



KATONAI MŰSZAKI TUDOMÁNYOK ONLINE

VII. Évfolyam 4. szám 2012. december

NKE
BUDAPEST

A szerkesztőbizottság elnöke:

Prof. Dr. Halász László ny. ezredes, DSc

A szerkesztőbizottság elnökhelyettese:

Prof. Dr. Munk Sándor ny. ezredes, DSc

A szerkesztőbizottság tagjai és egyben rovatvezetők:

Prof. Dr. Berek Lajos ny. ezredes, CSc (Biztonságtechnika)

Dr. Eleki Zoltán, PhD. (Fizikai felkészítés)

Prof. Dr. Haig Zsolt mk. ezredes, PhD (Védelmi elektronika, informatika és kommunikáció)

Dr. habil. Horváth László alezredes, PhD (Védelmi igazgatás)

Dr. Jászay Béla ny. ezredes, PhD (Védelemgazdaság)

Prof. Dr. Lukács László nyá. mk. alezredes, Csc (Katonai műszaki infrastruktúra)

Dr. Szűcs László ny. ezredes, CSc (Katonai logisztika és közlekedés)

Prof. Dr. Turcsányi Károly ny. mk. ezredes, DSc (Haditechnika)

Dr. Földi László mk. alezredes, PhD (Környezetbiztonság, ABV- és katasztrófavédelem)

Főszerkesztő: Prof. Dr. Kovács László mk. alezredes, PhD

Szerkesztő: Serege Gábor mk. főhadnagy

A szerkesztőség elérhetősége:

Nemzeti Közszerológálati 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@uni-nke.hu

web: <http://hadmernok.hu>

Kiadó: Nemzeti Közszerológálati Egyetem Hadtudományi és Honvédtisztképző Kar

ISSN 1788-1919

Jelen számban megjelent írások szerzői:

Balogh Péter mk. ezredes – NKE HDI doktorandusz

Dr. Bartha Tibor ny. mk. ezredes – NKE HHK egyetemi docens

Dr. Berek Tamás mk. őrnagy – NKE HHK egyetemi docens

Prof. Dr. Bukovics István – NKE KTK egyetemi tanár

Csuka Antal – NKE KMDI doktorandusz

Derzsényi Attila alezredes – NKE KMDI doktorandusz

Dr. Fleiner Rita – Óbudai Egyetem

Dr. Földi László mk. alezredes – NKE HHK egyetemi docens

Hollós Tamás – NKE RTK

Dr. habil. Horváth Attila alezredes – NKE HHK egyetemi docens

Dr. Fáy Gyula

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

Dr. Krasznay Csaba – HP Magyarország kft.

Dr. Kun István

Prof. Dr. Munk Sándor– NKE HHK egyetemi tanár

Nagyné dr. Takács Veronika – NKE KMDI doktorandusz

Dr. habil. Négyesi Imre mk. alezredes – NKE HHK egyetemi docens

Puskás Béla

Szabó Sándor – MH Összhaderőnemi Parancsnokság

Szentgáli Gergely – NKE Biztonság és védelempolitika Msc szak hallgató

dr. Tóth Krisztián – Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara

Venekei József alezredes – NKE HHK egyetemi adjunktus

Tóth Krisztián

toth.krisztian@szvmszk.hu

A TESTŐRÖK SZEMÉLYVÉDELMI FELKÉSZÍTÉSÉNEK EGYES SZAKMAI SZEMPONTJAI A MAGÁNBIZTONSÁGI SEKTORBAN

Absztrakt

A személyvédelem komplex rendszerének a kellő hatékonyság megteremtése érdekében a személybiztosításon túl – a veszélyeztetettség szinthez igazodó módon és időtartamban – legalább a védett személy szállás- és munkahelyének, programjai helyszíneinek, valamint közlekedési útvonalak biztosítására is ki kell terjednie. A csekély létszámú személyi állomány foglalkoztatása során gyakorta nincs lehetőség a biztosítási részfeladatok ideális megosztására, egy testőrnek egy személyben több ember munkáját is el kell látnia. Ehhez nélkülözhetetlen a szilárd alapokon nyugvó, multifunkcionális ismeretanyagot magában foglaló magabiztos szaktudás, valamint mindazon készségek és képességek, amelyek az interperszonális kapcsolatok vonatkozásában professzionális fellépést, elfogadott és eredményes akaratérvényesítést biztosítanak a testőrnek. Publikációm a magántestőrök személyvédelmi szakmai felkészítésének szempontrendszerét, a szükséges állomásainak és az egyén szignifikáns személyes kvalitásainak elemzését mutatja be.

Due to the complexity of the personal safety system, for good efficiency we need to look beyond the degree of danger and time span – at the least the protected assets accommodation and workplace, furthermore the location of the programs and lines of transportation should also be considered. Because of the small number of safety personal, there is no possibility of distributing the smaller tasks ideally, a bodyguard needs to complete the work of many people at the same time. For this to be so, it very important to have a good set of professional skills which can be used self-confidently, as well as the ability and capability for interpersonal relations with a professional attitude, acceptable and effective verbal communication. In my publication the personal bodyguard's professional method system, shows the necessary stations and the individual qualities required for this.

Kulcsszavak: magánbiztonság, személyvédelem, testőr, szakmai szempontok, készség, képesség ~ private security, close protection, bodyguard, professional methods, skill, ability

A MAGÁNBIZTONSÁGI SZEKTOR GLOBÁLIS TÉRNYERÉSE A SZEMÉLY- ÉS VAGYONVÉDELEM TERÜLETÉN

Az utóbbi évtizedek szakmai statisztikai elemzései egybehangzóan igazolják, hogy a magánbiztonsági szektor térnyerése világszerte egyre dinamikusabban növekvő tendenciát mutat. A civil szférában szervezett biztonsági szolgáltatók munkájára a korábbiakban megszokottnál is nagyobb igény mutatkozik, hiszen az egyes államok rendfenntartó-bűnüldöző szervei a legális erőszak monopóliumának letéteményeseiként egyre kevésbé képesek önállóan a hazai közrend és közbiztonság megnyugtató mértékű biztosítására. Köszönhető mindez többek között a fejlett és fejlődő országok között húzódó gazdasági-kulturális-világnézeti törésvonalak szélesedésének, a globalizációs versenyfolyamatok által generált válságjelenségeknek, a megélhetési nehézségekhez kapcsolódó bűnözés expanziójának, valamint egyes térségekben a fokozott terrorfenyegetettség mindennapokat átölelő nem kívánatos jelenlétének.

Az egyes országok jogszabályai taxatív felsorolják azokat a személy- és vagyonvédelmi feladatokat a hozzájuk rendelt jogosultságok és kötelezettségek deklarálásával, amelyeket a magánbiztonsági szolgáltatók (az arra feljogosított szervezetek illetve személyek) az állam által delegált feladatkörükben az adott ország területén legálisan végezhetnek. Ezen feladatokból adódó köteleességek hatékony teljesítése a szükséges forrás- és eszközállomány biztosításán túl csak a megfelelő elméleti felkészítésen és gyakorlati kiképzésen átment, majd rendszeresen továbbképzett személyi állomány tevékenységén keresztül valósítható meg.

A SZEMÉLYVÉDELEM ÁTFOGÓ RENDSZERÉNEK MULTIFUNKCIONÁLIS KÖVETELMÉNYEI

A hazai magánbiztonsági jogi jogviszonyok primer szabályozására alkotott, a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvényben foglalt definíció értelmében személyvédelmi tevékenységnek minősül a természetes személyek életének és testi épségének védelme, valamint ezen tevékenységnek a szervezése és irányítása. A gyakorlatban mindez kiegészül még a védett személy egyes személyhez fűződő jogai sértetlenségének biztosításával, különös tekintettel az emberi méltóság és a személyes szabadság integritásának védelmére, valamint a jó hírnév és a becsület csorbitatlanságának megőrzésére.[1]

Vitathatatlan tény, hogy magánbiztonsági szektorban tevékenykedő testőrök szakmai feladatai a személyvédelem komplexitásának teljes spektrumát átölelik. Ez alapesetben a védett személy személyi biztosításán túl annak lakó- vagy szálláshelyének, munkahelyének, programjai helyszíneinek, közlekedési útvonalainak, külföldi utazásainak biztosítását is magában foglalja, igény szerint kiegészítve a családtagok, egyéb hozzátartozók védelmével. Emellett hangsúlyozott szerephez kell jutnia a támadások illetve a rendkívüli események előfordulási kockázatát minimális mértékűre csökkenteni hivatott előkészítő-felderítő tevékenységnek, valamint a személybiztosítók munkáját a háttérből segítő, a biztosítás konspiratív vagy demonstratív jellegéhez igazodóan pozicionált támogató erők alkalmazásának. Mindez komoly tervezési-szervezési feladatokat ró a biztosítási tervet összeállító és a biztosítást végrehajtó magántestőrökre, akiknek tulajdonképpen egyszemélyben kell rendelkezniük azokkal a sokrétű ismeretekkel és kompetenciákkal, melyek alkalmassá teszik őket a személyvédelem minden egyes szegmensét átfogó multifunkcionális követelmények teljesítésére.

Ehhez egyrészt javasolt, hogy a magántestőrök személyvédelmi oktatását-képzését végző szakemberek tudásbázisa és annak részeként az általuk összeállított kötelezően számon kérendő tananyag az elméleti ismereteken túlmenően az instruktorok több évtizedes tényleges,

a magánbiztonsági iparágban megszerzett operatív tapasztalatain nyugodjon. Ennek hiányában sem az alap-, sem a továbbképzés nem tudja megfelelően betölteni azon fő rendeltetését, amely a magánszektor mindennapjaiban előforduló biztonsági kockázati tényezők és veszélyhelyzetek felismerésére, a támadások illetőleg a szándékosan előidézett vagy véletlenül bekövetkező rendkívüli események megelőzésére és jogszerű-szakszerű elhárítására irányuló multifaktorális szemléletrendszer és szaktudást hivatott a hallgatóknak átadni.

Másrésről lényeges a képzésekben résztvevő aspiránsok személyiségjegyeinek ergonómiai feltérképezése annak érdekében, hogy már a felkészítésük startpontjánál kiderüljön milyen típusú biztonsági feladat ellátására predesztinálják őket az adottságaik, a már meglévő és fejleszthető készségeik, képességeik. Az egységes alapképzést követően a képzési rendszer moduláris felépítése remek esélyt kínál erre, hiszen így mindenkinek lehetősége adódik a személyiségéhez és elhivatottságához legjobban illeszkedő szakterület megválasztásához. Szakmai berkeken belül köztudomású tény, hogy egy kitűnően dolgozó rendezvénybiztosító nem okvetlenül nyújt hasonlóan kiváló teljesítményt a személybiztosítás területén és egy munkájában elismert objektumőr sem biztos, hogy kritikai hangok nélkül megállná helyét a pénzszállítási feladat végrehajtása során.

A szakosodás szükségessége tehát a személy- és vagyonvédelmi tevékenységek sokrétű platformján nyugszik. Azonban a szakma csúcsának tartott személyvédelem keretei között szolgálatot teljesítő testőröknek a magánbiztonsági szakág összes általános és speciális részterületén átívelő tudásanyagot megfelelően ismerniük és magabiztosan alkalmazniuk kell. Ráadásként a szakmai hozzáértést reprezentálni hivatott kompetenciák elsajátításán túl egyéb szignifikáns készségek és képességek is meghatározó szerepet kapnak abban, hogy az egyén a jövőben magasan kvalifikált testőrré fejlődhessen.

A SZEMÉLYVÉDELEM VÉGREHAJTÁSÁT MEGELŐZŐ SZÜKSÉGSZERŰ SZAKMAI ÁLLOMÁSOK

A szakmai kompetenciákat megalapozó kritériumok vonatkozásában a magánbiztonsági szakmának is vannak olyan szükségszerű állomásai és területei, amelyek mentén haladva el lehet sajátítani a testőri munka lényegi alapjait jelentő elméleti és gyakorlati ismeretanyag jelentős részét. A személyvédelmi feladatok összetettségét alapul véve fontos, hogy a leendő magántestőr a személybiztosítási felkérését megelőzően szakmai tapasztalatokat gyűjthessen az objektumőrzés, a rendezvénybiztosítás valamint a pénz- és értékszállítás illetőleg kísérés területein is.[2]

Objektumőrzés

Az objektumőrzés során az őr általában egy térben körülhatárolt létesítmény őrzés-védelméről gondoskodik, amely mind a személy- mind a járműforgalom vonatkozásában viszonylag jól átlátható és kezelhető. Ideális körülmények között elég idő áll rendelkezésre a bebocsátásra váró személyek és járművek azonosítására, a belépési jogosultságok ellenőrzésére, szükség esetén biztonsági szempontú átvizsgálásukra, avagy a kiléptetésükhöz kapcsolódóan a hasonló intézkedések megtételére. A pontőrzést illetve járőrszolgálatot végrehajtó személyi állomány létszáma is még viszonylag alacsony, a felállítási helyeken az egyéni illetve néhány fős egységek munkavégzését szükséges csak összehangolni. Az élőerős őrzés mellett általában hangsúlyos szerepet kap a különböző mechanikus és elektronikus vagyonvédelmi rendszerek alkalmazása is.

Az objektumőrzésben való részvétel a testőr jövője szempontjából többek között az alábbi tapasztalatszerzési lehetőségeket kínálja:

- a szolgálati fegyelem elsajátítását: a váltásoknak az őrutasítás által meghatározott időpontban pontosan kell megtörténniük, az őrknek az előírt egyenruhában, felszereléssel és állapotban kell megjelenniük, a szolgálatvezető utasításait végrehajtani, stb.
- a szolgálati dokumentáció precíz vezetését: átadás-átvételi naplók, jelenléti ívek, járműnyilvántartások kitöltését, kulcsdobozok, támadáselhárító eszközök, hozzáférési kódok átadásának-átvételének szabályainak elsajátítását
- a terület őrzését elősegítő mechanikai és elektronikus vagyónvédelmi rendszerek (zárak, kerítések, telepített akadályok, tűz- behatolásjelző- és riasztórendszerek, megfigyelő- és beléptetőrendszerek) telepítési, működési és alkalmazási gyakorlatának megismerését
- a védett objektum személyforgalmával (dolgozók, ügyfelek, egyéb szolgáltatást nyújtók) szembeni határozott, tiszteletteljes, segítőkész bánásmód és együttműködési készség kialakítását, a konfliktuskezelési módszerek elsajátítását
- a híresszeköttetésre szolgáló kommunikációs eszközök kezelését
- a járműforgalom és a szállítási okmányok ellenőrzését, a parkolási rend kialakításának megtervezését és lebonyolítását, indokolt esetben a jármű utas- és csomagterének biztonsági átvizsgálását
- a beérkező csomagok, szállítmányok biztonsági szempontú átvizsgálását és elkülönítését, csomagröntgenek, kézi fémdetektorok használatának elsajátítását
- az objektumban található szobák, irodák előzetes technikai átvizsgálási módszereinek elsajátítását
- a pénz és értékszállítás biztosítását a létesítmény területén
- menekítési útvonalak kijelölését és biztosítását, menekítési helyek kialakításának feltételeit és felszereltségük meghatározását
- támadás vagy rendkívüli esemény bekövetkezésekor az objektumvédelemhez kötődő intézkedések jogszerű és szakszerű végrehajtását, a támadáselhárító eszközök indokolt esetekben történő alkalmazását

Rendezvénybiztosítás

A szakmai fejlődés ranglétráján a következő fokot a rendezvénybiztosítás jelenti, az innen származó tapasztalatok sem hiányozhatnak a majdan professzionális szolgáltatást nyújtani képes testőr kellektárából. Általában a rendezvények is még térben jól körülhatárolható helyszíneken zajlanak, karakterüktől függően azonban már többnyire nagyobb létszámú tömegeket mozgatnak meg. Emiatt biztosításuk mindenképpen gyorsabb és dinamikusabb cselekvési- és szemléletmódot kíván meg az objektumőrzésnél elemzett viszonylagosan statikus állapotokhoz képest. Ennek szükségszerű eredőjeként a rendezvénybiztosítást végző személyi állomány is már jóval több tagot számlál, amely okán csapatként való összehangolt együttműködésük elengedhetetlen feltétele a munkavégzésük eredményességének.

A rendezvénybiztosítások végrehajtása során a leendő testőr empirikus úton megtanulja:

- a "csapatszellem" kialakítását és az operatív fegyelem erősítését az egyéni elgondolások keretek közé szorításával, az eligazításban foglaltak, a biztosításért felelős vezető, valamint a szektorfelelősök utasításainak fegyelmezett végrehajtásával
- a rendezvényhelyszín előzetes technikai átvizsgálását, tűzszerész átvizsgálásának megszervezését

- a védelmi körök határainak kijelölését, ellenőrző-áteresztő és stratégiai megfigyelő pontok felállítását, kordonok, fémdetektoros kapuk és egyéb mobil mechanikai és elektronikus védelmi eszközök telepítését
- a közlekedési útvonalak biztosítását, a parkolási rend kialakítását, a vészkijáratok akadálytalan megközelítésének és szükség esetén használatának biztosítását
- a rendezvényre látogató tömeg gyors és hatékony beléptetését, ruházatának, csomagjainak átvizsgálását, a fellelt kirekesztendő tárgyak tárolási-megőrzési lehetőségeinek kialakítását
- intézkedés foganatosítását tiltott tárgyak fellelése esetében, a bűncselekmény vagy szabálysértés elkövetésén tetten ért személlyel szemben
- a játéktér, nézőtér, sajtószoza, VIP páholy valamint egyéb helyiségek biztosítását, a menekítési utak és helyek kijelölését, felszerelésük biztosítását
- a VIP személy kísérését, a védelmi alakzatok alkalmazását, a védett személy környezetében való professzionális viselkedés elsajátítását
- együttműködés kialakítását a rendvédelmi, katasztrófavédelmi és az egészségügyi háttért biztosító szervekkel, a rendezésben résztvevő egyéb személyekkel, szervezetekkel
- a sajtó és média képviselőivel szemben tanúsítandó megfelelő magatartás elsajátítását, a szabad mozgásukat biztosító útvonalak kijelölésének szempontjait
- nyílt és rejtett kommunikációs eszközök használatát tömegben, nagy háttérzajban
- a tömeggel szembeni közérthető kommunikáció és magabiztos, határozott fellépés elsajátítását
- a tömeg mozgásának és hangulatának figyelését, a pánikhangulat kialakulásának megelőzését
- gyors reagálást a renitens elemekkel szemben, a probléma eszkalálódásának megakadályozását
- elkülönítési-kiemelési-elvezetési taktikák és technikák csapatban történő alkalmazását
- rejtett biztosítóként való elvegyülést a tömegben
- támadás vagy rendkívüli esemény bekövetkezésekor a menekítés, kiürítés szakszerű végrehajtását
- a rendezvény végén a tömeg kiléptetésének és biztonságos távozásának biztosítását

Pénz- értékszállítás és kísérés

A harmadik szükségszerű állomásunk – a pénz- vagy értékszállítás illetőleg kísérés végrehajtása – újabb hasznos elemekkel bővítheti a testőrjelölt szakmai ismereteinek repertoárját. A feladat teljesítése során kilép már a térben körülhatárolt biztosított helyszínnek átlátható keretei közül és olyan nyílt terepre kerül amelynek "ellenséges" mivoltára folyamatosan számítnia kell. A járművel történő pénz- értékszállítás és kísérés a közlekedési eszközök veszélyes üzemi jellegéből adódóan, valamint az egyes közúti, vasúti, légi vagy vízi közlekedési útvonalak biztonságának sarkalatos kérdéseihez kötődve számtalan új rizikófaktor emelkedik felszínre. Közúton – amely a magánbiztonsági szektorban a leginkább alkalmazott pénz- és értékszállítási forma – a véletlen közlekedési balesetek bekövetkezésének kockázata mellett a pénzszállító gondjaira bízott értékek nagyságával egyenes arányban a rajtaütésszerű támadások veszélye is fokozottan fennáll. A szolgálat ellátása jellemző módon többnyire fegyveresen történik, a szállítóeszközök jobb esetben megerősítettek (páncélozottak), amely miatt egészen más menettulajdonságokkal rendelkeznek mint hagyományos társaik.

A pénz- értékszállítási vagy kíséresi szolgálat ellátása során is rengeteg olyan meghatározó szakmai tapasztalat birtokába kerül a testőrjelölt, amelyek nélkülözhetetlenek lesznek számára a személyvédelmi megbízás teljesítése folyamán. A gyalogos vagy járművel történő kísérés, szállítás szakmai protokolljainak elsajátítása a következő tanulási-fejlődési lehetőségeket kínálja:

- az átadás-átvétel helyszíneinek biztosítását, a nyílt és rejtett ellenséges megfigyelésük megakadályozását, elhárítását
- az útvonaltervezés lényeges elemeinek kidolgozását: a lehetséges közlekedési, alternatív és menekítési útvonalak kijelölésének szempontjait és a bejárásukra, előzetes ellenőrzésükre vonatkozó követelményeket
- a potenciális megfigyelési, elrejtőzési és rajtaütési helyek (kockázati pontok) releváns paramétereinek feltérképezését (útakadályok, nehezen belátható kereszteződések, szinteltolások, éles sarkok és kanyarok, dús vegetáció az út mentén)
- az útba eső védett helyek kiválasztására vonatkozó szempontrendszer kialakítását (rendőrség, laktanya, követségi épület, egyéb őrzött objektumok)
- a szállító- vagy kísérijármű gondos felkészítését célzó intézkedéseket (teletankolt jármű, hibátlan műszaki állapot, rendben lévő okmányok, előzetes technikai átvizsgálás elvégzése)
- a gépjárműbe telepített tájékozási, kommunikációs és védelmi rendszerek használatát
- a nyílt terepen alkalmazandó támadáselkerülési illetve elhárítási stratégiák kidolgozását (követés detektálása, felkészülés az irányított ütközésekre, a színlelt közlekedési balesetekkel, álrendőrökkel szembeni cselekvési rend rögzítése)
- az életmentést szolgáló elsősegélynyújtás önálló alkalmazását
- speciális gépjárművezetési technikák elsajátítását (offenzív-defenzív-evazív vezetési módszerek)
- járműves kísérés esetében a biztonsági gépjárműoszlopban, védelmi alakzatokban történő közlekedés rutinjának kialakítását
- előőrs alkalmazását a közlekedési útvonalon való zavartalan haladás biztosítására, a primer tervtől való eltérésre okot adó körülmények jelzésére

A SZEMÉLYVÉDELEM ELLÁTÁSÁHOZ SZÜKSÉGES KÉSZSÉGEK ÉS KÉPESSÉGEK

A fentiekben nyomon követhettük, hogy a magánbiztonsági szektor személyvédelmi területén dolgozni kívánó testőrjelöltnek milyen utat kell bejárnia a szakmai ranglétrán – a tényleges személyvédelmi munkáit megelőzően – ahhoz, hogy a megszerzett tudásának köszönhetően alaposan felkészült, felelősségteljes döntéseket hozni és végrehajtani képes testőr válhasson belőle. Ezzel párhuzamosan rendelkeznie kell a foglalkozása jogi-, szakmai-, és etikai protokolljaihoz igazodó olyan készségekkel és képességekkel, amelyek megfelelő alkalmazása révén lehetővé válik számára a tevékenységének tartósan magas színvonalon történő gyakorlása.

Elöljáróban tekintsük át röviden a készségek és a képességek közötti disztinkciókat:

A készségek a cselekvés automatikus, többnyire a tudat közvetlen irányítása nélkül működő elemei. Általában olyan kevésbé összetett cselekvések vagy kisebb cselekvési egységek amelyek egy hosszabb folyamat eredményeképpen, jellemzően tanulás vagy gyakorlás révén fejlődnek ki. Egyes szerzők megkülönböztetnek tanulható és nem tanulható készségeket, az utóbbiakat a tehetség absztrakt kategóriája alá sorolva. Az egyéni teljesítmények volumene azonban a veleszületett talentum hiányában is – mentális, lelki vagy

fizikai korlátozó tényezők nélkül – kellő elhivatottsággal, kitartással és szorgalommal bizonyos mértékig fejleszthető.

A képességek az egyénnek a tevékenységekben, cselekvésekben megnyilvánuló tudása. Az adottságok alapján és a tevékenység gyakorlása révén fejlődnek ki. A készségekkel összevetve a képességekben jelentősebbek a gondolkodási összetevők és a tudati irányítás.[3]

Az adott tevékenység elemzése során a készségek inkább a cselekvés, a képességek pedig inkább a személy jellemzőjeként fogalmazhatók meg.

A következő szövegpanelek a személyvédelem ellátásához szükséges legfontosabb készségek és képességek pozitív enumerációját adják, alkalmazási területüket egy-egy példával illusztrálva.[4]

Készségek

- kommunikációs készség – szóbeli, írásbeli, szövegértés (a VIP személy együttműködésre való felkészítésénél, a megkötendő megbízási szerződés tartalmának meghatározásánál)
- elemzési-értékelési-következtetési-visszacsatolási készségek (a veszélyeztetettségi szint felmérésénél, az egyes kockázati tényezők meghatározásánál)
- tervezési készség (az útvonaltervek kialakításánál)
- szervezési készség (a rendezvényhelyszínek előzetes tűzszerész átvizsgálásának alkalmával)
- idegen nyelv-ismereti készség (a külföldi utazás előkészítésénél és biztosításánál)
- meggyőzőkészség (a védett személy biztonságát szolgáló intézkedések szükségessége mentén való érvelés kapcsán)
- kapcsolatteremtő-fenntartó készségek (a védett személy családtagjaival és közvetlen munkatársaival kialakított személyes kontaktusok vonatkozásában)
- együttműködési készség (a védelmi egység tagjai között és a biztosításban részt vevő más szervekkel, szervezetekkel)
- alkalmazkodási készség (a biztosítási érdekek és a védett személy egyéni igényeinek kompromisszumos összehangolása kapcsán)
- motiváló készség (a biztosításban részt vevő egyéb szereplők hasznos és hatékony együttműködésre ösztönzésénél)
- vezetői-irányítási készségek (a védelmi egység belső vezetése és külső irányítása kapcsán)
- konfliktusmegelőző illetve megoldó készségek (a védett személy ellenséges megfigyelésének detektálása, elhárítása idején)
- megfigyelési készség (a potenciális támadók tömegből történő kiszűrésénél)
- tájékozódási készség (a menekítési utak és helyiségek kijelölése és megközelítése során)
- emlékezőkészség (a VIP személy környezetében többször felbukkanó gyanúsán viselkedő személyek észlelése kapcsán)
- kezdeményezőkészség (a támadások megelőzésére szolgáló preventív intézkedések megtételekor)
- gyors reagálási készség (a támadás elhárítása és a menekítés végrehajtása során)
- készségi szinten rögzült mozgáskoordinációk (az önvédelmi fogások, a testfedezék biztosítása a védett személynek, a fegyverkezelés, a gépjármű-vezetési technikák végrehajtásakor)

- speciális szakmai készségek (az információgyűjtés, a védelmi és híradástechnikai eszközök használatának, a szakmai dokumentációk elkészítésének, az elsősegélynyújtás végrehajtásának során)

Képességek

- a személy jellemzői (megbízhatóság, pontosság, határozottság, udvariasság)
- elhivatottság, elkötelezettség
- gyors, logikus és gyakorlatias gondolkodás
- figyelem-összpontosítás
- rendszerező és áttekintő képesség
- elővigyázatosság, körültekintés
- tudatosság
- felelősségteljeség
- helyzetfelismerés
- döntésképeség
- önállóság
- precizitás
- rugalmasság
- diszkréció, tapintat
- önfegyelem
- monotónia tűrés
- állóképesség, terhelhetőség
- érzelmi stabilitás, kiegyensúlyozottság
- mentális és fizikai felkészültség
- stressz kezelés, regenerálódás

ÖSSZEGZÉS

A fentiekben áttekintettük, hogy a magánbiztonsági szektorban testőrként dolgozni kívánó aspiránsnak a pályája során milyen szakmai területeken kell előzetesen tapasztalatokat gyűjtenie annak érdekében, hogy a jövőben felkészülten és felelősségteljesen vehessen részt személyvédelmi feladatok végrehajtásában.

