through this "account giving" phase of the learning process, as a source of joy and, as a result, they will be more motivated regarding their self-development and study results. This goal is being served even by reward works, which is a further acknowledgement of the results achieved and at which the students can arrive through the solution of a simple task (affirmation of the acknowledgement).



Figure 5. The launch of a reward task

http://www.lengyelpiroska.hu/szamvitele/konyv/Peldatar_jutalomfeladat_start.html

The acknowledgement, the reward is a determining element of the self-relied learning process. It enhances the self-confidence and serves as basic foodstuffs for feeding the

intellectual health and the success. In the different motivation theories – work motivation theory, need theory, personality theory – the acknowledgement, the appreciation appears as the basis of the intellectual development. The acknowledgement is a motivating factor which makes certain kind of activity to start into the direction of satisfying this need.(Murray). [11] The "acceptance", the "approaching", the attitude of the appreciation can become one of the most efficient changeable forces (Rogers). [12] The acknowledgement produces a potential for the spiritual, intellectual development (Hertzberg). [13]

THE FOURTH LEVEL OF THE LEARNING PROCESS, THE "STAGE" MODULE

The Stage, "the acting level" emphasizes the importance of "the acting school" [14], the view that the "acting" is inevitable both for developing the thinking and for maintaining the interest. It gives an opportunity to the students to try how they can apply their knowledge in practice.

The students choose a case study out of the "Practices", they prepare its script, then they present it, they "play the story" and show its possible solution.

The assessment of the student teams' presentations will be carried out, under teacher's guidance, in the framework of "a stage debate", prepared in advance according to appropriate appraising points.

The Stage – according to my expectations – gives the experience of joyful learning, it raises the lower status students' interest, too and increases their autonomy sensation. Its atmosphere, being characterized by cooperation, enhances the inner motivation, the long lasting maintenance of which may only be fruitful in such a learning environment, where the single elements, the "players" are strengthening and presupposing each other.



Figure 6. The Stage
http://www.lengyelpiroska.hu/szamvitele/konyv/Pódium.html

CONCLUSION

Educating in the virtual environment may only be fruitful, if we create high quality learning materials, following the differences in the individual cognitive styles and learning habits of the students, when relying on such learning methods, which will keep the students' interest alive, will motivate them for learning; if we, in other words, as an educator, are aware of "what are the students interesting in", "how do they study", "what are their learning styles", "how can the students' interest be raised". These basic requirements are relevant not only for civil education, but for the military one, as well.

What may specifically the methodology, presented by the present paper, for the education and training systems used by the Hungarian Defence Forces, stand for? According to Miklós Vörös [15], it is necessary to continuously introduce and disseminate the new teaching/learning methods, devices and mediums in case of the Hungarian Defence Forces, as well. The individual's competitiveness is directly depending on the full career long learning, where the continuous development of the creativity, the flexibility, the adapting-, problem-solving-, and learning skills are of basic importance. The self-relied learning and -education is going to become one of the major conditions for staying in the field and being promoted.

Joining to the above thoughts, the basic goal of electronic learning materials, developed by myself, is to pass over state-of-the-art economic knowledge both to civil and military training participants in the field of financial-, taxation-, and accounting studies, in the framework of on-line training courses, relying on "experience pedagogy", thus multimedia-based learning materials and devices.

In case of military students, the knowledge acquired in the economic sciences can efficiently complement their special military-technical education, the practical benefit of which is evident for both the individuals (increasing vocational competence, preparedness, promotion) and the whole society, as well.

Being member country of the NATO, professionals in the army are, on the one hand, obliged to acquire and possess complex, interdisciplinary type of knowledge, crossing over different fields of sciences and Hungary, on the other hand, can be equal and competitive with a high-standard skilled-stuff training and a well developed high education system and well educated intelligence, only. Though the traditional education will never be totally replaced by distance pedagogy either in civil or in military education, the methodology presented by this paper can complement it both in civil and military sectors, as well.

BIBLIOGRAPY

[1] Szegediné Lengyel Piroska: Elektronikus könyvek http://www.lengyelpiroska.hu/elkonyv.html

[2] Noszkay Erzsébet: E-tanár a felsőoktatásban, In eVilág, 2006. 6. sz. p. 27-28

[3] Montessori M, 1912. The Montessori Method. In The discovery of the child. Oxford UK, 1991. Clio Press Ltd

[4] Bruner, J. S.: Új utak az oktatás elméletéhez, Budapest, Gondolat kiadó, 1974

[5] Falus Iván: Didaktika, Tankönyvkiadó 2003, p. 306; 382-385

[6] Johnson D. W. : Educational Psichology Englewood, Cliffs N. J, 1979

[7] Puschert-Weinert: SIMGAME –vom theoretischem zu praktisch anwendbarem betriebswirtschaftlichem Wissen in: Planspiele in derberuflichen Bildung, 2005.

[8] Deci, E. L. – Nezlek, J. – Scheinman, L 1981. Characteristics of the rewarder and intrinsic motivation of the rewardee. Journal of Personality and Social psychology, V. 40, 1-10. p.

[9] Réthy Endréné: Teljesítményértékelés és tanulási motiváció. Budapest, Tankönyvkiadó, 1989.

[10] Réthy Endréné: Teljesítményértékelés és tanulási motiváció. *Pedagógia Szemle,* 1986. 10. 972-978

[11] Harold F. O'Neil-Jr. Michael Drillings: Motiváció elmélet és kutatás Vince Kiadó 1999

[12] Rogers, Carl R.: Lényegi tanulás a terápiában és oktatásban, kiadta a Rogers Személyközpontú Iskola, Budapest, 1998

[13] Dobák Miklós: Vezetés-szervezés II. Aula, 1996 p.24-37

[14] Aebli, H. Lélektani didaktika, Budapest, Országos Pedagógiai Intézet, 1984

[15] Vörös Miklós: eLearning a katonai felsőoktatásban http://www.szamalk.hu/eLearning/Default.htm (loading time: september 12,: 2009)