Természetesen ennél a pontnál még senkiből sem válik testőr, a személyvédelem átfogó rendszerén belül is szükséges a kötelező szakmai állomásokat végigjárni. Részt kell venni – csak már a védett személyhez kötődően – először a lakóhelye, ideiglenes szálláshelye, munkahelye, rendezvényei és programjai helyszíneinek biztosításában, majd a közlekedési útvonalai kijelöléséhez, bel- és külföldi utazásai biztonsági szempontú megszervezéséhez kapcsolódó feladatok végrehajtásában is.

Végül a személybiztosításban való közreműködés – akár a védett személy, akár a családtagjai vagy egyéb hozzátartozói vonatkozásában – ennek a fejlődési ívnek a tetőpontja lehet, amennyiben az egyén az egyes részterületeken szerzett szakmai tapasztalatainak köszönhetően már rendelkezik a tevékenység ellátásához szükséges – a fentiekben kifejtett és részletesen elemzett – készségek és képességek közel teljes arzenáljával. Magabiztos felkészültségéből kifolyólag már a gondjaira bízható az egyedi és megismételhetetlen legfőbb védendő érték, az emberi élet. Ettől a pillanattól kezdve mondhatjuk azt, hogy a biztonsági szakember testőrként dolgozik, majd néhány évnyi sikeres szakmai működés után kijelenthetjük, hogy testőrré vált.

Felhasznált irodalom

- [1] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól
- [2] [3] [4] Geoffrey Padgham: Close Protection - The Softer Skills. Entertainment Technology Press, London 2006.

Bartha Tibor

bartha.tibor@uni-nke.hu

NEM HALÁLOS FEGYVEREK INTEGRÁCIÓJÁNAK HELYZETE A NATO-BAN

Absztrakt

Az 1990-es évek közepén egyre inkább felértékelődött a nem halálos fegyverek szerepe a NATO nem háborús katonai műveleteiben. Szakmai körökben sokan azt prognosztizálták, hogy ezen fegyverek meglehetősen gyorsan fognak integrálódni a tagországok fegyverzeti eszköztárába, jellegüknél fogva népszerűek lesznek és alkalmazásuk a mindennapokban egyre nagyobb jelentőséggel fog bírni. Az eltelt közel 20 év viszont pontosan az ellenkezőjét látszik bizonyítani. Azaz a fegyverek korántsem olyan népszerűek, mint azt korábban gondolták és integrálásuk a NATO tagországok fegyverzeti arzenáljába meglehetősen akadozva folyik. Jelen cikk, Cees M. Coops a NATO Védelmi Kollégiumának¹ vezető kutatója tanulmányára alapozva vizsgálja, hogy a lassú integrációs folyamat és a negatív megítélés milyen okokra vezethető vissza.

In the middle of 90's the non-lethal weapons played a great part in NATO-led Military Operation Other than War. A great many experts predicted, that these weapons had got into the service of armament systems of NATO countries quite quickly and in consequence of their nature they would be very popular in the every day routine of soldiers, however experience of the last 20 years shows just the opposite. The weapons are not very popular and the process to put these weapons in the armament service of NATO countries is very slow and lingering. This paper, based on a study written by Cees M. Coops, analyses the reasons of the above mentioned problems.

Kulcsszavak: Nem halálos fegyverek, nem halálos képesség, NATO, nem háborús katonai műveletek ~ Non-Lethal Weapons, Non-Lethal Capabilities, NATO, Military Operations Other Than War

¹ NATO Defense College

BEVEZETÉS

Az 1990-es évek közepére tehető, amikor nem halálos fegyverek alkalmazása a NATO katonai műveleteiben egyre nagyobb hangsúlyt kezd kapni. E fegyverek tervezése és később az alkalmazásuk során is elsődleges cél a halálos kimenetelű sérülések és a járulékos károk lehető legkisebb mértékre való csökkentése. Bár ez eléggé tetszetősen hangzik vagy hangozhat – főleg olyanok számára, akik a hagyományos (értsd: halálos) fegyverek alkalmazása ellen emelik fel hangjukat, – mégis tényként kell kezelni, hogy napjainkban a nem halálos fegyverek megítélése katonai körökben meglehetősen ellentmondásos és a tagországok eszköztárába való integrálásának folyamata meglehetősen lassú.

E véleményének ad hangot meglehetősen élesen és egyértelműen Cees M. Coops a NATO Védelmi Kollégiumának vezető kutatója már egy 2008-ban megjelent tanulmányában² „Ezen eszközök integrálása a NATO tagállamok eszköztárában eléggé, mondhatni gyalázatosan lassú folyamat”.

Jelen cikk a jelzett tanulmányra alapozva tárgyalja a nem halálos fegyverek NATO általi megítélését, összefoglalja és kiegészíti a tanulmány főbb – ma is érvényesnek tekinthető – megállapításait. Vizsgálja, hogy milyen okokra vezethető vissza a lassú integrációs folyamat, keresi az ellentmondások, problémák alapvető okait, illetve rámutat arra, hogy milyen előrelépés történt a kérdéskörben az azóta eltelt időben.

Nem halálos fegyverek megjelenése a NATO katonai műveleteiben

A nem halálos fegyverek megjelenése a tagállamok eszköztárába az 1990-es években inkább a hidegháború utáni politikai realitás következménye volt, mintsem katonai követelmény. Ebben az időben a NATO erőik olyan nem háborús katonai műveletekbe kerültek alkalmazásra, amelyek eltértek azoktól, amelyekre a hidegháborús időszakban alapvetően felkészítették őket. Példaként említhető a NATO béketámogató műveletei a Balkánon.

Ezen műveleteknél a parancsnokok nem hagyhatták figyelmen kívül, hogy a média mindenütt való jelenléte lehetővé tette, hogy a katonai akciók esetenkénti „brutalitásáról” a világ pillanatok alatt tudomást szerezzen. A műveletek esetleges taktikai hibái negatív hatással voltak a stratégiai célokra is, nem egy esetben kockáztatva a misszió sikerét.

A nyilvánosság nemigen tolerálta a halálos kimenetelű sérüléseket azokban a katonai műveletekben, amelyeknek alapvető célja például a béke kikényszerítése vagy éppen fenntartása volt. Erre az időszakra tehető, amikor a NATO politikai és katonai vezetői elkezdtek keresni a halálos fegyverek alternatíváját, amit meg is találtak a nem halálos fegyverekben.

A kérdés már csak az volt, hogy honnan és hogyan lehet ezeket az eszközöket belátható időn belül a katonák részére biztosítani. Merthogy az időfaktor már akkor is igen fontos tényező volt, és a kialakult helyzet nem egy esetben a katonai erő azonnali beavatkozását tette szükségessé. A nem halálos fegyvereknek külön, a katonai erő részére történő önálló fejlesztése, annak időigényessége miatt, közvetlenül nem jöhetett szóba. Maradt tehát az a megoldás, hogy a piacon elérhető eszközökből kellett kiválasztani azokat, amelyeket a lehető legrövidebb időn belül a katonák kezébe lehetett adni. Lényeges szempont volt az is, hogy a kiválasztott eszközök alkalmazása érvényben levő nemzetközi egyezményt nem sérthetett és ugyanakkor megfelelő hatékonysággal kellett rendelkezniük.

Ebben az időszakban a nem halálos fegyverek legnagyobb alkalmazói nem a katonák, hanem az egyes országok belső rendfenntartó erői voltak³. Szerencsés módon a belső

² Cees M. Coops: NATO and the challenge of non-lethal weapons – Research Paper, Research Division – NATO Defense College, Rome – No.39 – September 2008.

³ Rendőrség, csendőrség, büntetés-végrehatás szervezetei.

rendfenntartó erők által alkalmazott és a piacon beszerezhető nem halálos fegyverek döntő többsége kettős, azaz katonai és polgári felhasználású volt. Ez kedvezett is a résztvevő csapatoknak, hiszen a katonai feladatok számos esetben a rendőri munka alapelemeit is tartalmazták.

A hadsereg újonnan megjelenő igénye ösztönzőleg hatott a nem halálos fegyverek fejlesztésére és a katonai igények kielégítése kezdett prioritást élvezni. A fejlesztések olyan ütemben valósultak meg, amelyek végül egy túlkínálatot eredményeztek a piacon.

Másik jellemzője ennek az időszaknak, hogy a hagyományos katonai feladatok egyre inkább eltolódtak a nem háborús katonai feladatok irányába, mint pl.: béketámogató műveletek, humanitárius segítségnyújtás, katasztrófa-elhárítás, terrorizmus elleni harc, kábítószer elleni küzdelem, polgári hatóságok katonai támogatása, fegyverzetellenőrzés, szankciók érvényesítése stb. Ezekben a feladatokban kiemelten kezelték a halálos sérülések és a járulékos károk lehető legkisebb mértékre való csökkentését. Ezen elvárás teljesítése során a nem halálos fegyverek jelentős hangsúlyt kaptak, miután képesek voltak betölteni az egyszerű katonai jelenlét⁴ és halálos erő alkalmazása közötti „rés”-t. Alkalmazásukkal a kialakult helyzetre adható megfelelő válaszok árnyaltabbá váltak és lehetővé vált az erő arányos alkalmazása, ezáltal csökkentve a feszültség esetleges eskalációjának lehetőségét. Ma már kijelenthetjük, hogy e fegyverek alkalmazására minden kétséget kizárólag szükség volt.

A NATO 1999-es nem halálos fegyverekre vonatkozó irányelvei⁵ definiálják e fegyvereket, ugyanakkor a dokumentum kiemeli, hogy a nem halálos fegyverek nem helyettesítik, hanem kiegészítik a halálos fegyvereket, azokban az esetekben, amikor a hagyományos halálos fegyverek alkalmazása indokolatlan vagy túlzott mértékű, illetve az általuk okozott járulékos károk elfogadhatatlanok lennének. Az irányelvek egyértelmű választ adnak azokra a kritikákra, amelyek a nem halálos fegyvereket a hagyományos halálos fegyverek helyett kívánják alkalmazni⁶.

Talán a legkiemelkedőbb jellemzője a nem halálos fegyvereknek, hogy alkalmazásuk egy olyan lehetőség a parancsnokok kezében, amellyel időt nyerhetnek egy esetleges ellenséges szándék megkülönböztetésére, mielőtt a halálos fegyverek alkalmazásához folyamodnának. A nem halálos fegyverek biztosítják a parancsnokok számára a lehetőséget, hogy miután észlelték az ellenséges szándékot, elrettentsék, megakadályozzák, vagy megfutamítsák a szemben álló felet. Ha ez mégsem járna sikerrel, még mindig használhatják halálos fegyvereiket – már ha a rendelkezésre álló idő és a helyzet ezt lehetővé teszi⁷. A hagyományos fegyverek nem tudják ezt a „lélegzetvételnyi” szünetet biztosítani, a végleges döntés meghozatala előtt, mert ha az ellenséges támadás valóban kezdetét veszi, akkor az egyedüli biztonságos lehetőség a pusztító, halálos erő alkalmazása.

Törekvések a nem halálos fegyverek az integrációjára

A NATO-ban tehát, a 90-es évek közepétől elindult egy olyan folyamat, amely során a szakemberek újragondolták a meglévő fegyverzeti és technikai eszközöknek a megváltozott feladatokhoz való megfelelőségét.

A nem halálos fegyverek megváltozott feladatrendszerhez való illesztése érdekében több konferencia került lebonyolításra és számos tanulmány született. Ezek a konferenciák és tanulmányok alapvetően arra kerestek választ, hogy hogyan támogathatják a nem halálos fegyverek a NATO különböző nem háborús katonai műveleteit. A munka már 1994-ben a

⁴ Katonai erő alkalmazása nélküli késztetés

⁵ NATO Policy on Non-Lethal Weapons - DOCUMENT C-M(99)44 - NATO Unclassified - 1999

⁶ Az elmúlt több mint tíz év is kevésnek bizonyult arra, hogy a köztudatból kitöröljék azt a téves nézetet, miszerint a nem halálos fegyvereket a nem a halálos fegyver helyett, hanem azok mellett kell alkalmazni.

⁷ Meg kell azonban jegyezni, hogy erre azonban nem mindig van lehetőség.

NATO tagállamok Nemzeti Fegyverzeti Igazgatóinak konferenciáján megkezdődött, és amely közel öt év alatt vezetett el csak oda, hogy a tagországok által elfogadásra került a NATO nem halálos fegyverekre vonatkozó irányelvei. Szakértők szerint ez abban az időben egy kisebbfajta csodának számított, miután az előkészítés időszakában meglehetősen éles viták zajlottak le a fegyverek támogatói és ellenzői között.

Az irányelvek elfogadását végül is nagyban felgyorsították az Amerikai Egyesült Államok katonai egységei által Szomáliában és Haitin, valamint a NATO csapatok Balkánon szerzett tapasztalatai. Ezek a tapasztalatok egyértelmű rámutattak arra, hogy a nem halálos fegyverek képesek kitölteni a már említett „rés”-t, elsősorban a nem háborús katonai műveletekben⁸.

Az irányelvekben foglaltak megvalósítását segítették elő azok, a NATO kutatási és technológiai szervezetének⁹ (RTO) szakemberei által elkészített hosszú távú tudományos tanulmányok, amelyek a nem halálos fegyverek műszaki, alkalmazástechnikai, jogi, politikai, etikai, orvosi aspektusait vizsgálták a jövő nem háborús katonai műveleteiben. A jelentősebbek ezek közül a következők:

- Nem halálos fegyverek hatásosságának értékelése (Non-Lethal Weapons Effectiveness Assessment, RTO SAS-035¹⁰ panel, 2004);
- Nem halálos fegyverek és a jövő békekikényszerítő műveletei (Non-Lethal Weapons and Future Peace Enforcement Operations, RTO SAS-040 panel, 2006);
- Nem halálos technológiák emberi szervezetre gyakorolt hatásai (Human Effects on Non-Lethal Technologies, RTO HFM-073¹¹ panel, 2006);
- Nem halálos fegyverek hatásosságának értékelése: fejlesztés és kiértékelés (Non-Lethal Weapons Effectiveness Assessment: Development and Verification, SAS-060 panel, 2007).

A NATO vezetői felismerték, hogy a Szövetség hitele a képességeken alapul. A NATO-n belül megindult egy olyan kezdeményezés (DCI)¹², amely a katonai képességek növelését, fejlesztését célozta meg az akkor már meglévő és a várható biztonsági kihívásokra. A DCI 58 különböző képességterülettel foglalkozott, többek között a nem halálos képességekkel is. Sajnálatos módon e kezdeményezés ellenére a nem halálos fegyverek integrálása a NATO koncepciójába, és az egyes tagországok hadseregeinek fegyverzeti rendszerébe továbbra sem gyorsult fel. Az integráció sokat késett, illetve egyes tagországok esetén késik mind a mai napig.

Coops tanulmányában ezt az alábbiakkal indokolja:

- A hidegháborús gondolkodás a NATO több tagországában még hosszú ideig tovább élt (él). A NATO 1999-es stratégiai koncepciója ellenére, az „agyakban” még sok esetben rakéták és harckocsik élnek és nem olyan „szürreális” dolgok, mint például a nem halálos fegyverek;
- A DCI 58 területe közül a nem halálos fegyverek meglehetősen alacsony prioritást kaptak;
- A NATO-nak ebben az időben más, fontosabb kérdésekkel kellett foglalkoznia. Ilyen volt például a Szövetség bővítésének folyamata, Partnerség a békéért, Mediterrán Dialógus, védelmi költségvetés csökkentése, és egy későbbi szakaszban a transzformáció, NATO Reagáló Erők, Irak, Afganisztán, stb...;
- 2001. szeptember 11.-i terrortámadás után kétséget kizárólag megváltozott a NATO stratégiai gondolkodásmódja. Ellentétben az aszimmetrikus hadviseléssel, a nem

⁸ Megítélésem szerint, a háborús katonai műveletekben is vannak olyan helyzetek, amikor a nem halálos fegyverek kiemelt szerepet kaphatnak.

⁹ RTO – Research and Technology Organization

¹⁰ SAS - System, Analysis and Simulation – Tanulmányok, Elemzések és Szimuláció

¹¹ HFM – Human Factor and Medicine – Emberi Tényezők és Orvostudomány

¹² NATO Defense Capabilities Initiative (DCI) – NATO Védelmi Képességek Kezdeményezése

halálos fegyverekre – legalábbis kezdetben – nem úgy tekintettek, mint egy lehetséges és életképes választási lehetőségre;

- 2002-ben egy moszkvai színházban lezajlott túszzabadító akcióban alkalmazott altatógáz rámutatott a nem halálos fegyverek egyik problematikájára és kiélezte a már meglevő vitákat.

A moszkvai eseményeket követően az érezhetően lelassult folyamatot a NATO nemzeti fegyverzeti igazgatóinak 2006-os konferenciája próbálta felgyorsítani, amikor is létrehoztak egy szakértői csoportot, azzal a feladattal, hogy a mérje fel a területen meglévő képességeket és hiányosságokat, valamint tegyen javaslatot más NATO munkacsoportok ez irányú tevékenységére.

A munkacsoport a képességvizsgálaton túlmenően javaslatot tett arra, hogy a NATO fordítson kellő figyelmet a nem halálos fegyverek politikai, jogi és etikai kérdéseire is. Bebizonyosodott az is, hogy az eltelt évtizedben nem sok történt a fogalmi vonalon fennálló problémás kérdések, ellentmondások feloldására. Fontos volt annak kimondása is, hogy a nem halálos fegyverek integrálásának folyamata a NATO koncepciókba, stratégiákba, doktrínákba eléggé kezdeti stádiumban van. Megállapították, hogy az eltelt időszakban a nem halálos fegyverek tudományos és technikai oldaláról számos értékes és szükséges tanulmány készült, és az ilyen típusú tanulmányok készítését továbbra is folytatni kell.

Megfogalmazásra került az is, hogy a nem halálos fegyverek integrációjának és alkalmazásának legfőbb gátlótényezői továbbra is jelen vannak, és felszámolásuk a nyilvánosság, a jog és a politika területeken még nem kezdődött el.

Az integráció során jelentkező főbb akadályok, ellentmondások

Az elmúlt közel két évtized tapasztalatai azt mutatják, hogy a nem halálos fegyverek alkalmazása jelentősen csökkenti az áldozatokat, és a járulékos károkat. Egyúttal joggal merül fel az a kérdés, hogy akkor mégis miért olyan ellentmondásosak ezek a fegyverek?

Erre teljesen egzakt választ nem lehet adni, viszont meg lehet kísérelni néhány okot, problémát feltárni, amelyek megoldásával talán segíteni lehet e fegyverek pozitív megítélésében.

Néhány létező probléma felvetése előtt el kell mondani, hogy azon relatív rövid időszak, ami a nem halálos fegyverek katonai alkalmazását jellemzi számos siker könyvelhető el. Szomália és a Balkán katonai műveletei bizonyították, hogy a nem halálos fegyverek alkalmazásával elkerülhető az esetleges vérontás, csökkentve a feszültség további eszkalációját.

Coops lényegesnek tartja – és ezzel csak egyetérteni lehet –, hogy fel kell tární és el kell mondani a nem halálos fegyvereknél meglévő ellentmondásokat, problémákat azért, mert így nagyobb eséllyel lehet e fegyvereknek jogosultságot és elfogadottságot szerezni a politikusoknál, a közvéleményben, valamint a hadseregben. Ez azért is fontos, mert a másik oldalról a kutatók, fejlesztők jobbnál jobb eszközök kifejlesztésével folyamatosan hozzájárulnak a már amúgy is meglévő széles spektrumhoz. Nézzünk meg néhány meglévő problémát, ami a nem halálos fegyverek körül kialakult.

Az első probléma maga az elnevezés. Már a kezdetekben bebizonyosodott, hogy a nem halálos fegyver megnevezés helytelen. Ugyanis a *nem halálos* kifejezés azt sugall(hat)ja, azt a hamis képzetet kelt(het)i, hogy ezekkel a fegyverekkel nem lehet ölni, ezt pedig nyilvánvalóan nem igaz. Számos egyéb – talán helyesebb – javaslat merült már fel, pl.: életre kevésbé veszélyes fegyver, harcképtelenné/cselekvésképtelenné tevő fegyver stb., de mindezülig valamennyi elnevezés elbukott. Másik javaslat a „fegyver” szó elvetése volt, már csak azért is, mert a fejlesztők által megalkotott eszközök döntő része valójában nem fegyver. Ezért sokkal találóbb lenne a „rendszer”, „technológia” vagy „képesség” szavak használata.

Ebben a vitában jelentett áttörést 2009-ben, a NATO nem halálos képességekre vonatkozó Fehér Könyve¹³. A Fehér Könyv újradefiniálta a nem halálos fegyvereket és bevezette a nem halálos technológia kifejezést, amely ezt követően egyre inkább elfogadottabbá kezdett válni a NATO-ban.

Az 1999-es irányelvek a következő definíciót adták: „A nem halálos fegyverek azok a fegyverek, amelyeket kifejezetten azzal a céllal terveztek és fejlesztettek ki, hogy harc- vagy cselekvésképtelenné tegyék az ellenséges személyeket, elhárítsák azok támadásait lehetőleg úgy, hogy alacsony valószínűséggel okozzanak halálos kimenetelű vagy maradandó sérülést, valamint, hogy működésképtelenné tegyék a különböző haditechnikai eszközöket, felszereléseket minimalizálva a nem kívánt környezeti károkat vagy hatásokat”

2009-ben a Fehér Könyv már így fogalmaz: „nem halálos fegyver, amelyet kifejezetten azzal a céllal terveztek és elsősorban úgy alkalmaznak, hogy harc- vagy cselekvésképtelenné tegyen személyeket és működésképtelenné tegyen haditechnikai eszközöket, felszereléseket minimalizálva a halálos kimenetelű vagy maradandó sérüléseket és károkat a vagyontárgyakban és környezetben”. Látszik, hogy a definícióban az alkalmazói szándék már kellő hangsúlyt kap.

A Fehér Könyv bevezeti a nem halálos képesség fogalmát is, mely szerint: „a nem halálos képesség olyan képesség, amelyek kimondottan úgy alakítottak ki, hogy releváns katonai hatást fejtsenek ki személyekre, felszerelésekre, eszközökre és infrastruktúrára, a halálos kimenetelű vagy maradandó sérülések, valamint az infrastruktúrában és a környezetben a nemkívánatos károk okozásának jelentősen alacsonyabb szintű kockázatával, összevetve azzal, amely elvárható lenne, ha ugyanazt a feladatot hagyományos fegyverek alkalmazásával hajtották volna végre.”

A definícióból látható, hogy a nem halálos képesség nem az a kifejezés, amely a nem halálos fegyvereket helyettesítené. Ezért tehát úgy tűnik, hogy a nem halálos fegyverek elnevezés, mint pontatlan terminológia továbbra is megmarad.

Korábban – sőt egyes helyeken még ma is –, a csoportosításra vonatkozó változatok között meglehetősen extrém kategorizálást is lehetett, illetve lehet találni, amelynél olyan eszközöket is a nem halálos fegyverek közé soroltak, amelyek nyilvánvalóan nem tartoztak a kategóriába soha. A parttalan vita lezárásaként a NATO 2009-ben kiadott Fehér Könyve végre egyértelműen meghatározza, hogy milyen eszközöket nem tekint nem halálos fegyvernek vagy képességeknek. Ezek a következők:

- az információs hadviselés eszközei;
- a pszichológiai hadviselés eszközei;
- az elektronikai hadviselés eszközei;
- azon rendszerek, amelynek elsődleges funkciója az adott célpont megsemmisítése, ugyanakkor ezen elsődleges hatásuk mellett képesek a lehető legnagyobb mértékben minimalizálni a járulékos károkat;
- felderítő, megfigyelő, célazonosító és vizuális megfigyelő (Intelligence Surveillance Target Acquisition and Reconnaissance – ISTAR) eszközök, rendszerek, valamint – éjszakai megfigyelő és célazonosító (Surveillance Target Acquisition Night Observation – STANO) eszközök, rendszerek;
- hagyományos fegyverek, nem halálos módon való alkalmazása;
- személyi-, túlélőképességet biztosító védőfelszerelések.

A nem halálos fegyverek körül kialakult ellentmondás második és talán a legfontosabb kérdése a definíció interpretációja, értelmezése. A NATO új definíciója bár szélesebb körben, de még egyáltalán nem teljes mértékben elfogadott.

¹³ Non-Lethal Capability White Paper – NATO Army Armaments Group TG/3 – PFP(NAAG-TG/3)WP – (2009)0001

A vita elsősorban a szándékolt hatáson van szembeállítva azzal a hatással, amit ezen fegyverek a gyakorlatban, az alkalmazásuk során mutatnak. Támogatók rámutattak, hogy a nem halálos fegyverek a tervezés – azaz az általuk elérendő cél – szempontjából és etikailag valóban különböznek a halálos fegyverektől. Ellenzők ugyanakkor vitatják, hogy a tervezési szándékból adódó különbség automatikusan etikai fölényt is jelentene.

Ellenzők azt is erősen kifogásolják – tegyük hozzá joggal –, hogy még nem állnak rendelkezésre olyan egzakt vagy közel egzaktnak mondható mérési adatok¹⁴, sőt még elegendő gyakorlati tapasztalat sem áll rendelkezésre, amelyek alapján egyértelműsíteni lehetne, hogy ki vagy kik ellen, milyen körülmények között és hogyan lehet és kell az egyes kategóriákba tartozó nem halálos fegyvereket alkalmazni. El kell ismerni, hogy mindig is problémát okozott e fegyverek hatásainak és hatásosságának pontos mérése, igaz ez természetesen az új generációs nem halálos fegyverekre is¹⁵. El kell fogadni tényként azt is, hogy azon tényezők meghatározása, amelyek lehetővé tennének a hatás és a hatásosság egzakt mérését az egyes nem halálos fegyverek vonatkozásában, még eléggé gyermekcipőben jár. Ezért az egyes fegyverek hatását és szakszerű használatának tényét bizonyítani meglehetősen bonyolult (nem lévén adekvát mérőszámok) és ezt a problémát pedig a nem halálos fegyverek sérültjeinek ügyvédjei kíméletlenül ki is használják, bár a legtöbbször az ő álláspontjuk is meglehetősen mesterkelt.

Felvetődik az a kérdés, hogy mielőtt a szóban forgó fegyvert nem halálos fegyverré minősítenék (értsd: ebbe a kategóriába sorolnák) egyáltalán szükséges-e, lehetséges-e vagy követelmény-e olyan paraméterek meghatározása, vagy mérési módszerek kidolgozása, amelyek alapján biztosan állítható, hogy az adott fegyver nagy valószínűséggel nem okoz halálos vagy maradandó sérüléseket. Vagy elegendő megelégedni azzal a ténnyel, hogy szakszerű alkalmazásuk esetén sokkal kisebb valószínűséggel okoznak halálos sérüléseket, mint a hagyományos fegyverek.

Problémát jelent az is, hogy jelenleg sehol sem fogalmazódik meg kritériumként, miszerint a nem halálos fegyverek alternatívát biztosítanak a halálos fegyverek helyett.

E fegyvereket „nem halálos” tulajdonságaik miatt meglehetősen sok helyen méltányolják. A fegyverek ezen tulajdonsága vezetett azon paradox helyzethez, hogy a bennük rejlő képesség miatt, – miszerint jelentősen csökkentik a halálos kimenetelő sérüléseket és a maradandó sérüléseket –, az elfogadottságuk sokkal inkább ellentmondásosabb, mint a halálos fegyvereké. Mit kell értetünk ezalatt? Nos, ha egy nem halálos fegyver alkalmazásától a célszemély halálos sérülést szenved, az óriási felháborodást és visszhangot kelt, mivel a fegyver megnevezéséből fakadóan ennek nem lett volna szabad bekövetkeznie. Hogy lehetséges az, hogy egy nem halálosnak mondott eszköz mégis halált okoz? Nincs azzal viszont senkinek semmi problémája, hogy ha egy halálos fegyver okoz halálos sérülést – hiszen ez a dolga, ezt a hatást várták tőle.

A nem halálos fegyverek körül kialakult vita a háború és a fegyveres konfliktus között meglévő különbségekre is visszavezethető.

A legpusztítóbb fegyverek vonatkozásában a 19. és 20. századi háborúkban az államok között nemzetközi szándékként jelent meg, hogy szabályozzák, korlátozzák, vagy éppen tiltsák bizonyos fegyverek használatát. Ez a törekvés számos közismert nemzetközi egyezményt és megállapodást eredményezett.

¹⁴ Legalább is az adatok vagy ismeretlenek vagy elégtelenek.

¹⁵ Lényegében ezen hiányosság kiküszöbölésére hozták létre a Non-Lethal Weapons Effectiveness Assessment: Development and Verification (SAS-060) munkacsoportot.

A nemzetközi hadijog a nemzetközi humanitárius jogra alapozva, szabályozza a *ius in bello*¹⁶-t és egyértelműen korlátozza az erő alkalmazását háborús körülmények között, valamint tárgyalja a katonai szükségesség elvét, az emberiség elvét, a megkülönböztetés elvét, valamint az arányosság elvét.

Ezt a szándékot fokozatosan igyekeznek kiterjeszteni fegyveres konfliktusokra is, amelyeket a felek viszont a szó szoros értelmében konfliktusnak és nem háborúnak tekintenek. Lényeges kérdés tehát, hogy fegyveres konfliktusok esetén a felek mennyire tekintik magukra nézve kötelezőnek a háborúra vonatkozó egyezményeket és mennyire nem. Mi történik akkor, ha az egyik fél nem fogadja el és tartja be ezeket az elveket? Különös kiemelt jelentőségű e kérdés tisztázása az alkalmazott fegyverek tekintetében. Hát még olyan fegyverek tekintetében, amelyekre ilyen konvenciók még nem is léteznek.

További problémát jelent, hogy előrejelzések szerint az elkövetkező évtizedekben számos olyan korszerű nem halálos fegyver kerül a piacra, amelyek egyrészt küzdenek a már leírt problémákkal¹⁷, és ugyanakkor használatukra vagy korlátozásukra még semmilyen nemzetközi egyezmény nem született pl.: akusztikus, elektromágneses vagy kinetikus eszköz.

A nem halálos fegyverek egy újabb problematikus kérdése nem is igazán magukban a fegyverekben, mint inkább a katonai erő alkalmazásának kérdésében rejlik. A nemzetközi jogi törvények szerint, a katonai erő adott országon kívüli rendfenntartó feladatokra történő alkalmazása csak meghatározott esetekben és körülmények között engedélyezett. Ugyanis a rendfenntartás az adott ország belső jogi szabályozására alapul. Egy ország belső jogi szabályozása pedig másik országra csak akkor vonatkozhat, ha abba a másik ország is beleegyezik. Békefenntartás egy másik szuverén állam területén vagy annak kérésére vagy az ENSZ BT határozata alapján lehetséges – legalább is a nemzetközi törvények ekkor tekintik legitimnek.

A békefenntartó műveletek során a törvényesség és rend fenntartása a katonai oldal egyik nagy kihívása. Lényeges kérdés, hogy ilyen helyzetekben a katonai feladatokhoz milyen eszközök, fegyverek alkalmazhatók. Vegyünk példaként az ilyen helyzetekben gyakran alkalmazott nem halálos fegyvert, a könnygázt.

A vegyifegyverek kifejlesztésének, gyártásának, felhalmozásának és használatának tilalmáról, valamint megsemmisítéséről szóló egyezmény¹⁸ jogérvényesítésre, beleértve hazai/belső rendfenntartó célokra engedélyezi ezen anyagok használatát. Azaz egy adott ország rendfenntartó erői – hazai területen – tömegoszlátási céllal használhatnak például könnygázt. Ugyanakkor nem használhatják a könnygázt katonák ellen, még akkor sem, ha azok polgári személyeket élő pajzsként használják.

A helyzetet tovább bonyolítja, ha a szemben álló fél harcosai nem definiáltak, mert például polgári lakossággal keveredve vannak jelen, mintegy elrejtőzve köztük – ebben az esetben a hazai vagy akár a nemzetközi erők egy nehezen megoldható helyzettel állnak szemben. Bár a tömegoszlátás egy világos feladat, de hogyan lehet vagy célszerű kezelni ezt a helyzetet? Fenntartani a törvényes rendet, pl. könnygáz alkalmazásával – mint klasszikus tömegoszlátó eszközzel – vagy esetleg várni, míg valamelyik tömegben elrejtőzött „harcos” tüzet nyit? Ekkor viszont már érvényes 1997. évi CIV. Törvény I. cikk 5. pontja, miszerint „Minden részes állam vállalja, hogy hadviselési módszerként nem alkalmaz vegyi kényszerítő eszközt”. Ennek folyománya, hogy ha a könnygáz használata ebben az esetben már tiltott, – és más nem

16 A nemzetközi hadijogot vizsgálva két fontos terület a háborúhoz való jog (*ius ad bellum*), amely az általános nemzetközi jog szabályozási területe, valamint a háborúban alkalmazott jog (*ius in bello*) a nemzetközi humanitárius jog szabályozási területe. A témát tekintve a másodiknak van nagyobb jelentősége.

17 Hatás, hatásosság egzakt mérése

18 Hazánkban az 1997. évi CIV. Törvény: A vegyifegyverek kifejlesztésének, gyártásának, felhalmozásának és használatának tilalmáról, valamint megsemmisítéséről szóló, Párizsban, 1993. január 13-án aláírt egyezmény kihirdetéséről.

halálos fegyver nem vethető be – akkor csak a halálos fegyverek alkalmazása jöhet számításba, mint lehetőség? A helyzetet tovább bonyolíthatja, ha a műveletben résztvevő különböző nemzetek erőinek más és más hazai/belső szabályzóik vannak, amelyek megengedik, vagy tiltják bizonyos ingerlő harcanyagok (pl. könnygáz) alkalmazását. Az is előfordulhat, hogy az egyes országokban eltérőek az eszközre vonatkozó alkalmazási szabályozók is, amely szintén ellentmondást is eredményezhetnek.

Ilyen jellegű problémák kiküszöbölésére már több területen megindult vagy már megvalósult egyfajta harmonizációs folyamat, de a nem halálos fegyverek területén ez még meglehetősen hosszú folyamatnak ígérkezik.

A NATO ennek ellenére továbbra is kiemelten kezeli a nem halálos fegyvereket, támogatja azok alkalmazását és a nemzetközi jogi küzdelem bonyolultsága ellenére, arra ösztönzi a tagállamokat, hogy próbálják áthidalni a fennálló problémákat és az egyes tagországok hazai szabályzóinak harmonizálásával igyekezzenek megszüntetni a fennálló különbségeket.

A NATO 1999-es irányelvei ugyanakkor hangsúlyozzák azt is, hogy „a nem halálos fegyverek kutatásának és fejlesztésének, a beszerzésének, valamint alkalmazásuknak, minden esetben következetesnek kell maradniuk az érvényes nemzetközi egyezményekkel, szerződésekkel és a nemzetközi joggal, különös tekintettel, a nemzetközi hadijoggal, valamint a jóváhagyott műveleti-végrehajtási szabályokkal (továbbiakban: RoE)¹⁹.

A nem halálos fegyverek és a műveleti-végrehajtási szabályok

A nem halálos fegyverek alkalmazása tekintetében az egységesítésre való törekvés elsősorban azon országokban haladt előre látványosan, amelyek e fegyverek fejlesztésével intenzíven foglalkoznak²⁰. Sajnálatos tény, hogy a többi ország – bele értve a PfP országokat is – igen csekély érdeklődést mutat a nem halálos fegyverek irányt. A NATO-n belüli képességekülönbség a nem halálos fegyvereket illetően csak növekszik, fenyegetve ezzel az interoperabilitást. Többnemzetiségű műveletekben különösen fontos a résztvevő egységek megfelelő kiképzettsége, amely magába foglalja azt is, hogy mindenki tudatában van az általa alkalmazott fegyver, eszköz alkalmazástechnikai sajátosságaival, előnyeivel, hátrányaival. A nem halálos fegyverek alkalmazása ugyanis többet jelent, mint a „hogyan” kérdésének megválaszolása. Ugyanis ezen eszközök az erő alkalmazásának folytonosságában más-más szinteken foglalhatnak helyet.

A hagyományos hadviselésben a RoE korlátokat jelent a halálos erő alkalmazása tekintetében. Többnemzetiségű műveletekben a közös RoE sok esetben akár megosztó kérdés is lehet. Még akkor is, ha közös cél vezetett ahhoz a döntéshez, hogy egy adott műveletet végrehajtsanak. A nemzeti politikai megfontolások vagy kifogások akár a csapatok alkalmazásának korlátozását is eredményezhetik. Politikusoknak kiemelt szerepet kellene vállalniuk abban, hogy egy adott katonai művelethez való csatlakozást megelőzően meggyőzzék a választópolgárokat a részvétel szükségességéről. Lényeges annak hangsúlyozása is, hogy a műveletben alkalmazott technikai eszközök biztosítják a minimális kockázatot²¹, illetve lehetőséget biztosítanak arra, hogy minimálisra csökkentésük a halálos áldozatok számát és az anyagi javakban okozott károkat. Ezt persze politikusok nem szívesen vállalják fel. Mert ha egy előre nem látott esemény miatt mégis a „legrosszabb forgatókönyv” jönne be, és a halálos áldozatok száma több lenne, mint ami „előre várható” volt, akkor bizony szembe kellene állni a választókkal és megmagyarázni a történeteket, esetleg vállalni a politikai és erkölcsi felelősséget is.

¹⁹ Rules of Engagement (RoE) - több fajta megnevezés is létezik e fogalomra pl.: harcérintkezési szabályok, harci alkalmazási szabályok, erő alkalmazásának szabályai stb...

²⁰ Elsősorban az Amerikai Egyesült Államokban, és kisebb mértékben az Egyesült Királyságban.

²¹ Mind a csapatok, mind polgári lakosság tekintetében

A közös RoE hiánya tehát a NATO-n belül nem egy esetben problémát jelenthet. A nem halálos fegyverek megjelenése pedig csak tovább bonyolítja a helyzetet. Többen szorgalmazták a nem halálos fegyverekre vonatkozó RoE kidolgozását, amely azért is lenne eredmény, mert ezen fegyverek alkalmazási küszöbe alacsonyabb, mint a halálos fegyvereké. Sőt az igazság az, hogy a nem halálos fegyverekre vonatkozó RoE-t inkább kombinálni lenne célszerű a halálos fegyverekre vonatkozó RoE-vel, így a katonák is inkább megértenék a fegyverek lényegét és jobban tudnának azonosulni velük.

Nem halálos fegyverek és közvélemény

Függetlenül a tervezői és az alkalmazói szándéktól, ki kell mondani, hogy a nem halálos fegyverek elfogadottsága általában és döntően negatív. Néhány olyan eset, amelyekben a fegyverek alkalmazása súlyos sérülésekhez vagy halálhoz vezetett hosszú ideig tovább él a közvélemény tudatában.

Valahányszor, ha például egy Taser²² alkalmazását követően halál következik be, a hír meglehetősen nagy nyilvánosságot kap, kihangsúlyozva az eszköz negatív vonatkozását. Nem egy esetben a „mindenhez értő” média műszaki-technikai szempontból – tudatosan vagy hozzá nem értésből – teljesen valótlan állításokkal még inkább elferdíti a valóságot. Azt persze igen ritkán kap nyilvánosságot, hogy az évek során hány ember köszönhette életét annak, hogy megfékezésükre halálos fegyverek helyett Taser-t alkalmaztak.

A nem halálos fegyverek alkalmazásának legrosszabb esete következett be 2002. októberében Moszkvában, a Melnyikov utcai színházban, amikor csecsen terroristák kb. 900 túszt ejtettek foglyul. Ez egy „nem-nyerő” helyzet volt az oroszoknak. A biztonsági erők egy cselekvésképtelenséget okozó altatógázt²³ juttattak be a színházba mielőtt megrohamozták azt. Megölték az összes terroristát és megmentették a túsztok többségét, de sajnos 129-en a fentanyltól szintén meghaltak. Az áldozatok többsége a rohamot követő nem megfelelő orvosi ellátás hiányának köszönhette halálát, amely mulasztásért Moszkva elég sok bírálatot kapott. Habár a nemzetközi jogi szakértők általában egyetértenek abban, hogy a fentanyl alkalmazása törvényes volt²⁴, ennek ellenére az akció közvélemény általi megítélése meglehetősen negatív volt.

Az olyan eszközöket, amelyek – legalább is a nevükben – nem halálosak és mégis „ölnek”, nehéz eladni vagy inkább beadni a közvéleménynek és a médiának. Úgy tűnik, hogy a nem halálos fegyverek eléggé szenvednek ettől az általános és szükségszerű mellékkörülménytől.

A nem halálos fegyverek, mint terminológia tehát egy oximoron²⁵ és a „nem halálosság” egyáltalán nem garantált. Bár a NATO irányelvei ebben is világosan fogalmaznak: „a nem halálos fegyvereknél nem követelmény a halálos kimenetelű sérülések vagy a maradandó sérülések teljes kizárása...”, ez az üzenete a dokumentumnak kevésbé ismert, és ha talán ismert is, de az általános közvélemény által rosszul értelmezett. A hangsúlyt az áldozatokra tenni, mintsem inkább a megmentett életekre, nem egészen segíti az avatatlanok eligazodását a témakörben.

Ha a politikai vezetők valóban elkötelezettek a halálos kimenetelű sérülések és a járulékos károk csökkentésében, akkor segíteniük kell megértetni a közvéleménnyel a nem halálos

²² Kilőhető elektródás elektromos sokkoló

²³ A támadás során egy a heroinnál sokkal erősebb, M99 nevű, fentanyl és ópium származékot vetettek be. A gáz túladagolása légzésbénulást, keringésbeli, szív- és máj-problémákat okozhat. Nyugati források szerint ez az eset volt az M99 főpróbája.

²⁴ Ugyanis az extrém helyzetben a nem halálos fegyver hiánya esetén a halálos fegyverek alkalmazása még több áldozattal járt volna.

²⁵ Ellentétes értelmű szavak kapcsolása.

fegyverek lényegét, alkalmazásának szükségességét, megnyerve támogatásukat, mint elengedhetetlen feltételt. A kommunikáció tehát a kulcstényező.

Nehéz vitába szállni Coops azon véleményével, hogy a jövő víziójának nyilvánvaló hiánya, valamint számos előre nem látott akadály nagymértékben felelős azért a tényért, hogy a NATO nem halálos fegyverre vonatkozó irányelvei még nem kerültek be a Szervezet stratégiai gondolkodásának fő áramába. Mint olyan, egy egyedül álló, minden támasz nélküli irányelv marad, mintegy rohanva a marginalizálódás felé, amely egyszer talán feledésbe is merülhet.

Az 1999-es irányelvben ugyan megfogalmazásra kerül, hogy a NATO tervezőinek gondoskodniuk kell, hogy a nem halálos fegyverek potenciális részvételét teljes mértékben vegyék figyelembe már tervezés folyamatában. Ez a szándék viszont ma, alig ha tekinthető megvalósultnak.

A technológiai fejlődés csak tovább növeli az egyenlőtlenséget a Szövetségen belül a nem halálos fegyverek területén, különösen a lehetséges alkalmazási területek tekintetében.

A konfliktusok megváltozott természete is rámutat, hogy a nem halálos fegyverek NATO integrációjára sürgősen szükség van, továbbá, hogy a már elavult irányelvek felülvizsgálatát is meg kell kezdeni. A nem halálos fegyverek nem jelentenek általános gyógyírt, amely mindenre jó, de e fegyverek hozzájárulását az elfogadott stratégiai célokhoz, valamint az a politikai kényszer, hogy csökkenteni kell a halálos sérülések számát és a járulékos károkat a NATO műveletekben, többé már nem lehet figyelmen kívül hagyni.

Felhasznált irodalom

- [1] Cees M. Coops: NATO and the challenge of non-lethal weapons – Research Paper, Research Division – NATO Defense College, Rome – No.39 – September 2008.
- [2] NATO Policy on Non-Lethal Weapons – www.nato.int/docu/pr/1999/p991013e.htm - letöltve: 2012. május 21.
- [3] Non-Lethal Capability White Paper – NATO Army Armaments Group TG/3 – PFP(NAAG-TG/3)WP – (2009)0001
- [4] 1997. évi CIV. törvény: A vegyifegyverek kifejlesztésének, gyártásának, felhalmozásának és használatának tilalmáról, valamint megsemmisítéséről szóló, Párizsban, 1993. január 13-án aláírt egyezmény kihirdetéséről.
- [5] NATO kézikönyv – Stratégiai és Védelmi Kutatóintézet, Budapest, 1999

Szabó Sándor – Földi László – Berek Tamás

szabosan@yahoo.com – foldi.laszlo@uni-nke.hu – berek.tamas@uni-nke.hu

LATEST CBRN DECONTAMINATION TECHNOLOGY AT THE HUNGARIAN DEFENCE FORCES

Abstract

At the age of asymmetric warfare the CBRN¹ threat level has been increasing and the importance of CBRN decontamination is more revaluated. At the beginning of the 21st century, modern CBRN procedures and devices appear in the world, which represent more effective technologies. The Hungarian Defence Forces is committed to develop their own CBRN decontamination technology according to the principles of NATO STANAG's. New decontamination procedure has naturalised with bringing the DECOCONTAIN 3000 GDS system into service, which is capable of taking out the old fashioned, outdated technology and making an appearance of a new operational capability possible. The examination of technology and procedure could demonstrate at the subunit level that the new decontamination system is able to face the CBRN challenges at the present time.

Az aszimmetrikus hadviselés korában az ABV fenyegetettség szintjének emelkedésével az ABV mentesítés jelentősége is felértékelődik. A 21. század elején korszerű mentesítési eljárások, eszközök jelennek meg a világban, amelyek hatékony technológiát képviselnek. A Magyar Honvédség elkötelezett a saját ABV mentesítési technológia fejlesztésében a NATO STANAG alapelvek szellemében. A DECOCONTAIN 3000 GDS berendezés rendszeresítésével olyan új mentesítési eljárás honosodik meg, mely képes kiváltani a régi, elavult technológiát és egy új műveleti képesség megjelenését teszi lehetővé. Az alegységszintű technológiai- és eljárás vizsgálat bebizonyította, hogy az új mentesítő eszközrendszer a kor ABV kihívásaival képes megbirkózni.

Keywords: CBRN decontamination, asymmetric warfare, Hungarian Defence Forces DECOCONTAIN 3000 GDS system. ~ ABV mentesítési eljárás, aszimmetrikus hadviselés, Magyar Honvédség, DECOCONTAIN 3000 GDS rendszer.

¹ CBRN – Chemical, Biological, Radiological and Nuclear, formerly called NBC (Nuclear Biological, and Chemical) referring to the types of Weapons of Mass Destruction (WMD). The new CBRN abbreviation stands in order of dangerousness, as chemical threat is the most seriously possible.

INTRODUCTION

Since the attacking enemy force usually has the initiative in terms of where and when it will attack, a defending commander must take a wide range of actions to protect his forces from losses due to enemy actions. These steps include ensuring all-around defence, among other things, NBC (or, in latest terms, CBRN) defence. In the course of offensive operation the surprise, concentration, tempo, and audacity characterize the offense. The commander manoeuvres his forces to advantageous positions before contact. [1]

The rapid and accurate conduct of decontamination activities is very important both in defence and in offense in order to help commanders maintaining combat power and manoeuvre flexibility.

CBRN contamination may cause casualties, degrade performance, slow manoeuvres, restrict terrain and disrupt operations. CBRN decontamination prevents the erosion of combat power and reduces possible casualties resulting from inadvertent exposure or failure of protection. Decontamination allows commanders to sustain combat operations. Decontamination principles involve:

- conducting decontamination as quickly as possible;
- decontaminating only what is necessary,
- decontaminating as far forward as possible, and
- decontaminating by priority. [2]

Use of CBRN weapons creates unique residual hazards that may require decontamination. In addition to the deliberate use of these weapons, collateral damage, natural disasters, and industrial emissions may require decontamination. Contamination forces units into protective equipment that degrades performance of individual and collective tasks. Decontamination restores combat power and reduces casualties that may result from exposure, thus allowing commanders to sustain combat operations. [3]

Against the background of the increasing number of terrorist attacks, effective NBC defence is of principal importance for the armed forces as well as for civil defence and disaster management units either. Chemical, biological, radiological, and nuclear decontamination is the elimination of undesirable hazardous CBRN materials from humans, vehicles, weaponry, equipment, terrain, e.t.c. Decontamination reduces the dose that soldiers may receive from polluted surfaces, clears chemical, biological, radiological, and/or nuclear contamination away, and reduces the disposal costs associated with the components or the materials. [4]

Prompt and effective decontamination of persons, tanks and other vehicles, air- and watercrafts, personal weapons, clothing and equipment as well as sensitive materials ensure the ability of the concerned troops to survive.

Kärcher² develops and produces market-leading products for the most varying needs in the area of NBC defence and delivers them to its customers all over the world.

The DECOCONTAIN 3000 GDS was designed and constructed for the application of revolutionary non-aqueous decontamination agents such as GDS 2000 and forms the technical basis for the quick set-up of an on-site decontamination station. [5]

² Alfred Kärcher GmbH & Co. is one of the largest manufacturers of cleaning equipment

GENERAL PRINCIPLES OF DECONTAMINATION

CBRN contamination is a hazard to the life and health of personnel. Contamination places constraint on the use of equipment and areas affected, compels personnel to take NBC defence measures and may thus considerably impede or prevent mission accomplishment by units. Active decontamination operations reduce hazard levels by removing or neutralising liquid or solid contamination. It is carried out when CBRN contamination, which cannot be avoided, will adversely affect the unit's operational capabilities. [6] However, CBRN contamination can have an adverse effect on certain materials (i.e. composites) and can cause significant functional damage to surfaces of optical and sensor equipment.

Working or combating in Individual Protective Equipment (IPE) will degrade troops' performance, increase fatigue and possibly lower force cohesion and morale. Moreover, it reduces the overall speed, cohesion and freedom of movement of forces in the local area because of contaminated areas and assets. It also restricts the local use of ground and operational assets. If decontamination has become necessary, it needs to be undertaken as quickly as other operational priorities allow it. [7]

Decontamination is valuable in terms of manpower, time, space, and materials. These resources are also required to fight the battle, so commanders must apply them wisely and sparingly. The wisest way to conserve these resources and still sustain combat power is by following these four principles:

- speed,
- need,
- limit and
- priority.

Decontaminate as soon as possible (SPEED):

This is the most important principle out of the four. Commanders must consider this principle before considering any other. Speed is essential when the unit is contaminated. Contamination on personnel not in mission oriented protective posture (MOPP) gear poses an immediate hazard and can be lethal within minutes after contamination. Combat power drops as soon as personnel put on MOPP Gear. As soon as contamination is removed, commander can reduce MOPP level and restore combat power.

Decontaminate only what is necessary (NEED):

If commander expect to survive and win on the contaminated battlefield, he mustn't waste precious resources decontaminating everything. Commander must consider mission, time, extent of contamination, MOPP status, and decon assets available and decontaminate only what is mission essential to conserve resources and help sustain combat power.

Decontaminate as far forward as possible (LIMIT):

Commander must organise the decontamination as close to the site of contamination as possible to limit the spread of contamination. It is prohibited to move contaminated equipment, personnel, or remains away from the operational area, if it is possible to bring decon assets, organic or supporting units, forward safely. This will keep the equipment on location, speed up decontamination, and limit the spread of contamination. Limiting the number of personnel and amount of equipment in the area helps to prevent the spread of contamination. Commander makes every effort to confine NBC contamination to as small an area as possible. This also reduces the amount of decon required. Units moving from a contaminated area into a clean area should decontaminate at or near the edge of contamination. The unit marks all contaminated areas and reports their location to other

friendly units to keep them from entering the contaminated area unknowingly. Contaminated materiel presents additional problems for limiting the spread of contamination. If the situation permits, materiel can be left and allowed to weather. If the equipment is mission essential, it must be decontaminated on the spot or brought back to the rear and decontaminated. If the situation permits, decontaminate as far forward as possible. If this is not possible, then materiel may have to be transported to the rear for decontamination. If contaminated materiel must be moved:

- Use as few transport vehicles as possible.
- Use one route, especially around congested areas.
- Monitor the route periodically for contamination.
- Cover the materiel to keep confined.
- Warn personnel downwind if a vapour hazard is present.
- Monitor and decontaminate transport vehicles before transporting noncontaminated materiel.
- Ensure that transport crew wears appropriate MOPP Gear.

Decontaminate by priority (PRIORITY):

The commander must decontaminate the most important items first and the least important items last. Naturally, as human lives are the most important, decontamination of persons has the key priority. Then unit commanders decide which vehicles and equipment are most important to the mission. Battalion and brigade commanders decide which elements to pull "off line" to decon or whether to decon during the reconstitution process. Division and corps commanders must set priorities and concentrate decon assets. [8]

THE DECOCONTAIN 3000 GDS DECONTAMINATION SYSTEM

The DECOCONTAIN 3000 GDS is used for the simultaneous decontamination of vehicles, persons, equipment and road sections, and stands out due to its compact design and immediate readiness for operation. It forms the mobile material basis for the establishment of a complete decontamination site. The integrated 3000 litre stainless-steel tank enables the transport or storage of drinking water.



1. figure. The Kärcher DECOCONTAIN 3000 GDS decontamination system
(source: authors)

Development

The Kärcher DECOCONTAIN 3000 GDS decontamination system was designed for deployment at battalion level or higher and forms the technical basis for the fast establishment of a decontamination site. The DECOCONTAIN 3000 GDS is a new-generation compact, high-performance system mounted in a standard six metre ISO container. The DECOCONTAIN 3000 is designed to manage all essential decon activities simultaneously following NBC contamination: vehicle, personnel, clothing and equipment.

Description

“The DECOCONTAIN 3000 GDS is comprised of various modules:

- Independent diesel-powered MPS 3200;
- Pre-treatment module (HD-4000);
- Main-treatment module (AMGDS-2000);
- Post-treatment module (HDS-12/14 ST Eco);
- Shower module (HWM-35C).

The procedure used is dependent on the type of decontamination. Radiological decon uses a hot-foam procedure, while disinfection uses various biocidal solutions. CW-agent decon uses the GDS 2000. Personnel decon is conducted using a two-step, pulsating shower procedure in special decontamination site. Clothing and equipment decon is accomplished by using hot steam inside a collapsible tent. In addition, terrain is treated with an aqueous decontaminant solution. The system is equipped with a 57 kW high-performance generator and an insulated heatable water tank which allows the DECOCONTAIN 3000 GDS to operate independently for long periods.” [9]

Regarding the DECOCONTAIN 3000 GDS Containerised Full Decontamination System handbook the operational capabilities are the followings:

- Personnel decontamination: up to 120 persons/h.
- Road decontamination: 600 meters/h.
- Vehicle decontamination: 6 to 8 tanks, or 12 to 16 average size vehicles/h.
- Clothing decontamination: 20 to 30 sets/h.



2. figure. Vehicle decontamination with GDS 2000 solution
(source: authors)

GDS 2000 solution against chemical live agents

“In consideration of the huge increase in environmental awareness, Kärcher has developed a new non-aqueous decontamination agent (GDS 2000; NATO Supply No. 6850-12-366-1321) against chemical warfare agents which has important advantages compared to the known decontamination agents with regard to storage, handling, efficiency, application and corrosiveness as well as a considerably improved ecological behaviour. It is produced industrially and is available for application. It meets the requirements of water pollution class 1 (low hazard level to waters) and is biologically degradable. For example, the complete detoxification of a combat tank requires only 12 to 24 litres of GDS 2000. The high decontamination efficiency of GDS 2000 against all relevant chemical warfare agents (including chemical warfare agents containing thickeners) has been proven in many laboratory and field tests carried out by WISABC-SchutzBw and other independent test institutes. Industrially manufactured, ready-to-use non-aqueous decon agent, which works universally against all known chemical warfare agents and warfare agents containing a thickener.

Complete C (chemical) decontamination requires only approximately 0.1 – 0.2 l/m². BTR-80 and other armoured vehicles can be totally decontaminated in 5 – 10 minutes, using only 10 – 20 litres of GDS 2000. GDS 2000 may be stored for more than 10 years, if kept in its original packaging, unopened and under the given storage conditions. GDS 2000 can be applied by means of appropriate devices at temperatures ranging from -30 °C up to +49 °C”.
[10]

Generally one of the limiting factors of the decontamination is the availability of water. The actual amount of water required varies by the vehicle and its contamination level. The use of new decontamination solution facilitates to develop a water resupply plan for thorough decontamination operations.

DECONTAMINATION TECHNOLOGY AND PROCEDURES WITH DECOCONTAIN 3000 GDS

Decontamination of Vehicles

Decontamination of materials means radioactive decontamination, disinfection or detoxification of tanks, wheeled vehicles, artillery systems, engineering equipment, aircrafts, helicopters, etc. Pre-treatment, main treatment and post-treatment are carried out simultaneously using special electrically-driven decontamination modules.

First of all the contaminated unit performs predecontamination actions, to include segregating vehicles by checking for contamination.

1. The vehicle crews, except for the drivers, dismount. As the crews dismount, they remove all contaminated equipment, including sensitive items (i.e. electro-optical), from the top and sides of the vehicles. Once the crews have exited the vehicle, they will not re-enter. This prevents contamination from being spread into the vehicle interior.
2. Using the pioneer tools from the contaminated vehicles, the crew removes all heavy mud and debris. They concentrate on the undercarriage, which would be the most likely place for contamination to collect and the hardest place to decontaminate. Once the crew is finished with the pioneer tools, they are placed back on the vehicle. The initial removal of the mud and debris makes it more likely that the decontamination wash will remove any remaining contaminants.

3. Seat covers (when applicable), canvas items, camouflage netting, wooden rails, and any other material that can absorb liquid contamination are removed. These items create a potential transfer hazard and are not easy to decontaminate.
4. Equipment and supplies that are exposed after removal of coverings should be checked for contamination. If the items that can be removed are uncontaminated, they should be moved via a clean route to the postdecontamination area. Contaminated equipment and supplies will be decontaminated or disposed of properly. [11]

Pre-treatment:

During pre-treatment, coarse dirt with its CBRN contaminants is removed from tanks, vehicles, etc. by applying cold water under high-pressure (approx. 60 bar) using the HD 4000 decon module with two high-pressure spray lances.

Main treatment:

The main treatment depends on the type of CBRN contamination:

Chemical (C) decontamination: Detoxification using the highly effective GDS 2000 detoxification solution (AMGDS 2000 decon module).

Biological (B) decontamination: Disinfection is using the effective BDS 2000 disinfectant system (HDS 12/14-4 ST decon module).

Radiological/nuclear (RN) decontamination: Radioactive decontamination is using the highly efficient RDS 2000 hot foam (HDS 12/14-4 ST decon module).

Post-treatment:

During post-treatment, the decontamination residues are removed from the decontaminated surface using hot water under high-pressure (approx. 80 °C and 60 bar) or hot steam (approx. 140 °C) which is applied via one or two high-pressure spray lances.



3. figure. Vehicle decontamination with hot and high-pressure water
(source: authors)

Decontamination of Persons

Decontamination of persons means removal of contaminants from the skin to avoid any damage to health.

In the standard model, thorough decontamination of persons is carried out by means of a shower system integrated into the container side walls through which persons can pass. This

system includes an inflatable tent for undressing and a second tent for re-dressing. The persons to be decontaminated enter the shower section via the entrance stairs, thereby activating the first showers via an IR sensor. These showers automatically spray water enriched with a special decontamination agent. Subsequently and after a certain time interval, further showers delivering clear water for rinsing are activated. The decontaminated persons leave the shower section via the exit stairs. A tunnel installed between the tents and the shower section protects the persons from being seen and from the effects of the weather. The shower water is supplied via the hot water module integrated into the container. The waste water can be pumped off, collected and, for example, be used for material decontamination pre-treatment. Further shower types integrated in different shower tents are available on request.

Decontamination of road sections

NBC decontamination of road sections, take-off and landing runways is carried out using decontamination solutions. These decontamination solutions are applied by means of two AMGDS 2000 decontamination modules in a sufficient quantity directly during the decontamination process via four special spray nozzles. The DECOCONTAIN 3000 GDS covers a spray width of more than 2.60 m.

Decontamination of Personal Equipment

This means NBC decontamination of clothing, personal CBRN protection equipment and personal combat equipment. Decontamination is carried out using hot gas/hot steam in a specially designed hot gas/hot steam chamber. Thermal BC decontamination depends on temperature and time. Optimal decontamination temperatures vary between 130°C and 170°C. The necessary decontamination conditions inside the chamber are ensured by the decontamination module particularly suitable for this decontamination method.

Decontamination of the interior

Rooms are preferably decontaminated by means of aerosols. B decontamination of the interiors of shelters, vehicle cabins, aeroplanes, etc. is carried out by means of a highly efficient aerosol technology using a special thermal aerosol generator.

For thorough interior decontamination, the optionally available SN 50 Decon hot fogger is used. This thermal aerosol generator atomises the active agent of the thermally stable peroxyaceticacid (Wofasteril SC 250) in an effective droplet size.

EXAMINATION AND TEST OF DECOCONTAIN 3000 GDS SYSTEM

The examination and technical test of DECOCONTAIN 3000 GDS system were carried out by CBRN decontamination company. The examination procedures were executed at the base of CBRN decontamination coy and the testing period was 10 months. The testing of DECOCONTAIN 3000 GDS system was divided into two separate phases during the examination.

The following functions of the decon system were tested during the first phase:

Design and loading:

- The completeness of DECOCONTAIN 3000 GDS equipment.

- The mechanical equipment management and control units of marker signs, presence of signs, their placement.
- Protection of metal surfaces, the paint design and quality.
- The loading of built-in units and their placement, ensuring their accessibility.
- Immobility of loaded units and equipment inside the container.

Operation and handling:

- The testing of functional operation of the equipment.
- The operation of decontamination container, its handling and operational safety.
- The operation of safety systems.
- The assuredness of continuous operation.
- The applicability of decontamination containers during night and in low visibility conditions.
- The assuredness of water supply.

Several kind of predefined tasks were performed at the first phase. One of the most important was the container loading examination during railway transportation. The establishment was that the normal ISO standard container is suitable for railway transportation, but the loading procedure needs skilful operators. The other part of the examination focused to the handling of built-in modules and portable decontamination equipments and installations. The result of this part of the examination showed that devices and instruments are well designed, trustable and the ergonomic features are really outstanding. The training of the members of CBRN decon coy was the vital part for carrying out this really difficult examination and that is why every key members of the test had received special preparation from the decontamination procedures. The "Dragon Fire 2011" cooperative infantry exercise was one the best opportunity to test the decontamination containers with operators from the CBRN decon coy, where thorough decontamination of an infantry company was carried out at the simulated combat enviroment.



4. figure. The examination and technical test of DECOCONTAIN 3000 GDS system (source: authors)

The following functions of the decon system were tested during the second phase:

Installation and deployment:

- The conceptual scheme of CBRN decontamination station (tools installation, water supply, and contaminated liquids collection of environmentally friendly design options).
- The deployment time and standards.
- The determination of equipment capacity and capability.

Operation and handling:

- The operation and storage of DECOCONTAIN 3000 GDS system at winter weather conditions.
- Theoretical feasibility of CBRN decontamination patterns.
- The determination of time requirements for different CBRN decontamination methods.
- 7 and 23 days of reckoning for the application of CBRN decontamination data base definition.

Performed tasks during the second phase:

- Application and impact assessment of CBRN decontamination solution.
- Determination of time requirement at the CBRN decon station.
- Definition of commander's and operators' tasks at the CBRN decontamination station.
- The requisition of DECOCONTAIN 3000 GDS system at winter weather conditions.
- The examination of camouflage possibilities for CBRN decon sites.
- The examination of CIS possibilities for CBRN decon unit.
- CBRN decontamination station deployment at the training field of MH BHK Csörlőháza.
- Determination of technical and logistic service system of DECOCONTAIN 3000 GDS equipments.

Positive experiences:

- *Application security:* Due to the strict separation between the “clean” and “unclean” areas, and taking other general decontamination principles into consideration, a sluice-gate function is generated, which reliably avoids the spread of contamination.
- *Variability:* The commander can choose one of three shower variants for the decontamination of persons.
- *Multifunctionality:* The compact decon system is equipped with all necessary components for the establishment of a full decontamination site. Simultaneous, highly effective operation for CBRN decontamination of persons, material and equipment.
- *Operational safety:* Due to the integrated 3000 l water tank, the DECOCONTAIN 3000 GDS can also be used for independent decontamination tasks. It can be transported by rail, vehicle, ship, and air.
- *Central energy supply:* All electrical consumers are supplied with energy via a central electrical power generator.
- *Efficiency:* All stations of the decontamination site for vehicles can be run simultaneously and in parallel to the decontamination of persons without any

capacity restrictions. Also very suitable for use in military or special civil defence facilities.

Negative experiences:

- *Ineffective decontamination kit of road sections:* Road decontamination system is not fixable to the front of Hungarian RÁBA H-25 trucks. Suggestion: Road decontamination system is recommended to redraft to plan for using of Hungarian RÁBA H-25 trucks.
- There is not any C decontamination solution for SN 50 Decon hot fogger at the present time, only B decontamination solution is available. Suggestion: C decontamination solution is under the testing phase at Kärcher laboratory. After this testing period the C decontamination solution is needed to provide for CBRN decon units.
- The chassis washing system is not able to control the amount of liquid and the consuming of water is strongly wasteful. Suggestion: The chassis washing system is useless without a control device. This chassis washing system is replaceable with high pressure decon spears.
- Hoses of AMGDS module are too short (15 meters) and they are not suitable for carrying out the vehicle decontamination. Suggestion: Hoses of AMGDS module are needed to extend for more than 15 meters (all together 30 meters) hoses.
- In absence of stepladder the opening-closing procedures of container side-doors are not secure. Suggestion: The DECOCONTAIN 3000 GDS container is placed and used at the platform of a Hungarian RÁBA H-25 truck, the lock of container side-doors is relatively high and that is why the stepladders are necessary.

These born suggestions have already been approved by dealer firm and they are going be solved within a couple of months.

CONCLUSIONS

For deployed forces, and those operating in a potential or actual CBRN threat area, all active defence functions must be operable in CBRN environment without prejudicing operational tempo and combat effectiveness. [12]

At all levels, decontamination capability should be reserved, in order to carry out decontamination of attacked sub-units or those unable to bypass contaminated areas at the earliest possible moment to maintain combat effectiveness. Therefore each combat means should accompanied by an appropriate decontamination equipment in order to accomplish crew level immediate decontamination without waiting on superior's support.

Decontamination process has to be well integrated into coherent operational and tactical concepts in order to ensure the continuity of the operation.

Generally speaking, while the fighting unit is under decontamination it is especially vulnerable to enemy fires. The decontamination station has to be deployed over the range of enemy indirect fire. In this case the time is essential, and also specialist CBRN subunits can only conduct independent decontamination operations for short periods.

With the increase in the intensity of threats perception and possibility of mass casualties in case of a chemical, biological, radiological, and nuclear emergency, there is a need to develop novel and effective systems for decontamination. [13]

The decontamination ensures preserve the forces so the commander can apply maximum combat power. Preserving the force includes protecting personnel, may provides the success of the operation.

The participant units of military operations can keep their survivability through to employ CBRN defence rules, inter alia contamination avoidance, CBRN protection, and CBRN decontamination. All units have to be trained to operate in a CBRN environment to survive and accomplish their missions, and after training and many exercises have to be able to accomplish the decontamination in order to increase their fighting capacity through reducing their MOPP level. Decontamination assets within these units are limited, and these circumstances determine their capability, so the fastest and most effective decontamination only CBRN decontamination subunits can provide. The time plays key role during operations, therefore supplying the decontamination platoon with sophisticated items - which allows enhancement in the CBRN decon platoon's performance – is very important.

The DECOCONTAIN 3000 GDS represents the state of the art in its performance class. Due to its modular construction, this decontamination system can be set up readily and flexibly and is adaptable to the operational situation. In addition, the decontamination agents foreseen for the DECOCONTAIN 3000 GDS fulfil the strict regulations of reliable environmental protection. The Hungarian Defence Forces have a new operational capability which can be used in a wide spectra of military operations or disaster relief tasks without limited deployment capabilities.

Following a confirmed CBRN incident NATO military forces must be fully prepared to respond to and recover from the consequences of a CBRN incident against their own forces, infrastructure and assist to their partners, if necessary. In addition due to the likelihood that major civil emergencies can pose a threat to security and stability and because CBRN consequence management is challenging and could be a massive, costly and protracted effort, NATO should be prepared to support national authorities, if requested. This includes eliminating contamination to required levels of cleanliness, restoring operational capabilities, re-establishing conditions which are as close to the “status-ante” as possible, providing support to civilian lead consequence management operations and conducting CBRN forensic investigations. [14]

The decontamination platoon is required to meet the above challenges that include carrying out decontamination of civilian population and material assets. In this case the decon sub-unit have to look after the force protection only.

Technology changes continues to be a key driver of developing the performance of the decon platoon that will pose both new problems and new opportunities. As access to current and emerging technology becomes more widespread, there will be greater opportunities for the CBRN units to develop effectively their means for assembly their enhanced decontamination process.

References³

- [1] Field Manual No. 3-90: Tactics, Headquarters Department of the Army Washington, DC, 4 July 2001.
- [2] Field Manual 3-11-4: Multiservice tactics, techniques, and procedures for nuclear, biological, and chemical (NBC) protection, June 2003.
- [3] Field Manual 7-20: The infantry battalion, Headquarters Department of the Army Washington, December 2006.

³ The last download date of the internet references was: April 20, 2012

- [4] Vinod Kumar, Rajeev Goel, Raman Chawla, M Silambarasan, Rakesh Kumar Sharma: Chemical, biological, radiological, and nuclear decontamination: Recent trends and future perspectives, <http://www.jpbonline.org/article.asp?issn=09757406;year=2010;volume=2;issue=3;page=220;epage=238;aulast=Kumar>
- [5] Futuretech Kärcher: The Swedish Army Orders Four Additional Containerised DECOCONTAIN Full-Decontamination Systems, http://www.karcherfuturetech.com/futuretechfr_en/news/2007/the_swedish_army_orders.htm
- [6] STANAG 2426 NBC (edition 2) - Nuclear, biological and chemical (NBC) hazard management policy for NATO forces.
- [7] AJP-3.8 Allied joint doctrine for NBC, July 2003.
- [8] Field Manual 3-5, Headquarters, Department of the Army: NBC Decontamination.
- [9] Futuretech Kärcher: DECOCONTAIN 3000 GDS Containerised Full Decontamination System- Handbook.
- [10] Product Details: GDS 2000 Decontamination Solution, https://www.rkb.us/contentdetail.cfm?content_id=177883
- [11] Field Manual 3-11-5: Multiservice tactics, techniques, and procedures for nuclear, biological, and chemical (NBC) decontamination, April 2006.
- [12] Guidelines for operational planning (GOP) final revision 1, June 2005.
- [13] Abdul Wadood Khan, Sabna Kotta, Shahid Hussain Ansari, Rakesh Kumar Sharma, Vinod Kumar, Sudha Rana, and Javed Ali: Chemical, biological, radiological, and nuclear threats-Decontamination technologies and recent patents, http://jrse.aip.org/resource/1/jrsebh/v4/i1/p012704_s1?isAuthorized=no
- [14] Comprehensive NATO Chemical, Biological, Radiological, Nuclear (CBRN) Defence Concept, Headquarters, Supreme Allied Commander Transformation, Norfolk, Virginia, December 2010.

VII. Évfolyam 4. szám - 2012. december

Derzsényi Attila

attila.derzsényi@hm.gov.hu

AZ ÉLELMISZER ELLÁTÁS HATÉKONYSÁGÁNAK ELEMZÉSE

Absztrakt

A rendszerváltozás óta tartó politikai, gazdasági szféra, valamint az ezzel összefüggő hazai és nemzetközi jogszabályi környezet folyamatos változásai jelentős hatást gyakoroltak és gyakorolnak a közigazgatás – ezen belül a honvédelmi tárca - logisztikai rendszerére. A cikk a honvédelmi szervezetek élelmiszer ellátásának – kiemelten a beszerzésre vonatkozó - hatékonyságát vizsgálja, továbbá hazai és nemzetközi tapasztalatok alapján újszerű megoldási javaslatot, korszerű ellátási rendszert fogalmaz meg.

The continuous changes of the political, economical spheres established after the system change and the domestic and international legal environment had and still has a significant effect on the logistic system of the administration, including the Ministry of Defence. The article examines the effectiveness - particularly in procurement approach - of the food supply of the defence bodies, and based on the domestic and international experiences it draws up an innovative solution proposal, a modern supply system.

Kulcsszavak: *logisztikai ellátás, beszerzés, élelmiszer beszerzés ~ logistic supply, procurement, food purchase*

BEVEZETŐ

A Magyar Honvédség csapatai tevékenységének logisztikai támogatása a haza védelme, a szövetségben vállalt kötelezettségek teljesítése és a békeműveletek sikere érdekében sokrétű feladatellátást igényel. A honvédelmi tárca feladata, struktúrája, eszköz és szolgáltatás igénye, az igények keletkezése illetve a feladatorientált tervezése nagymértékben eltér a közigazgatás más szervezeteitől.

A honvédelmi tárca évről évre jelentős költségvetési forrásokat használ fel a haderőfejlesztése és a szövetségi kötelezettségek teljesítéséhez szükséges katonai képességek megteremtése céljából, amelyeknek megvalósításának egyik legfontosabb eszköze a (köz)beszerzés. A beszerzés feladatkörébe nemcsak a fejlesztések, a képesség megteremtéséhez szükséges eszközök és szolgáltatások megszerzése, hanem a napi élet biztosítása is beletartozik. Ennek hatására a beszerzési feladatok végrehajtása rendkívül összetett feladattá vált, és a közvélemény különösen érzékenyen reagál az egyes fontosabb eseményekre. A honvédelmi tárca vezetésének legfontosabb törekvése mindig is az volt, hogy a tárca hatáskörébe tartozó beszerzések átláthatók, ellenőrizhetők legyenek, a lebonyolítás a jogszabályi keretek között valósuljon meg, és a közpénzek felhasználásával, a köztulajdon használatának nyilvánosságával, átláthatóbbá tételével és ellenőrzésének bővítésével, figyelembevételével biztosított legyen a (köz)beszerzések nyilvánossága.

Megállapítható, hogy az egyes áru, illetve szolgáltatás csoportokban a legnagyobb megtakarítás a "nagymegrendelői" pozícióból érhető el, ehhez célszerű az egyes költségvetési szervezetek beszerzéseinek összevonása, együttes versenyeztetése. Ennek alapján a kisebb méretű szervezetek részére is biztosítható jelentős árkedvezmény. A központosítás egyben javítja az ellátás biztonságát, lehetővé teszi professzionális beszerző személyzet, szervezet kialakulását. A közbeszerzési törvény az ilyen típusú beszerzésekre lehetővé tette a központosított közbeszerzések rendszerének kialakítását.

A Honvédelmi Minisztérium illetve a Magyar Honvédségen belül értékhatártól, illetve jogosultságoktól függően többszintű ellátási, beszerzési logisztikai rendszer működik. A feladat ellátásához, illetve a fenntartáshoz szükséges anyagok, eszközök, szolgáltatások egész körére kiterjedően (haditechnikai eszközök, hadianyagok és egyéb hadfelszerelési cikkek) beszerzést a HM, ill. a megfelelő háttérintézmények végzik a Magyar Honvédség szükségleteinek megfelelően.

A haderő alaprendeltetéséből, feladatának sajátos jellegéből adódóan béke, veszélyhelyzet elhárítása, háborús időszak, illetve nemzetközi katonai szerepvállalás időszakában eltérő igények keletkeznek. A védelmi igények elsőbbséget kell, hogy élvezzenek minden más igényvel szemben.

A katonai szükségleteknek egy körére viszonylag könnyen alkalmazhatóak a polgári logisztika módszerei, mert ezeknél az anyagféléseknél a felhasználás jellege, mennyiségi és minőségi mutatói összehasonlíthatók a civil szféra anyag-felhasználási folyamataival.

A szükségletek beszerzése azonban ekkor is csak törvényeken alapuló eljárásrendnek megfelelően, a közbeszerzési alapelvekkel összhangban történhet.

A katonai szükségletek beszerzése mind béke, mind háborús időszakban feltételezi a katonai igények, eszközök, logisztikai rendszer működésének ismeretét. A honvédelmi tárca számára kötelezően alkalmazandó, (köz)beszerzésre vonatkozó jogszabályok alkalmazása során a beszerző szervezetnek biztosítani kell egyrészt a törvényességet, másrészt a katonai igényeknek megfelelő termékek, szolgáltatások beszerzését is. Ennek biztosítása érdekében a hazai és nemzetközi katonai logisztikai rendszer működését, valamint a katonai eszközöket ismerő, közbeszerzési gyakorlattal rendelkező szakemberekre van szükség.

A honvédelmi szervezetek élelmiszerrel történő ellátása elsősorban létszámfüggő. Az ellátási tevékenység jellegét és folyamatát, egyszerűbben megfogalmazva a katonák etetését

úgy kell kialakítani, hogy minden körülmények között (béke, missziós, válsághelyzet, háborús), ugyanazon színvonalat biztosítson.

- Figyelembe véve a mindenkori katonai létszámot, az élelmiszer alapanyagok a termelőtől (kis- nagykereskedőtől) a raktárig, a készétel a konyhából az az asztalra történő eljuttatásának logisztikai folyamata nagyfokú szervezést igényel. Ebbe a folyamatba az ételek minősége kiemelt figyelmet érdemel, hiszen rossz, fertőzött alapanyagok, rosszul tárolt ételek fogyasztása a honvédség alaprendeltetési feladatának biztosítását veszélyezteti. Napjaink nemzetközi biztonsági környezetében az élelmiszerellátási láncban is fel kell készülni a terrortámadások elleni védelemre, amely a katasztrófák, a gondatlanságból, vagy szándékosan elkövetett ételmérgezések állat- és közegészségügyi, társadalmi, politikai és egyéb következményei felszámolásában nyújt segítséget. Az élelmiszer ellátás sérülékenysége miatt. Dr. Horváth Attila: „Az élelmiszerellátási lánc kritikus infrastrukturális, terrorfenyegetettségének jellemzői” című tanulmányában kiemeli: *„A terrorcsoportok szemszögéből nézve az élelmiszerlánc elemeit könnyű pusztítani. Az ún. modernkori terrorizmus története szerencsére nem bővelkedik ilyen célpont elleni terrortámadásokkal. Az élelmiszer és vízellátás sérülékenysége miatt azonban ennek kockázatát komolyan kell venni.”*
- A honvédségen belül az ételmezési ellátás egyrészt jelenti az élelmiszer megfelelő helyen, időben, mennyiségben történő biztosítását, másrészt a minőségi követelmények elő- köztes és utólagos ellenőrzését is. A megfelelő szállító kiválasztásának, a szerződéses feltételek kialakításának, valamint a minőségbiztosítási követelmények kialakításának nem csapat, hanem magasabb, központi szinten kell megtörténnie.

A honvédségi szervezeteknél eltöltött évtizedes logisztikai tapasztalatom alapján olyan alternatív (élelmiszer) ellátási módszert kívánok bemutatni, amely a fent felsorolt jogszabályi, felsővezetői, illetve csapatigényeknek megfelelően alkalmazható.

TÖBBSZINTŰ LOGISZTIKAI RENDSZER

A honvédelmi szervezetek csapat hatáskörű ellátásának egyik legfontosabb kérdésköre az állomány élelmiszerekkel történő ellátása. A korábbi időszak beszerzési gyakorlata és előírásai alapján az élelmiszerek beszerzését a HM tárca központi beszerző szervezetei (HM Beszerzési és Biztonsági Beruházási Hivatal, HM Fejlesztési és Logisztikai Ügynökség, HM Fegyverzeti és Hadbiztosági Hivatal) hajtották végre az eljárást kezdeményező honvédelmi szervezetek megbízásai alapján. Szakmai pályafutásom alatt a korábban említett szervezeteknél eltöltött vezetői beosztásokban szerzett tapasztalatok alapján a honvédelmi tárca központi beszerző szervezeteinek kialakulását és tevékenységi körét a „Honvédség centralizált beszerzésének története” című korábbi cikkemben kifejtettem.

Az egyes élelmiszer típusok külön-külön (pld: hús, húskészítmény; tej; kenyér-pékáru, ásványvíz-üdítő, stb) kerültek meghirdetésre közösségi közbeszerzési eljárásban. Tekintettel arra, hogy MH szinten az egyes élelmiszer típusok összértéke önállóan is meghaladta a közösségi értékhatárt (kb. 54 Mft-ot), az egybeszámlítás nem volt vizsgálat tárgya.

Az éves költségvetési tervezés alapján az utóbbi években kizárólag tárgyévi – azaz költségvetési évre vonatkozó – élelmiszer beszerzésekre került sor. Ennek oka egyrészt a több évre vonatkozó költségvetési fedezet igazolásának hiányában, másrészt az egyes honvédelmi szervezetek igényeinek folyamatos változásaiban keresendő.

Az „Élelmiszer beszerzés aktuális kérdései” című tanulmányomban a központi beszerző szervezetekkel kapcsolatosan az alábbi megállapításokat tettem:

„A korábban említett központi beszerző szervezetek által lefolytatott eljárások előnyei:

- az MH egészére vonatkozó igény alapján figyelembe vehetőek voltak a gazdaságossági szempontok (nagyobb tételben kedvezőbb árajánlat várható)
- az MH egészére vonatkozóan egységesen kerültek szabályozásra a szerződéses feltételek, késedelmi, megghiúsulási kötbér, szállítási feltételek, stb.
- az MH egészére vonatkozóan adott élelmiszer termékcsoporthoz egy közbeszerzési eljárást kellett lefolytatni, ezáltal csökkentve az egyes szervezetek beszerzői-megbízói állomány leterheltségét;
- az élelmiszerbiztonsági, minőségi követelmények egységesen kerültek meghatározásra, továbbá ezek ellenőrzése a honvédelmi tárca egyedüli minőségbiztosítási szervezetének (amely a HM FLÜ, majd a HM FHH igazgatóságaként került átalakításra) feladatkörébe tartozik.

Hátrányai:

- az MH egészére vonatkozó szerződés megszüntetése, felbontása az összes szervezet részére kihatást jelent;
- az alakulati igények változásai alapján a szerződés módosítása hosszadalmas, időigényes;
- a helyi kistermelők az országosan kiírt közbeszerzési eljárásban a feltételeknek nem tudtak megfelelni.”

2011. év elején a honvédelmi szervezetek részéről felmerült igény alapján a „honvédelmi szervezetek beszerzéseinek eljárási rendjéről” szóló HM Utasítás 2011. július 30-ai módosítása alapján az élelmiszerek beszerzése csapathatáskörbe került.

A Magyar Honvédség katonai szervezeteinél rendkívül heterogén a beszerzésekkel kapcsolatos személyi és tárgyi feltételek biztosíthatósága. Kevés szervezetnél áll rendelkezésre beszerzési tapasztalattal rendelkező jogi végzettségű személy, több szervezetnél a beszerzési ügyek intézésére kijelölt munkatársak is, a beszerzés lebonyolításának sajátosságai miatt, állandó szakmai támogatásra szorulnak.

A csapathatáskörű élelmiszer beszerzésekre vonatkozó néhány általános következtetés levonható:

- csapatszinten minden esetben értelmezni és vizsgálni szükséges a közbeszerzési törvényben meghatározott egybeszámítás kérdéskörét;
- csapatszinten kell kialakítani és belső szabályozásban meghatározni az élelmiszerek minőségi követelményeit, valamint azok ellenőrzését;
- csapatszinten erősíteni kell a közbeszerzéssel foglalkozó szakállományt;
- HM tárca szinten ki kell alakítani az egységes nyilvántartást és jelentési rendszert az élelmiszerek beszerzéseire vonatkozóan.

KÖZPONTI BESZERZŐ SZERVEZET ELŐNYE

A Zrínyi Miklós Nemzetvédelmi Egyetem katonai logisztikai mesterképzési szakon írt szakdolgozatomban a rendszerváltás óta létrejövő hazai központi beszerző szervezetek kialakulásának folyamatát dolgoztam fel. Alapul véve a dolgozatomban részletesen kifejtett nemzetközi és hazai törvényi előírásokat és kormányzati törekvéseket, összehasonlítást végeztem a honvédelmi tárca és más kormányzati központi beszerző szervezetek céljait, működési feltételeit.

Az említett dolgozatomban tett megállapítások alapján álláspontom szerint a honvédelmi tárca beszerzési jogkörrel rendelkező központi beszerző szervezeténél és csapatszinten is biztosítani kell a honvédelmi tárca legfontosabb érdekeit:

- az államháztartás kiadásainak ésszerűsítését;
- az állami ráfordítások csökkentését;
- a költségvetési előirányzatok tervszerű felhasználását;
- általános használt, azonos használati célú, tipizálható termékek koncentrált beszerzését ("szabványosítás");
- a közpénzek felhasználása átláthatóságát;
- széles körű, nyilvános ellenőrizhetőségének megteremtését;
- a közbeszerzések során a verseny tisztaságának, az esélyegyenlőség; a nyilvánosság biztosítását;
- a belföldi áru előállítás; munkaerő-foglalkoztatás elősegítését.

A célok elérésével kapcsolatban kijelenthető, hogy ezen célok elsősorban központi beszerző szervezettel érhetők el.

A kormányzati szintű központi beszerző szervezet létrehozó jogszabály indoklásában a működtetésének további előnyeiként az alábbiakat fogalmazza meg:

- a kormányzati stratégia érvényesítésében segítséget jelent;
- a csapatok számára is elérhetők a központi szerződések;
- a beszerzés és az azzal kapcsolatos adminisztráció egyszerűbb, kevesebb humánerőforrást igényel;
- a rendelés és árképzés egységes, átlátható rendszerben kerül a csapatokhoz;
- az egységes műszaki követelményekkel, szerződési feltételekkel felépített keretszerződések biztosítják a csapatok flexibilis ellátásának lehetőségeit.

Álláspontom szerint a központi beszerzős szervezet által kötött keretszerződések azonban nem jelentenek végleges megoldást a csapatok eltérő igényeihez:

- csapatonként eltérő mennyiségű, eltérő minőségű termékekre lehet igény;
- évenként a csapatok igénye folyamatosan változik;
- azonnali, sürgős plusz igényre nem ad alternatív megoldást.

Napjainkban számos központosított közbeszerzési szervezet működik mind az Unióban, mind hazánkban közigazgatási és vállalati szinten is.

NATO Ellátó Ügynöksége (NspA), mint a NATO Támogató Szervezet központi beszerző szervezete, bármely nemzet részére folytat le beszerzési eljárást.

A GYEMSZI (Gyógyszerészeti és Egészségügyi Minőség- és Szervezetfejlesztési Intézet) a fekvőbeteg szakellátást nyújtó intézmények részére minden olyan egyéb, költséget jelentő fogyasztásra, melynél a centralizált közbeszerzésekkel megtakarítás érhető el (gáz, áram, mosoda stb.) központilag folytat le keretmegállapodásos eljárást, vagy köt keretszerződést.

A Kormány a 168/2004. (V.25) Korm. rendelet alapján újrászabályozta a központosított közbeszerzések rendszerét, valamint a központi beszerző szervezet feladat és hatáskörét. Ennek érdekében a kötelezett állami szervezetek részére a Közbeszerzési és Ellátási Főigazgatóság (KEF) folytat le közbeszerzési eljárásokat, ezen belül leggyakrabban keretmegállapodásos eljárás formájában.

A Kormány a közbeszerzések központosított eljárás keretében történő lefolytatását rendelheti el az általa irányított vagy felügyelt költségvetési szervek, alapított közalapítványok, valamint az állami tulajdonú gazdálkodó szervezetek vonatkozásában, meghatározva annak személyi és tárgyi hatályát, az ajánlatkérésre feljogosított szervezetet (központi beszerző szerv), valamint az eljáráshoz való csatlakozás lehetőségét.¹

A Rendőrség Beszerzési Szabályzata alapján a Központi Gazdasági Ellátó Igazgatóság (KGEI) folytat le közbeszerzéseket a rendőri szervek részére.

¹ Kbt. 25. § (1)

Az általa irányított szervezetek vonatkozásában a helyi önkormányzat jogosult a közbeszerzéseket összevontan, helyben központosítva lefolytatni. A közbeszerzés helyben központosításáról az önkormányzat rendeletet alkot. A helyben központosított közbeszerzési eljárásokra a Kbt. és az önkormányzati rendelet szabályait kell alkalmazni.²

Budapest Főváros Közgyűlése az önkormányzati ráfordítások csökkentése, a költségvetési előirányzatok tervszerű felhasználása, a központi beszerzési rendszerben rejlő előnyök közigazgatási célú hasznosítása érdekében helyi központi beszerző szervezetként a Budapesti Egészségközpont Zrt-t jelölte ki.

Általánosságban elmondható, hogy 2004/18/EC Európai Unió direktíva alapján szinte minden Unió tagállama rendelkezik központi beszerző szervezettel.(SKI- Dánia, HANSEL-Finnország, UGAP-Franciaország, CONSIP-Olaszország)

KERETMEGÁLLAPODÁS

A cikk megírásakor olyan témát kívántam feldolgozni, mellyel kapcsolatban tanulmány még nem készült. Az előkészítő tevékenységem során fontos szerepet kapott az információk, adatok összegyűjtése. Szakmai pályafutásom alatt a központosított közbeszerzési rendszer HM tárcánál történő bevezetésében folyamatosan részt vettem számtalan tárca szintű, illetve tanácsadóként a MeH KSZF központosított közbeszerzési eljárásában.

Az előző fejezetben említett hazai és nemzetközi központi beszerző szervezetek tevékenysége az évtizedek alatt folyamatos változáson ment keresztül, amelynek eredményeként jól működő rendszerek kerültek kialakításra. Ennek egyik változata az egyes – ellátási körbe tartozó – szervezetek részére biztosított keretmegállapodás kötése.

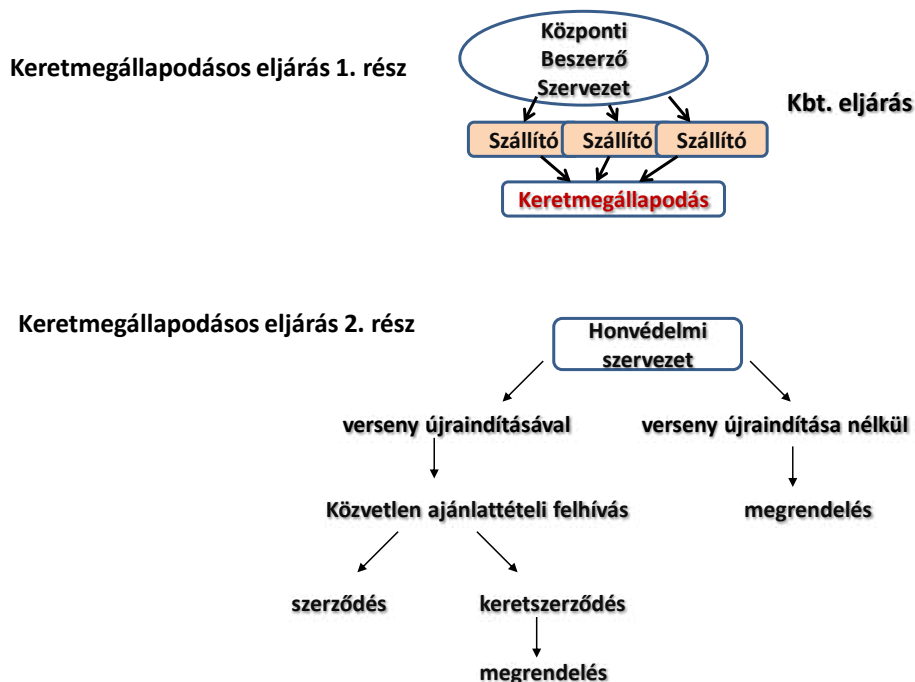
Tekintettel arra, hogy a honvédelmi tárcánál a keretmegállapodásos eljárás nem került bevezetésre, célszerű megvizsgálni annak alkalmazhatóságát. A továbbiakban – alapul véve a korábban említett szervezetek működési rendjét – a honvédelmi tárcánál történő bevezetésének, működtetésének feltételrendszereit mutatom be, kifejezetten a napjainkban előtérbe került élelmiszer ellátás példáján keresztül.

A keretmegállapodás az összesített csapat igények alapján a központi beszerző szervezet által lebonyolított keretmegállapodásos eljárás első szakaszának eredményeképpen jöhet létre. Keretmegállapodás legfeljebb négy évre köthető. A keretmegállapodásos eljárás második szakaszát keretszerződés vagy egyedi szerződés zárja le.

A keretmegállapodásos eljárás két egymástól jól elkülöníthető szakaszra osztható:

- a) Az első szakaszban a központi beszerző szervezet a csapatok irányából érkező, összesített igények alapján nyílt, meghívásos vagy tárgyalásos eljárást folytat le, és ennek eredményeképpen köti meg (akár több Szerződő féllel is) a keretmegállapodást. *Előnye*, hogy az első rész, sajátos jellegéből adódóan, hatékonyan tudja biztosítani a meghirdetéssel induló és nyilvánosság előtt zajló eljárásban a beszerzés átláthatóságát, amely a közérdek érvényesülésének alapvető letéteményese.
- b) Az eljárás második szakaszában vagy a központi beszerző szervezet, vagy pedig maga a csapat bonyolítja le a beszerzést, és ennek megfelelően keretszerződés vagy egyedi szerződés jön létre. Az eljárás második szakaszában tartandó konzultáció lehetővé teszi, hogy *a csapat érvényesíteni tudja speciális beszerzési igényeit és egyedi érdekeit.*

² Kbt. 25. § (5)



1. ábra. Keretmegállapodás folyamata
(Forrás: Saját készítésű ábra)

A rendszer szereplői különböző pozíciókban helyezkednek el. Az egyedi beszerzések megvalósítása során a honvédelmi szervezetek, mint megrendelők, a nyertes ajánlattevők, mint Szállítók, a központi beszerző szervezet pedig, mint a beszerzés kereteit, az ellátást biztosító szervezet jelennek meg.

A központi beszerző szervezet

Feladata a csapatok által megküldött igénybejelentések alapján megtervezni, előkészíteni és lefolytatni a keretmegállapodásos eljárásokat.

A csapatok megfelelő tájékoztatása érdekében:

- kezeli és frissíti a közbeszerzési adatbázist;
- működteti a beszerzési portált, ahol folyamatosan közzéteszi a keretmegállapodást érintő, az adatszolgáltatási és egyéb kötelezettségek teljesítéséhez szükséges adatokat, az adatszolgáltatás során alkalmazandó mintákat, a keretmegállapodások teljes szövegét, a szállítók nevét, a keretmegállapodásokból beszerezhető termékek és szolgáltatások listáját, árát;
- valamint megszervezi a szükséges oktatási feladatokat;
- figyelemmel kíséri a keretmegállapodások alapján feladott megrendelések teljesítését.

A honvédelmi szervezetek

A mindenkor hatályos „honvédelmi szervezetek beszerzéseinek eljárási rendjéről” szóló HM Utasítás hatálya alá tartozó szervezetek.

A Szállítók

A Szállítók a lefolytatott (köz)beszerzési eljárás eredményeként keretmegállapodást kötő ajánlattevők. A Szállítók feladata, hogy a honvédelmi szervezetek ellátását az egész ország területén biztosítsák. Ennek érdekében a Szállítók közvetlen kapcsolatot tartanak fenn a honvédelmi szervezetekkel és a folyamatos tájékoztatással, tanácsadással biztosítják a honvédelmi szervezetek beszerzéseinek gyors és rugalmas megvalósítását, az esetleges reklamációk kezelését.

A Szállító fogalma azt a gazdasági szereplőt jelenti, aki a keretmegállapodásos eljárás első részének nyertes ajánlattevője, illetve közös ajánlattevője, azaz keretmegállapodásos partnere a Központi Beszerző Szervezetnek. Egyéb szereplő nem minősül Szállítónak, így az alvállalkozó sem.

A keretmegállapodásos eljárás első részének célja:

- kiválasztásra kerüljenek azok az alkalmasnak ítélt ajánlattevők (illetve közös ajánlattevők), melyek önállóan is képesek a honvédelmi szervezetek országos ellátásának biztosítására;
- meghatározásra kerüljenek azok a speciális szerződéses feltételek, melyek a nagyszámú honvédelmi szervezeti kör nagyrészt egyedi igényeit hivatott kielégíteni;
- verseny révén kiválasztásra kerüljenek azok a szolgáltatás- és termékajánlatok, melyek költség-hatékony megoldást tudnak biztosítani a honvédelmi szervezetek tárgy szerinti termékcseré, termékbővítési és szolgáltatási igényeinek ellátására.

Az eljárás első részének indító felhívása, a nyílt eljárás ajánlati felhívása az Európai Unió Hivatalos Lapjában jelenik meg.

Az első rész egy egyszakaszos eljárás, mely az írásban benyújtott ajánlatok elbírálásán alapul.

A benyújtott ajánlatok ajánlati árának bontást követő módosítására elektronikus árlejtés során van lehetőség. („a közbeszerzési eljárásokban elektronikusan gyakorolható eljárási cselekmények szabályairól, valamint az elektronikus árlejtés alkalmazásáról” sz. 257/2007. (X.4.) Kormányrendelet alapján)

Az eljárás első részében ajánlatot benyújtó Ajánlattevőnek az ajánlat benyújtása előtt kell eldöntenie, hogy milyen „konstrukcióban” nyújtja be ajánlatát. Ennek során el kell döntenie, hogy önálló Ajánlattevő, közös Ajánlattevő illetve projektársaság formát választja.

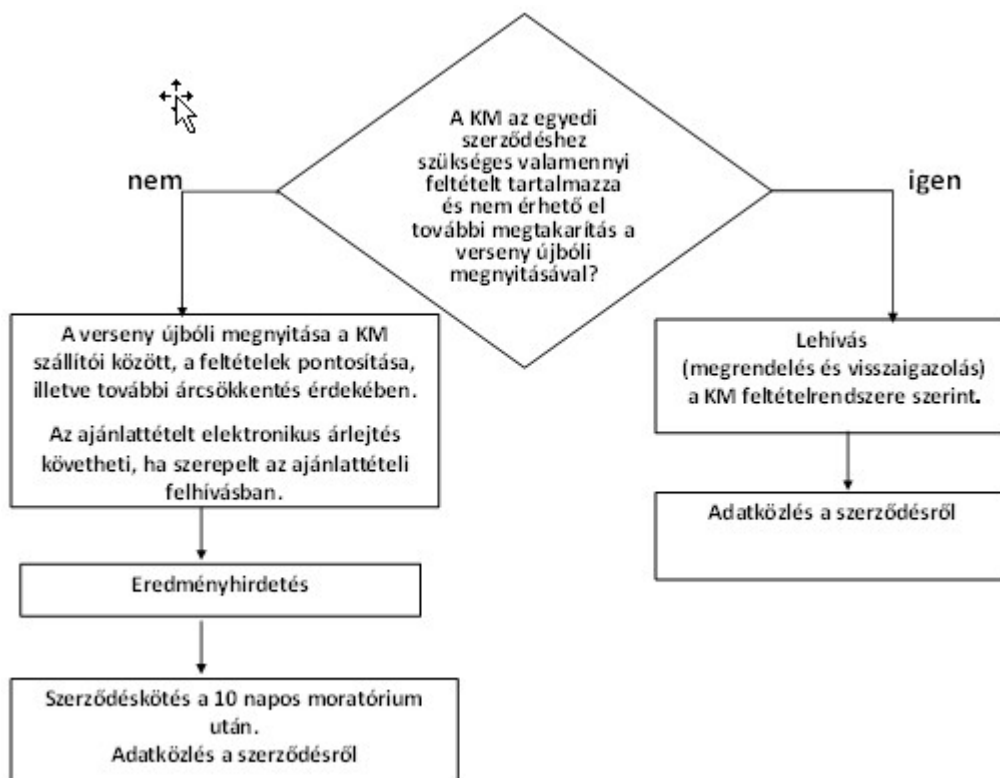
Központi beszerző szervezet az eljárás első részének eredményeképpen keretmegállapodásokat köt.

Tekintettel a speciális honvédségi ellátási körre lehetőség van régióként, járásonként; valamint terméktípusonként (hús, tej, kenyér, stb) is keretmegállapodásokat kötni.

A KERETMEGÁLLAPODÁSOS ELJÁRÁS MÁSODIK RÉSZÉ

A keretmegállapodásos eljárás második részében a honvédelmi szervezetek a beszerzési céljaiknak megfelelő módot választják (verseny újbóli megnyitásával történő, vagy újbóli megnyitása nélküli kiválasztás) a ténylegesen beszerezni kívánt termékekre és Szállító kiválasztására.

A verseny újbóli megnyitása nélküli mód csak akkor választható, ha a keretmegállapodás minden feltételt tartalmaz, valamint a verseny újbóli megnyitásával további megtakarítás a honvédelmi szervezet számára nem realizálható (a verseny újbóli megnyitása a gazdasági ésszerűséggel nem összeegyeztethető).



2. ábra. Folyamatábra a keretmegállapodásos eljárás második részéről (Forrás: Saját készítésű ábra)

A verseny újraindítása nélküli kiválasztás:

Amennyiben a keretmegállapodás minden feltételt tartalmaz, valamint a verseny újbóli megnyitásával további megtakarítás a honvédelmi szervezet számára nem realizálható (a verseny újbóli megnyitása gazdasági ésszerűséggel nem összeegyeztethető), az igény kielégítése megvalósítható a verseny újbóli megnyitása nélkül. Ez esetben, az eseti beszerzés vonatkozásában az első rész bírálati szempontja (a legalacsonyabb összegű ellenszolgáltatás javasolt) szerinti nyertes kiválasztásával, szükség esetén írásbeli konzultációt követően kerül sor a megrendelésre. („Sorba állítási módszer”: először azzal a gazdasági szereplővel kell felvenni a kapcsolatot, amely a legalacsonyabb ellenszolgáltatást tartalmazó ajánlattal felel meg az objektív beszerzési igénynek; amennyiben az első nem képes az adott áru, illetve szolgáltatás teljesítésére, úgy a másodikkal lehet felvenni a kapcsolatot.”)

Ezen a ponton már nincs lehetőség a műszaki és pénzügyi alkalmassági szempontok vizsgálatára, mint a keretmegállapodásos eljárás első részében.

A honvédelmi tárca hosszadalmas beszerzési eljárása miatt ebben a részben taglalt eljárás mód feltételekkel alkalmazható. A tárca döntési mechanizmusa (NFM engedélyeztetés) nem teszi lehetővé az aznapi kiválasztást követő még aznapi megrendelés megküldését. Mire a tárca beszerzési folyamatában sor kerül szerződéskötésre a Szállító legtöbb esetben már módosította termékeit, vagy az árakat.

Írásbeli konzultáció:

A honvédelmi tárca igénye alapján a keretmegállapodásos eljárásban kialakításra került a konzultáció lehetősége, amely biztosítja, hogy Ajánlatkérő rákérdezzen kötelezettségek nélkül Szállítóra, hogy pl. egy vagy két hónap múlva milyen termékeket, milyen áron tud szállítani)

A verseny újbóli megnyitása nélküli kiválasztás során amennyiben szükséges a honvédelmi szervezet konzultációra szóló felhívásban felhívhatja a beszerzendő termékek, illetve

szolgáltatások konkrét tárgya szerinti, a keretmegállapodásos eljárás első részében alkalmazott bírálati szempont és módszer alapján rangsorolt, legkedvezőbb ajánlattal rendelkező Szállítót a keretmegállapodás első részében tett ajánlata kiegészítésére.

A Szállító a központi beszerző szervezet által lebonyolított keretmegállapodásos eljárás első részének lezárásaként kötött keretmegállapodásban meghatározottakhoz képest, az ajánlat - az összességében legelőnyösebb ajánlat megítélésére szolgáló részszempontokkal összefüggő - tartalmi elemeire vonatkozóan, csak a keretmegállapodásban foglaltakkal azonos vagy a honvédelmi szervezet számára kedvezőbb ajánlatot tehet.

A konzultáció szabályozása azonban olyan mértékben korlátozásra került, hogy több Szállító esetében alkalmazhatatlan a honvédelmi tárca viszonylatában. Annak érdekében, hogy a beszerző ismerje minden – az adott terméket szállítani képes Szállító – nyilatkozatait, termékeit, árait egy meghatározott későbbi szerződéskötési időpontra vonatkozóan minden Szállítót meg kellene szólítani. A konzultáció egyik oldalról sem keletkeztet kötelezettséget, nehezen kezelhető a rangsor kialakításakor. Ebben az esetben a tárca szabályozása szerint ugyanazon folyamatot kellene végrehajtani, amely megegyezik a verseny újraindítása nélküli esetben.

A honvédelmi tárca központosított közbeszerzése esetében ezen eljárásmód kizárólag azon esetekben kerül alkalmazásra, amennyiben a központi beszerző szervezet által lefolytatott keretmegállapodásos eljárás első részében egy győztes került kihirdetésre.

A verseny újraindításával történő kiválasztás:

A verseny újraindításával történő eljárásmód megegyezik a Kbt. szerinti eljárásrenddel.

Ez esetben a honvédelmi szervezet, mint ajánlatkérő közvetlen írásbeli ajánlattételi felhívást küld valamennyi (részteljesítés esetén az adott rész vonatkozásában valamennyi) keretmegállapodásos partnernek. Az ajánlatok egyszerű kiértékelését követően szerződést köt a nyertes ajánlatot benyújtó keretmegállapodásos partnerrel. A verseny újbóli megnyitása során elektronikus árlejtés alkalmazható, amennyiben az erre való utalás szerepel az ajánlattételi felhívásban.

VÁLTOZÁSOK KEZELÉSE

Termékváltás:

Annak érdekében, hogy a keretmegállapodás időtartama alatt a honvédelmi szervezetek folyamatos ellátottsága biztosítható legyen, fenn kell tartani a teljesítőképességet a megszűnő termékek esetén kiváltó termék szabályozott formában történő bevezetésével.

Ennek formája az időszakosan lehetővé váló termékváltás.

A termékváltás tehát egy olyan lehetőség, amely során a megszűnő termék helyett a Szállító által egy, a kiváltandó termékkel azonos gyártmányú, legalább ugyanolyan műszaki tartalommal és egyéb feltételekkel rendelkező (helyettesítő) termék, amelynek ára nem haladhatja meg az eredeti termék árát. A kiváltó termék nem térhet el a dokumentációban, illetve keretmegállapodásban megkövetelt feltételektől. A kivont terméket későbbi időpontban újra nem lehet a szállítható termékek körébe visszaemelni. A kiváltott, már megrendelt (egyedi szerződéssel szerződött) termékek legkésőbbi szállítási határideje a termékváltást követő hónap utolsó napja, illetve az adott konkrét szerződésben szereplő szállítási határidő.

Árfolyamváltozás követése

A központi beszerző szervezet célja, hogy olyan feltételrendszert alakítson ki, amely a felek részére minél kevesebb kockázatot tartalmaz. Meggyőződésem, hogy csak ezáltal, s ennek következetes megvalósításával érhető el, hogy a beszerzés hatékony lehessen.

A keretmegállapodás keretében szállított termékek árai meghatározott ideig rögzítettek. A szerződéses árak ezt követően emelkedhetnek abban az esetben, ha a KSH által hivatalosan közzétett, az előző évre vonatkozó éves fogyasztói árindex mértéke az 3%-ot meghaladja. Az áremelés alapja a KSH által évente hivatalosan közzétett éves fogyasztói árindex. Az ilyen, fogyasztói árindexen alapuló ármódosítás nem igényel szerződésmódosítást.

A Szállítónak minden hónapban egy alkalommal, véglegesen vagy 1 naptári hónapos időtartamra lehetősége van egyes vagy valamennyi keretmegállapodás hatálya alá tartozó termék keretmegállapodásos árának csökkentésére.

A csökkentett áron való megrendelési/beszerzési lehetőség további feltételhez (mint például más termék egyidejű megrendeléséhez, stb.) nem köthető, az kizárólag valamennyi honvédelmi szervezet részére hozzáférhető, egységes feltételek szerint történhet.

KÖVETELMÉNYEK

Annak érdekében, hogy a korábban vázolt ellátási rendszer hatékonyan működjön az alábbi feltételeket szükséges megteremteni:

- A keretmegállapodásos eljárás első részében szükséges részletesen meghatározni az egyes élelmiszer termékek műszaki követelményeit (kiemelten az élelmiszerbiztonsági kérdéseket); a részajánlattételi kört (régiónként, területenként, vagy alakulatonként)
- Szükséges a központi beszerző szervezet honlapjának fejlesztése annak érdekében, hogy az adott keretmegállapodás feltételrendszerei (árak, akciók, eljárás mód, megrendelés) naprakészen elérhetővé válhasson;
- A honvédelmi szervezetek vonatkozásában célszerű áttekinteni az informatikai eszközparkot (internetes elérhetőség) az aktualitások eléréséhez;
- Szükséges pontosítani, hogy a honvédelmi szervezetek megrendeléseit a központi beszerző szervezet felé a Szállító jelenti be, vagy maga a honvédelmi szervezet;
- Tekintettel arra, hogy a jelenlegi jogszabályok alapján a keretmegállapodásos eljárás első és második részének lefolytatása NFM engedély köteles, kezdeményezni szükséges az ezirányú jogszabály módosítást;
- a Végrehajtó állomány részére az eljárás gyakorlati megvalósítása érdekében oktatás megtartása indokolt.

ÖSSZEGZÉS

Láttuk, hogy a honvédelmi szervezetek ellátása érdekében folyamatosan jól működő logisztikai rendszer kell működtetni. Az élelmiszer ellátás legfőbb problémája a folyamatosan változó piac, valamint a honvédelmi szervezetek igényeinek változásai.

A cikk felvázolt egy olyan megáldási javaslatot, amelynek segítségével a honvédelmi szervezetek kisebb időigénnyel, humán erőforrás növelése nélkül képesek ezen ellátást biztosítani.

A rendszer működő képességét kizárólag a gyakorlati tapasztalatok alapján lehet értékelni, azonban más (EU, államigazgatási, önkormányzati) szervezetek több éves tapasztalatai megfelelő alapot jelenthetnek.

Felhasznált irodalom

- [1] 1. Derzsényi Attila: Élelmiszer beszerzés aktuális kérdése (Hadmérnök: VII. Évfolyam 2. szám - 2012. június) pp.213-220.
Forrás: http://www.hadmernok.hu/2012_2_derzsenyi.pdf) (letöltés ideje: 2012. 10. 31.);
- [2] Derzsényi Attila: Honvédelmi célú beszerzésről közérthetően (Katonai Logisztika Online 2011. év 1. szám) pp. 95- 109. Forrás:
<https://www.parbeszed.hm.gov.hu/sites/kulso/Documents/katonaisajto/katonailogisztika/2011/1/Derzs%C3%A9nyi.pdf>);
(letöltés ideje: 2012. 10. 31.)
- [3] Derzsényi Attila: Honvédelmi tárca központosított közbeszerzése, Diplomamunka (Zrínyi Miklós Nemzetvédelmi Egyetem Budapest 2010) pp. 1-80.
- [4] Dr. Horváth Attila: „Az élelmiszerellátási lánc kritikus infrastrukturális, terrorfenyegetettségének jellemzői” (Hadmérnök: IV. Évfolyam 2. szám - 2009. június) pp.437-449; Forrás: http://www.hadmernok.hu/2009_2_horvatha.php
(letöltés ideje: 2012. 11.07.)
- [5] NATO General Administrative Clauses Procurement and Supplies Services;
Forrás: http://www.nato.int/structur/procurement/doc/GAC_EN.pdf
(letöltés ideje: 2012. 10. 31.)
- [6] Support for Improvement in Governance and Management:: Central Purchasing Bodies, (OECD publishing August 2011.);
Forrás: <http://www.oecd.org/site/sigma/publicationsdocuments/48630136.pdf>
(letöltés ideje: 2012. 10. 31.)
- [7] A „közbeszerzésekről” szóló 2011. évi CVIII. törvény (2012. október 31-én hatályos állapota);
- [8] 168/2004. (V. 25.) Korm. rendelet a központosított közbeszerzési rendszerről, valamint a központi beszerző szervezet feladat- és hatásköréről (2012. október 31-én hatályos állapota);
- [9] 46/2012. (III. 28.) Korm. rendelet a fekvőbeteg szakellátást nyújtó intézmények részére történő gyógyszer-, orvostechnikai eszköz és fertőtlenítőszer beszerzések országos központosított rendszeréről (2012. október 31-én hatályos állapota);
- [10] 12/2012. (VII. 30.) ORFK utasítás a Rendőrség Beszerzési Szabályzatáról;
- [11] 46/2009 (IX.5) Budapest Fővárosi Közgyűlés rendelet.

Horváth Attila

horvath.attila@uni-nke.hu

AZ UTÁNSZÁLLÍTÁS ELMÉLETÉBEN BEKÖVETKEZETT VÁLTOZÁSOK AZ 1930-AS ÉVEKBEN

Absztrakt

A trianoni békeszerződést követően az 1920-as évek végére alakult ki a két világháború közötti katonai stratégia. A hadászati tervek egy szomszédos kisantant országgal szembeni – Csehszlovákia vagy Jugoszláviai – elleni megelőző támadásra koncentráltak. A katonai stratégiai megvalósíthatóságának feltétele számos kérdést vetett fel. Ezek közé tartoztak pl. a trianoni békeszerzős katonai határozványainak kijátszása, a haderő korszerűsítése, a gyors felvonulás feltételeinek biztosítása. A célok megvalósítása érdekében az adott keretek között mozgékonyabbá kellett tenni a haderőt. Ez a feltétel érintette a hadműveleti utánszállítás szervezeteit, elveit és módszereit is. A cikkben a szerző azt vizsgálja, hogy a katonai stratégia milyen változásokat eredményezett a hadműveleti területen történő anyagszállítások elveiben és módszereiben. Ennek tapasztalatai, akár jól hasznosíthatók napjainkban is.

Following the Trianon Treaty the military strategy for the period between the two world wars had been formed by the end of 1920. The operational plans were focusing on a pre-emptive strike against neighbouring Little Entente countries such as Czechoslovakia and Yugoslavia. The feasibility of this particular military strategy indicated many questions like how to evade the military restrictions of the Trianon Treaty, how to develop capabilities, or how to increase the mobility of the military services, and so on. To achieve their aims within the frameworks available, the increase of operability of the armed forces seemed to be essential. This condition affected the operational logistics forces, their means and procedures. The author of this article also analyses how the changes in military strategy resulted in amendments in the rules and procedures of the flow of materials in the operational area. We hope that the lessons learnt may also be useful nowadays as well.

Kulcsszavak: katonai stratégia, ellátási rendszer, mozgékonyág, utánszállítási rendszer ~ military strategy, support system, mobility

BEVEZETŐ

Egy katonai stratégia megvalósításának számtalan feltétele és követelménye van. A kiemelt célok megvalósítását szinte bármilyen területen hátráltathatják vagy akár meg is hiúsíthatják, ha a stratégiát nem a komplex rendszerben értelmezik. A trianoni békediktátum tiltó rendelkezései ellenére a két világháború közötti magyar katonai stratégia lényegi elemeit az 1920-as évek végén határozták meg. A hadászati elképzelések megvalósítása komoly követelményeket támasztott a hadszíntéri utánszállítási rendszerrel szemben is.

A cikkben a szerző levéltári és szakirodalmi forrásokra támaszkodva tárja fel, hogyan felelt meg – a hadtörténelemben méltánytalanul elhanyagolt – szállítószolgálat a hadművelleti és hadászati követelményeknek. A tanulmány a korabeli szabályzatokra, illetve a katonai szaksajtóban megjelent cikkekre is támaszkodik. A témából lesűrhető tanulságokat nem csupán napjaink katonai vezetői és logisztikai szakemberei hasznosíthatják.

A két világháború közötti katonai stratégia szállító szolgálattal kapcsolatos feltételei

Magyarországnak 1927 után a közvetlen katonai ellenőrzés megszűnése után nyílt arra lehetősége, hogy a méltánytalanul szigorú trianoni békediktátum katonai határozványaiiban meghatározott feltételeket kijátssza. A Szövetségek Közi Ellenőrző Bizottság távozása korántsem jelentette a fegyverkezési egyenjogúság elnyerését, a fegyverkezést és a háborús hadrendre való áttérést továbbra is rejtve kellett megoldani. Az 1920-as évek végére körvonalazódtak a két világháború közötti magyar katonai stratégia elképzelései. A magyar hadászati elvek abból indultak ki, hogy egy gyors felvonulással ellensúlyozni lehet a kisantant államok nyomasztó katonai fölényét. Ugyanis az ún. utódállamoknak az 1920-as években még nem sikerült kiépíteniük egy a gazdasági, társadalmi és katonai érdekeiknek megfelelő egységes vasúthálózatot. Így realitásnak tekinthető az a számvetés, hogy a szomszédos országok hadseregei felvonulását a magyar haderő közlekedési szempontból megelőzheti. Ugyanakkor a vezérkar azzal is tisztában volt, hogy a kisantant országok fejlesztései révén ez az „előny” fokozatosan csökkenni fog.¹ Az erők gyors felvonulásával, a csehszlovák hadsereggel szemben az „Fr” (felriasztás) 9. napig, a román haderővel szemben a 7. napig lehetett erőfölényt fenntartani. A földrajzi viszonyok és a honvédség kedvezőtlen diszlokációja miatt Jugoszláviával szemben csak a meglevő túlsúly csökkentéséről lehetett szó.²

A katonai stratégiai elképzelések kialakításával párhuzamosan megkezdődött a magyar haderő szervezetének és felszerelésének korszerűsítése, valamint a mozgósítási „Fr” (felriasztási) hadrendre való áttérés feltételeinek javítása.³ A hadászati tervek megvalósíthatóságának egyik legfontosabb alapjának lehet tekinteni, hogy az ún. első vonalbeli hadosztályok gyorsan térjenek át a háborús „Fr” hadrendre, és két nap alatt ériék el a menetkésztséget.⁴ A vezérkar elképzelései szerint a honvédség alakulatai a menetkésztség elérése után egy gyors felvonulást követően megelőző támadást hajtottak volna végre Csehszlovákia vagy Jugoszlávia ellen. A csapatok a román haderővel szemben pedig a Tisza vonalán fedező védelemre rendezkedtek volna be. A felvonulási és a hadművelleti tervek is ebből a feltevésből indultak ki, így a hadsereg kétharmada a támadó főcsoportosítást, a

¹ Hadtörténelmi Levéltár (a továbbiakban HL.) Vkf. Eln. VI/7.k.o. 50049/ 1929. Tanulmány gyűjtemény, Tanulmány a katonai közlekedés fejlődéséről.

² HL. Vkf. Eln. VI/1.o. 1999/1/1929. Adatok a honvédség béke és "Fr." helyzetéről 1919-től 1931-ig.

³ Erről a kérdéssel lásd bővebben: Dombrády, Lőránd-Tóth, Sándor (1987): A Magyar Királyi Honvédség 1919-1945. Zrínyi Katonai Könyv- és Lapkiadó, Budapest.

⁴ Dombrády, Lőránd (2000): *Katonapolitika és hadsereg 1920-1944*. Ister Kiadó és Kulturális Szolgáltató Iroda. Budapest, 20. p.

fennmaradó rész pedig védelemre rendelkezett be.⁵ Egyben ez azt is tükrözi, hogy a magyar haderő egyszeri erő kifejtésre volt csak alkalmas, az erők és eszközök tartalékképzésére nem volt lehetőség.

Egy Csehszlovákia elleni támadás esetére a támadó hadművelet céljaként az Eperjes-Margittfalva-Zólyom-Nyitra-Pozsony vonal elérését, egy Jugoszlávia elleni támadáskor a Duna vonalára való kijutást határozták meg.⁶ A vezérkar tisztában volt a térség korabeli erőviszonyaival. Így azzal számoltak, hogy egy kedvező nemzetközi katonapolitikai helyzet kialakulásakor a megkezdett támadás tovább folytatható. Ennek a feltételezésnél abból indultak ki, hogy a szomszédos kisantant államok az első világháborút követően nem csupán Magyarország rovására terjeszkedtek, hanem más államok érdekeit is sértették pl. Ausztria, Bulgária, Németország és Olaszország.⁷ A magyar hadvezetés a geopolitikai helyzet kedvezőtlen alakulása esetén, a realitás talaján állva számvetett azzal is, hogy a megelőző támadás elakad és a kisantant haderők elfoglalják Budapestet. Ebben az esetben a megelőző támadást arra tartották alkalmasnak, hogy a főváros elfoglalásának idejét az „Fr”-től számított 3-4 hétig kitolják.⁸

A hadászati elképzelések megvalósítása teljes egészében érintette honvédség teljes szállítószolgálatát, beleértve a katonai vasúti hatóságokat és alakulatokat, illetve a műveleti utánszállításokat végző vonatalakulatokat is. A hadászati követelmények szerint a katonai vasúti hatóságoknak egy új irányítási rendszer bevezetésére és működtetésére kellett felkészülniük. A vasúti szállítással felvonuló csapatokat a menetkésztségük elérése után egyirányú körforgalom általánossá tételével tervezték el a kirakás körzetébe eljuttatni, ahol az újonnan hadrendbe állított rakodószázadok szükség esetén szükségakadókát építettek ki.⁹ Ennek a módszernek az alkalmazásával kívánták lerövidíteni a vasúti szállítások idejét. A nagyobb vasúti szállítási teljesítményt úgy lehetett megvalósítani, hogy a két egyvágányú vonal esetén körforgalmat kellett bevezetni, ahol az egyik vonalon a teli, a másikon az üres vonatok futottak. Bevezetésével a vonatsűrűséget a kétszeresére lehetett növelni.¹⁰

A korabeli elveknek megfelelően a mögöttes területekről, ameddig csak lehetséges volt, a hadműveleti területre vasúton szállították az anyagokat. Az anyagi szállítmányokat a vasúti felvételező helyekről a csapatokig vonatcsapatok szállító oszlopai jutatták el. A gyors felvonulás komoly akadályát képezték a hadszíntéri utánpótlási szállítások végrehajtására hivatott, túlnyomórészt fogatolt járművekből álló vonatalakulatok.¹¹ Az országos járművekkel kétfogatú utánszállító lépcsők jelentős mértékben lassították a sereg- és csapattestek menetét. Az utánszállító lépcsők három, egyenként 20 országos járműből álló szakaszra és egy 10 országos járműből álló saját részlegre tagozódtak.¹² Egy-egy szakaszba azért szerveztek 20 db 0,5t teherbírású fogatolt járművet, hogy a vasúti végállomásokról és felvételező helyekről legyenek képesek egy 10t-s vasúti kocsira rakott anyagot elszállítani. A sok jármű és állat miatt meglehetősen nehézkes volt az utánszállító lépcsők mozgásszervezése és menet közbeni

⁵ Horváth, Attila (2002): A hadszíntér előkészítés és a közlekedési ügy összefüggései a két világháború között pp. Hadtudományi Tájékoztató. Budapest, 2002 évi 2. szám 65-86.

⁶ HL. Vkf. Eln. VI/ 1.o. 9.205/hr/1935. Az 1935. évi Emlékirat

⁷ Horváth Attila: i.m. (2002).

⁸ HL. Vkf. Eln. VI/ 1.o. 9.205/hr/1935. Az 1935. évi Emlékirat.

⁹ Horváth, Attila (1997): *A Magyar Királyi Honvédség szállító szolgálatának működési elvei és annak gyakorlati kérdései (1922-1941)*. Kandidátusi értekezés. Budapest, Megőrzési helye: a Nemzeti Közzolgálati Egyetem Könyvtára.

¹⁰ Berger, Károly (1930): *A Vezetés Kézikönyve*. I. kötet. Stádium Sajtóvállalat Részvénytársaság Budapest. 248.o.

¹¹ A vonatcsapatoknak két szintjét különböztették meg, harcászati szinten (zászlóalj, ezred) a csapatvonatok feladata volt az utánpótlási anyagok szállítása, míg hadműveleti- és hadászati szinten ez a feladat a seregvonatok állományaiba szervezett szállítóoszlopok feladata volt.

¹² HL. Vkf. Eln. VI/ 3.o. 33. 402/ 1923. Vonatcsapat átszervezése "F" esetére.

vezetése is. Ráadásul az 1920-as évek elején kialakított hadrendben a hadosztály, hadtest, illetve a Fővezérség közvetlen seregvonatokot úgy osztották el, hogy az egyes hadművelleti szervezetek művelleti képességének biztosítsák az anyagi alapját. Így a honvédség „Fr” hadrendje olyan sok seregvonatot foglalt magában, amely jelentős mértékben hátráltatta a haderő mozgását, szinte lehetetlenné téve az előbbieken vázolt hadászati elképzelések esetleges megvalósítását.

Az utászallítási rendszer gyorsítására kétségkívül az utászallítási lépcsők fogatolt járműveinek kiváltása lett volna optimális megoldás. A gépkocsioszlopokat csak a gyorscsapatok, illetve a Fővezérség közvetlen szervezetek hadrendjébe állítottak be. Erre egyébként még az ún. „győri program” meghirdetése után sem nyílt reális lehetőség, mert az ország teherbíró képessége miatt még a gyorscsapatok gépjárművel való ellátása is csak nagy nehézségek árán sikerült. Ezért nem maradt más lehetőség, mint a hadászati követelményekhez igazítva átgondolni az utászallító lépcsők elosztását és alkalmazási elveit.

A HADMŰVELETI UTÁNSZÁLLÍTÁS SZERVEZETÉBEN ÉS ALKALMAZÁSAI ELVEIBEN BEKÖVETKEZETT FONTOSABB VÁLTOZÁSOK

A vázolt körülmények között az utászallítási rendszer rugalmasságát, illetve a seregtestek mozgékonyágát csak abban az esetben lehetett növelni, ha a honvédség hadrendjébe kevesebb seregvonatot szerveznek. Ezt csak úgy lehetett elérni, hogy csökkentették a csapatok által állandóan magukkal szállított élelmezési készlet nagyságát. 1933-tól kezdően a honvédség az ún. „központiasan” szervezett utászallítási rendszerre tért át. Ennek keretében jelentős mértékben csökkentették a hadrendben a seregvonatokot. Az utászallító lépcsők elnevezése kocsioszlop lett, ennél azonban jelentősebbnek lehet tekinteni tartalmi kérdésekben bekövetkezett vezetési és alkalmazási kérdéseket.

Fontosabb szervezeti és módszerbeli változások

Az átszervezést követően a központilag szervezett utászallítási rendszerben a kocsioszlopok tagozatonkénti kötött, egymásra épülő alkalmazása helyett a szállítási feladat nagyságrendjének és körülményeinek figyelembevételével, azok „panelszerű” elosztása vált lehetővé.¹³ A hadsereg „Fr” hadrendjében 1935-ben a felső vezetési szintekhez 57 kocsioszlopot szerveztek, ebből 6 egyenlő megosztásban a *hadtestek*, 9 a *hadsereg*, a fennmaradó 42 pedig a *Fővezérség közvetlen* állományába tartozott. A hadosztályok 4 löszert szállító és 1 élelmiszert szállító (a lovashadosztály 1-1 löszeres és élelmezési, H. A.) kocsioszloppal rendelkeztek.¹⁴ 1936-ban az „Fr.” hadrendben a dandár szervezetre történő áttérést követően a *hadtestek*hez egyenként 8 (amelyből 2 löszert, 3 élelmiszert, 3 a többi intézet anyagát szállította, H. A.), a *hadsereghez és Fővezérség közvetlen alakulatokhoz* 44 kocsioszlopot szerveztek.¹⁵ 1940. április 1-én a hadsereg kocsioszlopai az alábbiak szerint oszlottak meg: a *dandárok* 4 löszert szállító, az *1-2 lovas dandár* 1-1 löszert-, élelem-, és általános szállító, a *Fővezérség közvetlen alakulatok* 54 kocsioszloppal rendelkeztek. A hadtestek fogatolt utászallító egységeinek száma és eloszlása nem változott.¹⁶ A Fővezérség a kialakult hadművelleti és szállítási helyzet és a végrehajtandó feladatok szerint utalta ki a hadseregek részére a kocsioszlopokat.

¹³ Horváth, Attila (1993): *A Magyar Királyi Honvédség szállító szolgálatának működési elvei és annak gyakorlati kérdései (1922-1941)*. Kandidátusi értekezés. Budapest, Megőrzési helye: a Nemzeti Közszerológati Egyetem Könyvtára.

¹⁴ HL. Vkf. Eln. VI/ 1.o. 9.10/hr./1935. Az 1934. évi Emlékirat.

¹⁵ HL. Vkf. Eln. VI/ 1.o. 9.205/hr./1935. Az 1935. évi Emlékirat.

¹⁶ Csima János: i. m. 17. sz. Vázlat; A kivonuló hadrend 1940. április 1-én. 75.p.

A „központiasan” szervezett utánszállítási rendszer bevezetése az ellátó szolgálat szervezeteinél óhatatlanul jelentős változásokat eredményezett. Ezek közül kiemelkedik az ellátó oszlopok megalakítása. A folyamatos utánszállítás megkövetelte a szűk keresztmetszetet képező elosztó-, felvételező-, átrakóállomásokon végzendő átrakások és anyagrendezések gyorsítását, és az egyébként az anyag átadás-átvétellel együttjáró bizonylatolás lerövidítését. Az anyagáramlás folyamatában elkerülhetetlenül jelentkező tárolási, raktározási, elosztási feladatok elvégzésére az addigi utánszállító kirendeltségek, átrakó- és felvételező állomások funkcióinak átvételére, létrehozták az egyetemes jellegű szervezetszerű anyagi alakulatokat, az ún. ellátóoszlopokat. Ezeket a hadtápterület kezdő vasútállomására, illetve a hadművelleti területen az alkalmazás függvényében átrakó- illetve felvételező állomásként telepítették. Az ellátóoszlopok mint egyetemleges anyagi intézetek, magukban foglalták az oszloptörzset, az átrakó állomás-, a felvételező állomás- és munkásosztásokat, valamint a gazdasági hivatalt. Az átrakó- és felvételező állomások feladatait ellátóoszlopok létrehozásával integrálták az anyagi szolgálatok korábban vasútállomásokhoz vezényelt szakszemélyzetét.¹⁷

Az ellátóoszlop létrehozásával az ellátási csoportképzés egyszerűsödött, és a létrehozott csoportokat kiszolgáló anyagi intézet szervezete egységesebbé vált. Elvileg, lehetőség szerint külön, minden hadosztály és a felső vezetés által létrehozott vonatscsoport anyagi alapjának biztosítása érdekében külön ellátóoszlopot jelöltek ki. Ezt a hadtest, hadosztályvonat csökkentése ellenére minőségi előrelépésnek lehet tekinteni, mert az 1924-ben kiadott H. Sz. szerint a hadsereg részére egy teljesítőképessé vasútvonalat kellett kijelölni, és a megváltozott utánszállítási rendszerben elvileg minden hadtest külön vasútvonalat kapott.

Az ellátóoszlopok így módon történő decentralizálása ellenére is, azok a szállásmester alárendeltségében maradtak, aki meghatározta a telepítés módját és helyét. Az ellátóoszlopok nem kerültek az anyagi vezérkari tisztek vagy a vonat parancsnokok alárendeltségébe még akkor sem, ha az ő működési területükön tevékenykedtek. A szállásmester a hadművelleti terület hadtápi kezdő állomására beérkezett anyagokat a saját ellátóoszlopával vette át és osztatta el. Amennyiben az elosztóállomás forgalma vagy a meghatározott terület vasútműszaki jellemzői azt megkívánták, az anyaországból beérkező szállítmányokat több ellátóoszloppal rendezték. A kezdőállomásra kirendelt oszlopok tevékenységének összehangolására továbbra is kirendeltséget állítottak fel, vezetésére általában vezérkari tiszteket jelöltek ki.¹⁸

Az ellátóoszlopokat kedvező utánszállítási helyzetben egységes, kedvezőtlen körülmények között megosztott telepítésben alkalmazhatták. Az anyagáramlás gyorsaságának és a hatékony vezetés feltételeinek megteremtése céljából egyaránt az egységes telepítést tartották kívánatosnak, mivel ebben az esetben az utánszállítási folyamatot nem szakították meg átrakódással és raktári műveletekkel. Egységes telepítéskor az anyagátadást is a vasúti végállomáson vagy annak közelében hajtották végre. A megosztott telepítésre, a már tárgyalt elvek szerint, bonyolult hadművelleti és utánszállítási helyzetben került sor a vasúti végállomás lemaradásakor. A kényszerű, megosztott telepítéskor az ellátóoszlop parancsnoka az átrakóállomáson tartózkodott. Az utánszállítási vonal erőteljes leterheltségekor vagy ha a vasúti hálózat gyér sűrűsége azt megkívánta, egy vasúti végállomáson több ellátóoszlopot kellett üzemeltetni, a szállásmester az egységes irányítás biztosítása céljából külön közeget (általában vezérkari tiszteket, H. A.) rendelt ki.

A hadosztályok utánszállító egységeit az ellátóoszlopoktól a hadosztály felvételező helyre történő szállításkor csak szükség esetén, az utánszállítási rendszer összeomlásakor vonták be.

¹⁷ Vezérfonal az anyagi ellátás végrehajtására a csökkentett seregvonatokkal kapcsolatban. Segédlet. A Honvédelmi Minisztérium kiadványa. Budapest. 1933. /A továbbiakban: Vezérfonal: i.m. (1933)/ 5. p.

¹⁸ Az elosztó állomásra kiküldött vezérkari tiszti vezetése alatt álló kirendeltség állományát csökkenteni lehetett, mert az ellátóoszlopok szakközegei a szervezet jellegéből fakadóan a korábbi feladatokból átvettek.

A hadműveleti egységek a megmaradt rendszeresített szállítóeszközeikkel a felvételező helyről belső szállításokat végeztek a csapatok felé. A felvételező helyek a korábbi szolgálati áganként való település helyett egységes rendszerben települtek az anyagi vezérkari tiszt által kijelölt helyen, így a csapatok vételezése, illetve a kiszállítást végző kocsioszlopok megrakása egy körletben történt, egyszerűsítve és lerövidítve ezzel az országos járművek megrakását. A hadosztályvonatok csökkentése az ellátás szempontjából tovább szűkítette a hadműveleti egységek önálló irányban történő alkalmazásának lehetőségét. A felvonulási és alkalmazási tervek készítésekor viszont eleve számoltak – főként határbiztosítási feladatok ellátására – hadműveleti egységek vagy azok részeinek elkülönített alkalmazásával, elsősorban a tervezett román arcvonalon.¹⁹ Az átszervezéssel a hadosztályok nagyobb mértékű anyagi megerősítésre volt szükség, amelyet a Fővezérség biztosított az egyes utánszállító egységek, anyagi és egészségügyi intézeteknek az önálló feladat időtartamára történő alárendelésével.

Ezek a változások tették lehetővé az ellátási elemeknek már említett láncszerű egymásba fonódásával együttjáró tagozatonkénti utánpótlási folyamat megszűnését. Az új elvek szerint a vasúti végállomástól a hadosztályok felvételező helyéig az utánszállítást a hadseregparancsnokság hajtotta végre a saját szállítóeszközeivel. Az egyes szolgálati ágak intézeteinél is szervezeti változások következtek be, és ezzel párhuzamosan működési elveik is a „központiasan” szervezett utánszállítási rendszernek megfelelően módosultak.

Egy korábbi ellátó szervezeti elem a lőszertelep megszüntetésével egyidejűleg csökkentették a seregvonattal szállítandó lőszer mennyiségét. A csökkentést az tette lehetővé, hogy a lőszerfogyasztás mértékének megállapításánál a mozgóháború lövésszaki követelményeit érvényesítették. Ez alapján könnyű csatanapon 0,5 (1), közepes csatanapon 1 (2), heves csatanapon 1,5 (3), (erőszakos folyamatkezelések során és erődtímeny megtámadásakor az érték a megállapított norma értékének kétszeresére is emelkedhetett, H. A.) javadalmazás lőszerfogyással számoltak.²⁰ Az 1933-as átszervezést követően a lőszer tüzérségi segédszolgálat feladatköréből kikerült a tüzérség személyzete és lovai pótlása. A kialakított elvek szerint valamennyi fegyvernem személy- és a lópótlását egységesen kellett kezelni.²¹

A megváltozott rendszer hatása az élelmiszer készletek beszerzésére és biztosítására

A hadbiztonsági szolgálathoz tartozó élelmezési anyagok beszerzési- és szállítási problematikájának megoldása vált tulajdonképpen az átszervezés legfontosabb feltételévé. Az élelmezési anyagok biztosításának módját gyökeresen megváltoztatták, és azt szinte teljes egészében a helyszíni beszerzésre alapozták. Az élelmezési anyagok típusvonatokkal való utánszállításával az anyaországból csak az első felvonuláskor, illetve akkor számoltak, ha a hadműveleti terület segélyforrásai nem bizonyultak elegendőnek.²² A helyszíni beszerzés kiterjesztését egyrészt a vezérkar a lehetséges hadszínterekkel kapcsolatos számvetések, másrészt a várható háború felszabadító jellege miatt tartotta lehetségesnek, mert feltételezték a helyi lakosság (a trianoni határokon kívül élő magyarok, H. A.) együttműködését.

Az élelmezési ellátás aktuális kérdéseinek megoldásával kapcsolatban a Magyar Katonai Szemle szerkesztősege 1932-ben pályázatot írt ki, és a legjobb pályamunkákban megfogalmazott nézeteket az új szabályozók kialakításakor figyelembe vették. Putz Mátyás (a pályamunkáját az értékelést követően 1.000 pengővel jutalmazták, H. A.) lényegében a „központiasan” szervezett utánszállítási rendszer megvalósítását javasolta, a mozgó javadalmazás szintjének csökkentésével. Az általa kidolgozott változat szerint a lecsökkentett

¹⁹ HL. Vkf. Eln. VI/ 1. o. 9.010/hr./1935. Az 1934. évi Emlékirat.

²⁰ Vezérfonal: i.m. (1933) 11. p. A zárójelben levő értékek az 1924-ben meghatározott normát jelentik

²¹ HL. Vkf. Eln. VI/6. o. 72.112/1938. A H. Sz. III. Rész letárgyalása vezetőségi értekezleten.

²² Vezérfonal: i.m. (1933) 12. p.

mozgójavadalmazás nagysága lehetővé tette, hogy a vasúti végállomásról a hadművelleti egységek napi szükségletét átrakás nélkül lehessen kiszállítani. Felismerte a helyszíni beszerzés feszes megszervezésének és végrehajtásának fontosságát. Az ezzel kapcsolatos súlypont áthelyeződéssel törvényszerűen jelentkező feladatok megoldására az ellátóhivatalokat alkalmatlannak ítélte meg, és beszerző különítménnyé történő átszervezését javasolta. Putz szerint a beszerző különítmény megalakításával az ellátóhivatal szakszemélyzetét meg kellett kétszerezni, az addigi 30 fő helyett 60 főt tartott a beszerzési feladatok elvégzésére kívánatosnak. Az utánszállítási igények kielégítésére a különítményhez rendszeresített utánszállító lépcső felállítását javasolta.²³ A beszerzés megnövekedett feladatai elvégzésére az ellátóhivatalokat alkalmatlannak ítélte meg Koncz György is (akinek a pályázatát megjelenésre alkalmasnak ítélte meg a bíráló bizottság, H. A.). Az általa kidolgozott javaslat szerint felállítandó hadosztály gazdasági osztályok rendszeresítése és a hadművelleti egységek vonatai csökkentése nem haladta meg azt a mértéket, amivel a mozgékony módon számottevően javítani lehetett.²⁴

A Vezérfonal kiadásával egyidőben végül is a kétlépcsős beszerzési rendnek megfelelően, a beszerzés súlypontját (amely egyben térbeli kiterjedés és a beszerzés célja miatt második lépcsőt is jelentett, H. A.) képező hadművelleti terület hátsó határára, a hadtáp terület gabonaneműinek, vágóállatainak és más élelmezési készleteinek begyűjtésére, az ún. élelembeszerző oszlopokat rendszeresítették. Az 1933-ban létrehozott új anyagi szervezet létszáma a Putz Mátyás által megalakítandó beszerző különítményét is meghaladta, mert állományába 4-5 élelmezésügyi gazdasági tiszttel, 3 altiszttel, 120-140 főnyi legénységet, 1 kocsioszlopnak megfelelő számú országos járművet és 3 db. motorkerékpárt szerveztek.

A kialakított elvek szerint a hadsereg legalább annyi élelembeszerző oszloppal rendelkezett, mint amennyi hadosztály tartozott az alárendeltségébe. Az élelembeszerző oszlopok a begyűjtött készleteket rendszeresített szállítóeszközeikkel, a vezetésükre kirendelt hadbiztosok utasításai szerint a kijelölt fiók-, majd főgyűjtőhelyekre szállították.²⁵ A főgyűjtőhelyek kijelölésénél arra törekedtek, hogy azok vasútállomásokra, vagy nagyobb útcsomópontokra essenek, és egyben biztosítva legyenek a megfelelő feldolgozás (pl. elegendő malom álljon rendelkezésre, H. A.), valamint az előírás szerinti raktározás feltételei. A főgyűjtőhelyekről a hadsereg szállásmesterei az ellátóoszlopokon keresztül a hadművelleti egységekhez csak akkor szállították ki helyi utánszállítás formájában az élelmezési létszámnak megfelelő élelmezési anyagot, ha a csapatok és hadosztályok beszerzése eredménytelen maradt. Ezt az elvet azért így határozták meg, mert csapattek beszerzése a begyűjtés folyamatában első lépcsőt képezett.²⁶ A csapatok és hadosztályok ellátóhivatalaiból lényegében változatlan állománnyal megszervezett ún. élelmező oszlopok a folyó élelmezéshez szükséges készleteket gyűjtötték.²⁷

Az egészségügyi kiürítés rendszere

A mögöttes egészségügyi intézetek telepítésénél az első világháborút követően is arra törekedtek, hogy a vasút hálózat adta lehetőségeket minél jobban kihasználják. Ezt nem csupán a gyors és tömeges hátraszállítási lehetőségek miatt tartották szükségesnek, hanem azért is, mert a vasútállomások a tábori körülményeknél jobb infrastrukturális lehetőségeket biztosítottak a sérültek betegek ápolására.²⁸ A hadművelleti területről a sérülteket és betegeket

²³ Putz Mátyás: Háborús élelmezés megszervezése a mai közlekedési viszonyok mellett. Magyar Katonai Szemle. 1933. évi. 8. szám. pp. 159-173. és 1933. 9. szám. pp. 160-187.

²⁴ Koncz György: Háborús élelmezés megszervezése a mai közlekedési viszonyok mellett. Magyar Katonai Szemle. 1933. évi. 10. szám. pp. 161-193. és 1933. 11. szám. pp. 169-199.

²⁵ Vezérfonal: i.m. (1933) 12-13.p.

²⁶ Horváth Attila: i.m. (1997). 184.o.

²⁷ Vezérfonal: i.m. (1933) 14. p.

²⁸ Horváth Attila: i.m. (1997). 51.o.

a vasútállomásokon települt egészségügyi intézetektől vasúton szállították el a hátszági polgári és katonai kórházakba.

Az egészségügyi szolgálatban az 1933-as átszervezés során a hangsúlyt továbbra is arra fektették, hogy a sebesülteket és betegeket minél gyorsabban elszállítsák a seregtestektől. Ugyanakkor az intézetek (tábori kórházak, segélyhelyek, betegvonatok, kórházvonatok, rögtönzött betegszállító vonatok stb.) zömét, vagyis az ellátás súlypontját a hadművelleti terület hátsó határára a hadtápterületre helyezték. Az említett változásokból következően növelni kellett a sebesültszállító gépkocsioszlopok számát. Az „Fr.” hadrendben a hadosztályok és a hadtestek egyaránt 1-1 sebesültszállító gépkocsioszloppal rendelkeztek.²⁹ Az oszlopok szervezetszerüleg 10 db., 4 fekvő vagy 6 ülő sérült befogadásra alkalmas különleges, vagy a szükséges átalakítás elvégzése után 20 db. hatszemélyes személygépkocsiból álltak. Amennyiben személygépkocsikat tettek alkalmassá beteg-, vagy sebesültszállításra, akkor gépjárművenként 2 fekvő, vagy 5 ülő sérült szállító kapacitással számoltak.³⁰ A hadművelleti területen a sérültek hátraszállítása ott okozott nehézségeket, ahol a sebesültszállító oszlopok kapacitása elégtelennek bizonyult, a fogatolt járművekkel való sérült hátraszállítás kétségkívül veszélyeket rejtett magába és sokkal lassabb volt.

Az utánszállítási rendszer vezetése

A hadművelleti területen a „központiasan” szervezett utánszállítási rendszer bevezetése után az jelentette az egyik legnagyobb változást, hogy a hadsereg szállásmestere az alárendeltségébe tartozó hadművelleti egységek anyagi ellátását, lényegében a hadtestparancsnokságok kihagyásával, közvetlenül vezette. A megszervezett utánszállítás keretében a hadsereg saját, de többnyire a Fővezérség által rendelkezésre bocsátott szállítóeszközökkel szállította ki a hadosztályok anyagi szükségletét azok felvételező helyéig.³¹

Az új rendszer bevezetésével megváltozott az anyagi vezető szervek szerepe az utánszállítás és ellátás megszervezésében és irányításában. A Fővezérség anyagi osztályának szerepe az ellátás szempontjából korábban a hadművelleti területen működő seregtestek anyagi ellátásának biztosítására korlátozódott, kapcsolatot képezve a HM-en keresztül a hadiipar és a hadsereg között. A megváltozott rendszerben a Fővezérség szabályozó funkciója növekedett, mert az a hadművellet időtartamára a hadsereg rendelkezésre bocsátotta a szükséges anyagi intézeteket és szállító erőket. A szabályozó funkció főként az első felvonulás során érvényesült, mert a kijelölt hadszíntereknek megfelelően a felvonulási tervekben a megerősítéseket előre meghatározták. A Fővezérség a hadsereg utánszállítási és ellátási rendszerébe közvetlenül általában csak akkor avatkozott be, ha a működési körülmények a szabályzatokban, utasításokban leírtaktól lényegesen eltértek, vagy a hadművelleti helyzet azt megkívánta.³² A hadsereg szállásmesterének, és ezáltal törzskari szervezetének, azaz az I/c. osztálynak a szerepe az utánszállításért és az ellátásért való felelősség megváltozásával párhuzamosan teljes egészében módosult, mert a hadosztályok felé irányuló szállításokat közvetlenül irányították. A hadtestparancsnokságok szerepe az utánszállítás és ellátás lebonyolításának vezetésében másodrangúvá vált, és szinte csak arra korlátozódott, hogy az alárendelt hadművelleti egységek anyagi helyzetét pontosan nyilvántartsa. Az anyagáramlás folyamatába a hadtestparancsnokság operatíván csak akkor avatkozhatott be, ha a kialakult harcászati helyzetnek megfelelően, időközben a hadosztályok részére kiutalt

²⁹ HL. Vkf. Eln. VI/ 1. o. 9.010/hr./1935. Az 1934. évi Emlékirat.

³⁰ Vezérfonal: i.m. (1933) 19. p.

³¹ Hadtörténelmi Levéltár: Vkf. Eln. VI/3. o. 136.994/1933. Az „Írányelvek a felső vezetés számára” című szolgálati könyvhöz kiegészítő utasítás.

³² HL. Vkf. Eln. VI/3. o. 136.994/1933. Az „Írányelvek a felső vezetés számára” című szolgálati könyvhöz kiegészítő utasítás.

anyagmennyiséget célszerűbben újra el kellett osztani.³³ A beavatkozás hatékonyságát megkérdőjelezte, hogy ilyen esetekben a hadtestparancsnokság előzetes jelentési kötelezettséggel tartozott a hadsereg-parancsnokság felé, azaz a hadsereg szállásmester jóváhagyását minden ilyen esetben meg kellett várni.

A kialakított irányítási rendszerben a hadtestparancsnokságnak még a szabályozó funkciója sem maradt meg, annak ellenére, hogy ennek veszélyeire, vagyis az utánpótlásban beálló zavarokra Putz Mátyás a már említett tanulmányában felhívta a figyelmet.³⁴ Az 1933-ban megjelent Vezérfonal kiadásával a „központias” irányítási módszer és a rugalmas utánszállítási rendszer kialakítását azonban nem sikerült maradéktalanul elérni. Ugyanis – hadtestek a már tárgyalt, szinte teljes kikapcsolásával adott esetben a seregvonatoknak olyan távolságot kellett áthidalniuk, amely magát az anyagáramlás folyamatát merevítette meg. Az akkor rendszeresített, főként fogatolt szállítóeszközökkel a mozgóháború törvényei szerint megnövekedett a tér dimenziójának szerepe. A fogatolt kocsioszlopok túlsúlya, amit súlyosbított a hadtest irányító szerepének korlátozása, a mindenkor helyzethez való rugalmas alkalmazkodás lehetőségét is kizárta, annak ellenére, hogy az időtényező szerepét az ellátóoszlop rendszerbe lépésével sikerült lecsökkenteni.

A kialakult merev szállítási láncolaton az 1936 áprilisában életbe lépő „Fr.” hadrend bevezetésével párhuzamosan változtatni kellett. Erre azért volt szükség, mert a megalakult önálló dandárok szállító egységeit csak a napi szükséglet szállítására tették alkalmassá. Az önálló dandárok felé irányuló utánszállítást a hadsereg szállásmestere az új hadrendben képtelen volt vezetni, ezért a Vezérfonalban meghatározott elveket módosítani kellett. A vezérkar főnöke által ezzel kapcsolatban 1937. március 3-án kiadott „Irányelvek” szerint, a megalkotandó szabályzatnak rugalmas ellátási és utánszállítási rendszert kellett kialakítania. A vezérkar főnöke a Vezérfonalban megállapítottakhoz képest az alábbi változásokat szabta meg: a hadműveleti anyagi szolgálat irányítását továbbra is a hadsereg (illetve az önállóan alkalmazott hadtest, vagy hadműveleti egység, H. A.), az utánszállítást a Fővezérség, a hadsereg és a hadtest végezze. Az utánszállítás súlypontját a folyamatosság és a rugalmasság feltételeinek megvalósítása érdekében a hadtestre helyezték át.³⁵

Az 1924-ben kiadott harcászati szabályzat a hadműveleti területen az utánszállítással és az ellátással kapcsolatos előírásai, főként a rejtési szabályok betartása miatt általános elveket tartalmaztak. A konkrét határozványok főként a hadosztályokra vonatkoztak. A hadműveleti anyagi szolgálat végrehajtásával kapcsolatos szabályok nem különböztek el irányítási szintenként a különböző szakutasításokban sem. Főként erre lehetett visszavezetni azt, hogy a hadijátékokon, alkalmazó megbeszéléseken a csapatok szakközegeinek tájékozottsága az elvárt szint alatt maradt. Többek között ennek okán is már 1932-ben felmerült a harcászati szabályzat átdolgozásának gondolata. A vezérkar anyagi osztálya (3. vezérkari osztály) által kidolgozott javaslatában a megoldást abban látta, hogy a szolgálati ágakkal kapcsolatos szabályokat a fegyvernemek feladataitól elkülönítve, függelékként vagy külön füzetben, vezetési szintek szerint kell meghatározni.³⁶

Az új szabályzat kidolgozására csak 1937-38-ban kerülhetett sor. A szerkesztésre kiadott „Irányvonalban” megerősítették a helyi erőforrások kiaknázásának elsődlegességét, amelyből törvényszerűen következett, hogy továbbra is csak olyan anyagok utánszállításával számoltak, amelyekből a hadműveleti területen hiány volt. Az anyagi súlyképzést a hadműveleti siker zálogaként határozták meg, a harc-hadművelet eredményes megvívását olyan helyen látták biztosítottnak, ahol az erőfölény mellé anyagi fölény is párosult. Ebből az következett, hogy a rendelkezésre álló korlátozott szállítókapacitást is koncentrálni kellett, egyben a

33 Uo.

34 Putz Mátyás: i.m. (1933).

35 HL. Vkf. Eln. VI/6. o. 72.112/1938. A H. Sz. III. rész letárgyalása vezetőségi értekezleten.

36 HL. Vkf. Eln. VI/3. o. 136.428/1932. Szabályzatok átdolgozására javaslat.

szállítóegységekkel szemben egyre erősödő elvárássá vált a feladat jellegéhez való rugalmas alkalmazkodás, vagyis a hosszabb előkészületek nélküli készenlét a csapat- és anyagszállításokra egyaránt.³⁷

Az 1938-ban kiadott harcászati szabályzat tervezetben, majd annak 1939-ben életbe léptetett véglegesített változatában az utánszállítás menetét a hadművelleti területen a Vezérfonalban meghatározottak figyelembevételével az 1931-ben javasolt szerkezetben szabták meg.³⁸ Az elosztóállomásról az anyagszállítmányokat a hadsereg szállásmester kiadott rendelkezései alapján, a kezdőállomásra kirendelt vezérkari tiszt által meghatározott sorrendben, lehetőleg vasúton szállították az ellátóoszlopokhoz. Az ellátóoszlopok által telepített felvételező állomásról vagy átrakó állomásról a felvételező helyekig való szállítást a hadtestek, szükség esetén a hadosztályok végezték. A hadművelleti egységek részére kiutalt anyagszállítás ütemét az adott kötelék anyagi vezérkari tisztjének igényei szerint az ellátóoszlop parancsnoka szabályozta a lehetőleg gépkocsival járható út mentén települt felvételező helyig.³⁹

ÖSSZEGZÉS

Az 1920-as évek végére körvonalazódó magyar katonai stratégia hadászati elképzeléseinek megvalósításában a szállító- és ellátó szolgálatra is sok kötelezettséget rótt. Mindez olyan körülmények között, amikor a haderő fejlesztési elképzeléseket rejtve az ország fegyverkezési egyenjogúságának elismeréséig rejtve kellett végrehajtani. A „győri program” meghirdetéséig az anyagi és a pénzügyi források is csak szűkösen álltak rendelkezésre. A fegyverkezési program 1 milliárd pengőt irányzott elő egy ötéves intenzív haderő-fejlesztési program megvalósítására. Ebből a hadsereg fejlesztésére közvetlenül 600 millió pengőt irányozták elő, az ellátó- és szállítószolgálatok korszerűsítésére már nem jutott elegendő forrás.

Az eredeti stratégia elképzelések megvalósításában azonban a honvédség utánpótlási és utánszállítási rendszere igazodott a vezérkari hadászati követelményekhez. Az adott körülmények között sikerült egy rugalmasan működő rendszert kialakítani. Az utánszállítások akadozása a területgyarapítások során két alakalommal okozott súlyos ellátási zavarokat. Az első ilyen esemény sorozat Kárpátalja megszállásakor következett be, ahol a visszacsatolásban résztvevő egységeknél nem volt idő az „Fr.”-t elrendelni. Így a csapatok az előírtnál csapatok kevesebb készletet vittek magukkal, a művelleti területen pedig a helyszíni beszerzés lehetőségei meglehetősen korlátozottak voltak.⁴⁰

Hasonló, a politikai és hadászati vezetés hibáira visszavezethető hibák történtek a Délvidék megszállásakor 1941 áprilisában is, a későn kiadott és rosszul postázott mozgósítás miatt késedelmet szenvedett a magyar királyi 3. hadsereg felvonulása.⁴¹ A mozgósítás késedeleméből származó hiányok olyan mértékben hátrányosan hatottak az utánszállítások megszervezésére, amelyet a hadművelet során már nem lehetett kielégítő módon korrigálni. Nem tartozik szervesen a témához, de a magyar királyi 2. hadsereg 1943 januárjában bekövetkezett pusztulásáért a gyenge felszereltséget, az zord időjárási viszonyokat, valamint az ellátó- és szállító szolgálatok működést tették felelőssé. Igazat kell adnunk azonban Szabó Péter

³⁷ HL. Vkf. Eln. VI/6. o. 72.112/1938. A H. Sz. III. rész letárgyalása vezetőségi értekezleten.

³⁸ A szolgálati ágak működési rendjével az E-1-es Harcászati Szabályzat 1939. III. része foglalkozott. A szabályzat a szolgálati ágak négy csoportját határozta meg, úgymint A: tábori lelkeszi szolgálat, B. ellátó szolgálat: lőszer, tüzérségi anyag és fegyverzet pótlása, egészségügyi-, állategészségügyi- hadbiztossági-, műszaki (híradó) anyag-, anyaggyűjtő és vonatanyagi szolgálat, C: szállítószolgálat, D: Egyéb szolgálat: személyirányító-, tábori posta-, kat tábori posta-, katonai közigazgatási-, tábori rendészeti, egészségügyi rendészeti és kémelhárító-, hadtáp szolgálat és katonai igazságszolgáltatás.

³⁹ E-1-es H. Sz. 1939. III. rész. 46-56 pontok. 20-22.p.

⁴⁰ Horváth Attila: i.m. 1997.

⁴¹ Horváth, Csaba, Lengyel, Ferenc (2003): A Délvidéki hadművelet. 1941. április. Püldo, Budapest. 10-21. o.

hadtörténésznek, aki a témával összefüggő monográfiájában több alkalommal is felhívja arra a figyelmet, hogy milyen következményei lehetnek annak, ha egy hadsereget nem az ellen az ellenség ellen, és nem azon a hadszíntéren alkalmazzák, amelyre felkészítették.⁴²

A cikkben tárgyalt változások és fejlődés azonban világosan rámutatnak a magyar vezérkar gondolkodásmódjának komplexitására. A trianoni békediktátum tiltásai az ország nehéz anyagi helyzete miatt látványos haderőfejlesztés megindítására 1938-ig nem nyílt lehetőség. Az adott keretek között azonban számtalan olyan eredményt értek el, amely tanulságul szolgálhat a mai katonai szakemberek számára is. Ezek közül kiemelném, hogy a logisztikai rendszert hogy lehet megfeleltetni a hadászati követelményeknek, illetve miként lehet támaszkodni a katonai logisztikai szakemberek szaktudására.

Felhasznált irodalom

- [1] Berger, Károly (1930): *A Vezetés Kézikönyve*. I-II. köt. Stádium Sajtóvállalat Részvénytársaság Budapest.
- [2] Dombrády, Lóránd (2000): *Katonapolitika és hadsereg 1920-1944*. Ister Kiadó és Kulturális Szolgáltató Iroda. Budapest, 293 p.
- [3] Dombrády, Lóránd (1993): Magyar katonai stratégiai elképzelések 1927-1938-ig (Tanulmány), Magyarország katonai stratégiája (komplex kutatási téma) Elméleti kutatási terület. Országos Társadalomtudományi Kutatások. Szerkesztette Kovács Jenő. Budapest.
- [4] Dombrády, Lóránd-Tóth, Sándor (1987): *A Magyar Királyi Honvédség 1919-1945*. Zrínyi Katonai Könyv- és Lapkiadó, Budapest.
- [5] -1-es Harcászati Szabályzat I. rész Harcászati Elvek. A Honvédelmi Minisztérium 1924 évi kiadásának 1927. évi utánnyomása, Budapest.
- [6] E-1-es Harcászati Szabályzat. A Honvédelmi Minisztérium kiadása. 1939. I- III. rész.
- [7] Koncz, György (1933): Háborús élelmezés megszervezése a mai közlekedési viszonyok mellett. Magyar Katonai Szemle. 1933. évi. 10. szám. pp. 161-193.p. és 1933. 11. szám. pp. 169-199.
- [8] Horváth, Attila (1997): *A Magyar Királyi Honvédség szállító szolgálatának működési elvei és annak gyakorlati kérdései (1922-1941)*. Kandidátusi értekezés. Budapest, Megőrzési helye: a Nemzeti Közszerológiai Egyetem Könyvtára.
- [9] Horváth, Attila (2002): A hadszíntér előkészítés és a közlekedési ügy összefüggései a két világháború között pp. Hadtudományi Tájékoztató. Budapest, 2002 évi 2. szám 65-86.
- [10] Horváth, Csaba (1993): *A Magyar Királyi Honvédség felderítő rendszerének elvi és gyakorlati kérdései (1924-1942)*. Kandidátusi értekezés. Budapest, Megőrzési helye: a Nemzeti Közszerológiai Egyetem Könyvtára.
- [11] Horváth, Csaba, Lengyel, Ferenc (2003): *A Délvidéki hadművelet*. 1941. április. Püldo Kiadó, Budapest.
- [12] Nagy, Dr. Pusztai, Tóth, Dr. Zimonyi (1984): *A magyar katonai ellátó (hadtáp) szolgálat története*. Zrínyi Katonai Kiadó. Budapest.
- [13] Ordassy, Pál: Fogatolt vonatok teljesítményeit befolyásoló tényezők. Magyar Katonai Szemle. 1934. 5. szám. pp. 178-194.

⁴² Szabó Péter (2001): *Don-kanyar*. Corvina, Budapest.

- [14] Putz, Mátyás: Háborús élelmezés megszervezése a mai közlekedési viszonyok mellett. Közzétette az Magyar Katonai Szemle. 1933. évi. 8. szám pp. 159-173. és 1933. 9. szám 160-187.p.
- [15] Szabó Péter (2001): Don-kanyar. Corvina, Budapest.
- [16] Vezérfonal az anyagi ellátás végrehajtására a csökkentett seregvonatokkal kapcsolatban. Segédlet. A Honvédelmi Minisztérium kiadványa. Budapest. 1933.

Venekei József

venekei.jozsef@uni-nke.hu

NATO LOGISZTIKA ÉS A NATO MŰVELETI TÁMOGATÁSI LÁNC MENEDZSMENT

Absztrakt

A NATO logisztikai rendszere tulajdonképpen nem más, mint a tagországok logisztikai képességeinek az összessége, melyet olyan ügynökségek, tanácsok, testületek és fórumok támogatnak, melyek szövetségi szinten felelősek azoknak a feladatoknak a megtervezéséért, megszervezéséért és végrehajtásáért, melyek nemzeti szinten történő végrehajtása a termelési és a fogyasztói logisztika feladatát képezik. A NATO műveleti támogatási lánc menedzsment koncepciót elsőként egy NATO tervezési konferencia keretében fogalmazták meg 2006-ban annak érdekében, hogy a NATO különböző műveleteinek végrehajtása során nyert tapasztalatai alapján növeljék a logisztikai támogatás hatékonyságát. A koncepció elméleti és gyakorlati alapjai a polgári életben már megteremtődtek, ezeket az alapokat kellett a NATO logisztikai támogatási rendszerébe átültetni. Cikkemben a NATO műveleti támogatási lánc menedzsment koncepció elveinek a gyakorlatban történő megvalósulását mutatom be a brit Összhaderőnemi Ellátási Lánc Koncepció működésén keresztül.

System of NATO Logistics can be described as a complex entirety of Logistic capabilities of the member states, that are supported by the councils, bodies and forums who are responsible for the planning and execution of the tasks done by producer's and consumer logistics on national level. NATO Operational Support Chain Concept was drew up first in 2006 on a NATO planning conference with the aim to put the lessons learned from the previous NATO operations into the practice. raising this way the overall level of effectiveness of logistic support. Theoretical and practical fundaments of the concept has already been created in civilian life so the main task was to put theese fundaments into the NATO logistic support system. In my article I demonstrate the realization of the NATO Operational Support Management Concept in the practice throughout the operation of the British Joint Supply Chain Concept.

Kulcsszavak: NATO logisztika, NATO műveleti támogatási lánc menedzsment, Összhaderőnemi Ellátási Lánc Koncepció ~ NATO Logistics, NATO Operational Support Chain Management, Joint Supply Chain Concept

BEVEZETŐ

A logisztika nem új keletű fogalom, a hadászatban jelent meg. Már az Ókorban is nagy jelentőséget tulajdonítottak a haderők mozgatásának, a felszerelésének és ellátásának. A logisztika fejlődésének feltárása a hadtörténelem egyik olyan területe, amellyel eddig nem foglalkoztak eléggé a szakemberek. A logisztika történetét nem lehet csak az elnevezés alapján vizsgálni abban a korban és abban a hadseregben, amikor ezt az elnevezést használták a haderő szükségletei kielégítésére. A logisztikai szemlélet fokozatosan terjedt el a polgári életben, napjainkra ellátási lánc menedzsment részét képezi.

Az ellátási lánc menedzsment a logisztikánál jóval bonyolultabb, komplexebb, információs rendszerekre épülő tevékenység, amely magába foglalja a gyártást, a marketing tevékenységet, a finanszírozást, az üzleti kapcsolatok menedzselését, és kockázat-megosztást. Az ellátási lánc működtetésének számos módja van, ami hatékonyabbá teszi annak működését, de egységes séma véleményem szerint nem létezik, hiszen a külső és belső információk, gazdasági folyamatok, folyamatosan befolyásolják vagy befolyásolhatják a lánc menedzselését. Azonban kiemelhetünk néhány olyan elemet, amely ma, és feltételezhetően a jövőben is segíteni fogja az ellátási lánc menedzsment fejlődését. Ilyen elemek a láncon belüli hatékony kommunikáció, a vevőorientáció, a fogyasztói kapcsolat menedzsment és a gyors alkalmazkodó képesség, melyek nem tekinthetők az ellátási lánc menedzsment alapvető feltételeinek, de közvetítő és koordináló funkciójuk segítségével interdiszciplináris vagy multidiszciplináris módon, hatékonyan fejtik ki hatásukat.

Az alapvető különbség a civil és műveleti ellátási lánc működtetése között az, hogy míg a civil ellátási láncok működtetésének célja a profitszerzés, addig a műveleti ellátási lánc végpontján nem a vevő áll, hanem a katona, az általa működtetett haditechnika illetve katonai objektum, és célja nem a profitszerzés, hanem minden esetben a művelet sikeres végrehajtása vagy a harc sikeres megvívása. [2] A műveleti ellátási lánc elemeit nem a tulajdonosok, hanem a láncot alkotó logisztikai csomópontok képviselik, melyek meghatározott hierarchikus rendszert alkotnak.

NATO LOGISZTIKA

A hadsereg és a gazdasági élet polgári szereplői közötti kapcsolat hosszú történelmi múltra tekint vissza. Az állandó hadseregek fenntartása, ellátása komolyan igénybe veszi az egyes országok költségvetését és gazdasági erőforrásait, ugyanakkor elmondható, hogy jó lehetőséget biztosít egy sor olyan polgári cégnek, vállalkozásoknak, melyek részt vesznek a hadsereg ellátásában. Ezek a cégek, vállalatok vagy különböző szolgáltatásokat nyújtó vállalkozások akár a műveleti ellátási lánc szereplőivé is válhatnak. A jelenkori gazdasági helyzetben, mikor a védelmi tárcák költségvetése csökkenő tendenciát mutat és a rendelkezésre álló védelmi kiadások korlátozottak, kiemelt fontossággal bír a katonai és a polgári erőforrások hatékony kezelése. Meg kell teremteni a lehetőséget a polgári erőforrások maximális kihasználására, de ugyanakkor megfelelő egyensúlyt kell kialakítani a hadsereg önfenntartó képessége és a civil szférából származó kiegészítő ellátási források között. Ez a fajta harmonikus egyensúly lehetővé teszi a költségkímélő ellátást, a rendelkezésre álló erőforrások optimális felhasználását és megfelelő alapot biztosít a műveleti támogatási lánc hatékony működtetéséhez.

A NATO-ban elfogadott definíció szerint „A logisztika az erők mozgatásának és fenntartásának tervezési és végrehajtási tudománya”, mely a legáltalánosabb értelmezésben a következő katonai műveletek végrehajtásával foglalkozik:

- anyagtervezés- és fejlesztés, beszerzés, raktározás, szállítás, elosztás, fenntartás, karbantartás, eltávolítás és ártalmatlanítás;

- személyszállítás;
- létesítmények beszerzése, működtetése és karbantartása;
- szolgáltatások megrendelése és biztosítása;
- egészségügyi szolgáltatások biztosítása.

Az AAP-6-ban szereplő meghatározás lefedi a NATO szervezete különböző területeinek felelősségi köreit. Mégis van néhány olyan terület, amelynek közelebbi meghatározásához új definíciókat alkalmaztak, mint például a termelői és a fogyasztói vagy felhasználói logisztika.

A termelői (gyártási) logisztika az alapanyag-raktártól - a termelési folyamaton keresztül – a késztermék-raktárig terjedő anyagáramlást tervezi, szervezi, irányítja és ellenőrzi. Az anyag-, és információáramlás végigköveti a termelési folyamat minden fázisát, beleértve az egyes fázisok közötti esetleges közbenső tárolást, várakozást is. A technológiai folyamat és a gyártmányok bonyolultságától függően az anyagáramlás különböző bonyolultságú hálózatot képez. Ennek megfelelően a logisztikának ez az alrendszere foglalkozik a kutatással, tervezéssel, fejlesztéssel, gyártással, a szabványosítás és az interoperabilitás kérdéseivel, a minőségbiztosítással, a pótalkatrészek beszerzésével, a kodifikációval és a haditechnikai eszközök és felszerelések biztonsági szabványaival.

A fogyasztói vagy felhasználói logisztika a logisztika azon alrendszere, amely a késztermék átvételével, raktározásával, szállításával, technikai kiszolgálásával, működtetésével, a hadfelszerelések elosztásával foglalkozik és az integrált logisztikai tevékenység keretében a termelői logisztikával szorosan együttműködve részt vesz a katonai képesség építés és a haderő fenntartása logisztikai tervezési feladataiban. Ebből következik, hogy a fogyasztói vagy más néven felhasználói logisztikához tartozik a készletek ellenőrzése, az anyag- és eszköz ellátás, a mozgatási és szállítási feladatok, a haditechnikai eszközök üzemben tartásához szükséges alkatrészek és fenntartási anyagok beszerzése, a tárolás-raktározás és az üzemeltetéssel, kezeléssel kapcsolatos szakkiképzések végrehajtása.

A logisztikai támogatás integrált rendszerében a bemenő adatokat, tehát a hadsereg igényeit és követelményeit a fogyasztói logisztika szervezeti határozzák meg, a kimenő eredményeket a termelői logisztika szervezeti által végzett hatékony tevékenység biztosítja. Ennek megfelelően a termelési logisztikát felfoghatjuk úgy, hogy az a fogyasztói logisztika oldaláról érkező igények meghatározott fokú és mértékű kielégítője és közvetítője.

A termelői és a fogyasztói logisztika viszonyát tovább vizsgálva megállapítható, hogy a két alrendszer elhatárolása szinte minden NATO tagországban bonyolult feladat. Látható, hogy az egyes fogalmak alatt értendő tevékenységek akár mindkét alrendszer elemei is lehetnek. A NATO logisztikai fogalomrendszerében a logisztikai funkciók teljesülési módja és gyakorlati megvalósulása szerint további két területet különböztet meg, melyeket együttműködői és többnemzeti logisztikának nevez. Az együttműködői logisztika a nemzeti logisztikai képességeknek az összegyűjtését foglalja magába. Olyan két és többoldalú termelési és fogyasztói logisztikai megállapodások összessége, melynek célja a tevékenységek koordinálásának és ésszerűsítésének alkalmazásával a NATO erők logisztikai biztosításának optimalizálása.[3] A fő cél, az erőforrások ésszerű felhasználása a gazdaságosság figyelembevételével a béke-, háborús- és nem háborús katonai tevékenységek logisztikai támogatása hatékonyságának növelése mellett. Az együttműködő logisztikai tevékenységek fejlesztése és működtetése a termelői és fogyasztói logisztikai szervezetek széleskörű együttműködésén keresztül zajlik. A többnemzeti logisztika alatt azokat a nem tisztán nemzeti jellegű logisztikai támogatási tevékenységeket értjük, mint például a többnemzetiségű integrált logisztikai támogatás, a szerepkörre szakosodott támogatás és a vezető nemzeti logisztikai támogatás. [4]

A NATO logisztikai rendszere tulajdonképpen nem más, mint a tagországok logisztikai képességeinek az összessége, melyet olyan ügynökségek, tanácsok, testületek és fórumok támogatnak, melyek szövetségi szinten felelősek azoknak a feladatoknak a megtervezéséért,

megszervezéséért és végrehajtásáért, melyek nemzeti szinten történő végrehajtása a termelési és a fogyasztói logisztika feladatát képezik.

A NATO-logisztika elvei az MC 319/2 dokumentumban kerültek meghatározásra, mely a NATO logisztikával foglalkozó dokumentumainak rendszerében a legmagasabb szintet foglalja el. Ez a dokumentum a NATO-logisztika elveit a következőkben határozza meg:

1. *Felelősség:* A nemzeti és a NATO hatóságok kollektív felelősséggel viseltetnek a NATO nemzetközi tevékenységeinek logisztikai biztosításáért;
2. *Ellátás:* A nemzeteknek egyedileg, vagy együttműködési egyezményekkel biztosítaniuk kell béke, válság és háború esetén a NATO rendelkezésére bocsátott erők logisztikai erőforrásokkal történő ellátását;
3. *Együttműködés:* A nemzetek és a NATO hatóságok között létfontosságú az együttműködés;
4. *Jogkör:* A megfelelő szintű NATO-parancsnokoknak az erők fenntartásához és azoknak a leghatékonyabb módon való alkalmazásához elegendő jogkört kell biztosítani a logisztikai erőforrások felett;
5. *Elégségesség:* A szinteknek és a logisztikai erőforrások szétosztásának elegendőeknek kell lenniük a béke, válság és háborús helyzetben a szükséges katonai képesség biztosítására előírt készenléti szintek, az alkalmazási képesség és a mozgékonyság elérésére;
6. *Gazdálkodás:* A logisztikai erőforrásokat hatásosan, hatékonyan és gazdaságosan kell felhasználni;
7. *Rugalmasság:* A harcoló alakulatok szervezetszerű vagy kijelölt logisztikai biztosításának, a harcoló alakulatokhoz hasonlóan dinamikusnak, rugalmasnak, mozgékornak és alkalmazkodó képesnek kell lennie;
8. *Áttekinthetőség:* A NATO-erők hatékony vezetéséhez és a kiszolgálásuk koordinálásához létfontosságú a logisztikai eszközökről a nemzetek által hozzáférhetővé tett információ.[5]

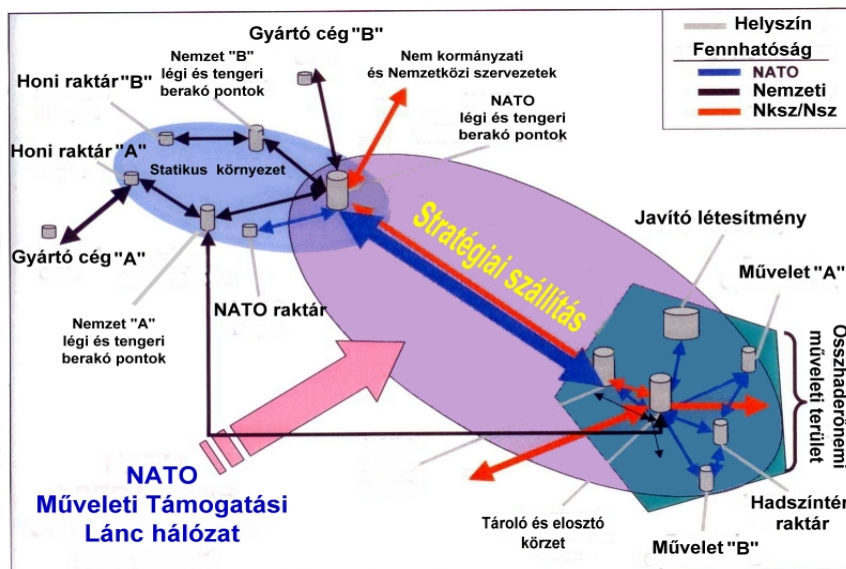
NATO MŰVELETI TÁMOGATÁSI LÁNC MENEDZSMENT

A NATO műveleti támogatási lánc menedzsment koncepciót elsőként egy NATO tervezési konferencia keretében fogalmazták meg 2006-ban annak érdekében, hogy a NATO különböző műveleteinek végrehajtása során nyert tapasztalatai alapján növeljék a logisztikai támogatás hatékonyságát. A koncepció elméleti és gyakorlati alapjai a polgári életben már megteremtődtek, ezeket az alapokat kellett a NATO logisztikai támogatási rendszerébe átültetni.

A NATO korábbi műveleteit független és sok esetben koordinálatlan nemzeti logisztikai támogatási rendszer alkalmazásával látta el, ami maga után vonta a pénzügyi, felszerelési és emberi erőforrások nem hatékony felhasználását, a felhasználók és a műveleti parancsnokok sok esetben nem tették átláthatóvá és korlátozták az ellátási erőforrások elérhetőségét, ami a készletek indokolatlan felhalmozódásához vezetett. Ezek a tapasztalatok, illetve a NATO Reagáló Erők hadrendbe állítása és fejlesztése vezetett a NATO logisztikai felfogásának jelentős átdolgozásához és a műveleti támogatási lánc menedzsment kialakulásához. Az erők gyors felvonultatásának szükségessége, a befogadó nemzeti támogatás gyakori hiánya megköveteli a támogatási lánc folyamatos fejlesztését és hatékony alkalmazását a műveleti területen. A hatékony alkalmazás záloga ugyanúgy, ahogy a civil ellátási láncok esetében egy kifinomult és széleskörűen alkalmazott információs rendszertámogatás és a teljes ellátási

forrás láthatósága (TAV),¹ ami lehetőséget biztosít a műveletet irányító parancsnoknak az ellátásban jelentkező hiányok kezelésére és az ellátási források újraelosztására. Emiatt a LOGFAS rendszer jövőbeni folyamatos fejlesztése a műveleti támogatási lánc működtetése szempontjából elengedhetetlen.[6]

A NATO műveleti támogatási lánc általános leírását a 8. számú ábra mutatja.



1. ábra. A NATO műveleti támogatási lánc

(Forrás: NATO ACT 1st Draft, 5 April 2006. 8. p. Fordította: A szerző)

Az ábra főbb jellemzői a következők:

1. A nemzetek a honi területről az összhaderőnemi hadműveleti területre (JOA),² érkezésükig, illetve az összhaderőnemi hadműveleti területen belül használhatják mind a saját-, mind pedig a NATO műveleti támogatási láncot a személyi állomány-, a felszerelés- és az egyes anyagosztályok vonatkozásában;
2. A felszereléseket gyártó cégek (OEM)³ a szükséges cikket letárolhatják honi területen lévő raktári létesítményekben, a nemzeti berakó pontokon (POE),⁴ vagy közvetlenül a NATO tengeri és légi berakópontjain létrehozott tároló létesítményekben (Mounting Base);
3. A nem kormányzati (NGO)⁵ és más nemzetközi szervezetek (IO)⁶ által a NATO rendelkezésére bocsátott erőforrásokat a NATO műveleti támogatási lánc használhatja, de ezek fölött a nem kormányzati és nemzetközi szervezetek rendelkeznek;
4. A szükséges cikkek, anyagok és felszerelések stratégiai szállítással kerülnek a NATO hadműveleti területen elhelyezkedő tengeri- és légi kirakópontjaira, ahonnan a műveleti területen elhelyezett elosztó körzetekbe kerülnek. Innen igény szerint kerülnek a műveletben résztvevő felhasználókhoz, javító bázisokhoz;
5. A NATO műveleti támogatási lánc elemeit a tengeri- és légi be- és kirakó pontok, a hadműveleti területen elhelyezett elosztó pontok, a végfelhasználók-, vagyis a műveletekben résztvevő kontingensek és azok tároló- és javító létesítményei alkotják.

¹ Total Asset Visibility

² Joint Operational Area

³ Original Equipment Manufacturer

⁴ Point of Embarkation (Air-, Sea and Rail)

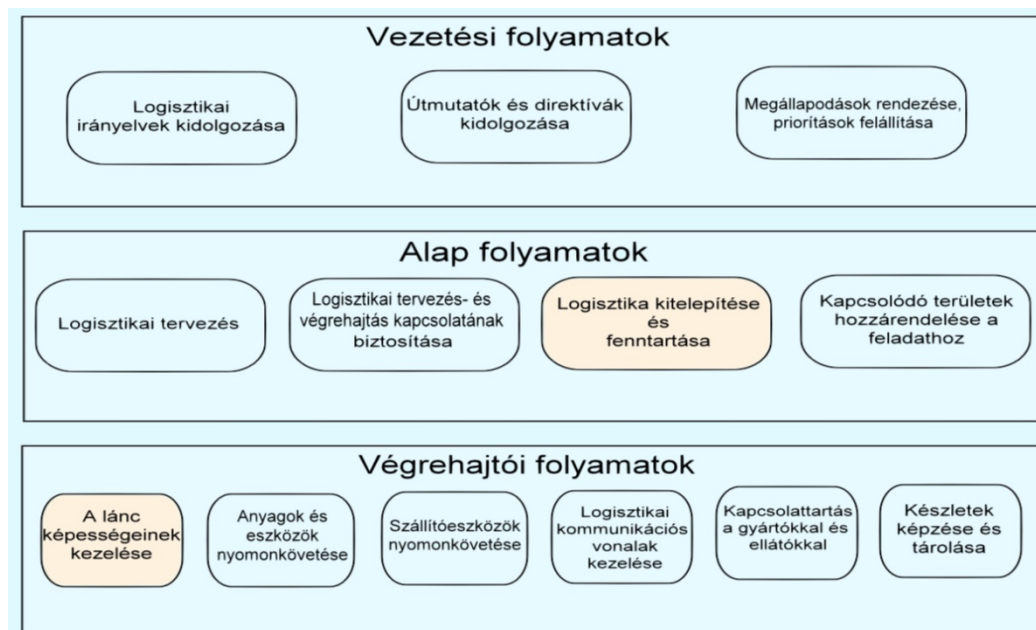
⁵ Non Governmental Organization

⁶ International Organization

A NATO műveleti támogatási lánc alapelvei szoros összhangban vannak az MC 319/2 dokumentumban lefektetett NATO logisztikai elvekkel és a következőkben foglalhatóak össze:

1. A műveleti támogatási láncon belül az információknak láthatónak kell lenniük a műveletben résztvevők számára;
2. A műveleti támogatási lánc legyen összetett és rugalmas a lehetséges műveletek spektrumán keresztül;
3. A műveleti támogatási láncot a műveleti és taktikai felhasználók követelményei alapján vezetik;
4. A műveleti támogatási láncot a hadművelet összes fázisában következetesen használni fogják;
5. A műveleti támogatási lánc lefed minden biztosítási területet, beleértve a műszaki-, egészségügyi- és a civil szolgáltatói ellátási támogatást;
6. A műveleti támogatási lánc nem irányít és ír elő nemzeti rendszereket vagy folyamatokat;
7. A forrásokat és lehetőségeket a NAMSA⁷ biztosítja, és ott használják fel, ahol ez lehetséges és fontos;
8. A műveleti támogatási lánc elég rugalmas, hogy összeegyeztesse a „tőlem” és a „neked” logisztikát, ha szükséges;
9. A műveleti területen a non-profit és profitorientált logisztikai tevékenység egyaránt jelen van;
10. Többnemzetiségű logisztikai szervezeteket ott alkalmaznak, ahol annak előnye előre látható;
11. A műveletek végrehajtása során az egyes nemzetek biztosítják az ellátási forrásaik feletti teljes átláthatóságot, lehetőséget biztosítva a műveleteket irányító parancsnokoknak a rendelkezésre álló erőforrások optimális elosztására.
12. Minden résztvevő nemzet a műveleti támogatási láncba veti bizalmát és megbízik a más nemzetek által működtetett ellátási láncokban.

A műveleti támogatási láncon belüli logisztikai folyamatokat a 2. számú ábra szemlélteti.



2. ábra. A NATO műveleti támogatási lánc logisztikai folyamatai
(Forrás: OLCM Deployment and Sustainment BPM Draft 28. p. Fordította: A szerző)

⁷ NATO Maintenance and Supply Agency, NATO Fenntartó és Ellátó Ügynökség

A NATO műveleti támogatási lánc logisztikai folyamatain belül a következő jellemzőket emelem ki:

Vezetési folyamatok

- A vezetési folyamatokon belül kiemelt fontossággal bír a logisztikai irányelvek pontos megfogalmazása. A NATO-n belül ennek alapidokumentuma az MC 319/2 dokumentum, ami meghatározza a logisztikai támogatás kollektív felelősségi elveit a NATO-n belül és a műveletekben résztvevő egyes nemzetek között. A NATO logisztikai irányelvei a legfelsőbb szinten kerülnek kidolgozásra. A NATO bizottságok, mint például a Logisztikai Bizottság (LC)⁸ felterjeszti ajánlásait a Katonai Bizottságnak (MC)⁹ és az Észak Atlanti Tanácsnak (NAC),¹⁰ melyeket mindkét szervezet jóváhagy;
- A NATO Stratégiai Parancsnokságai a jóváhagyott irányelvek alapján kidolgozzák a logisztikai tervezéshez szükséges direktívákat és tervezési útmutatókat, amelyeket a Stratégiai Parancsnokság intézkedéseiben és a STANAG-ekben¹¹ tesznek közzé;
- Stratégiai és hadműveleti szinten a logisztikai koordináció a J4 törzsek¹² feladatát képezi. A NATO logisztikai törzseivel szemben támasztott alapvető követelmény, hogy minden lehetséges helyzetet figyelembe véve megfelelő és garantált támogatást nyújtson a hadműveleti tervek elkészítéséhez és jelenlétével biztosítsa a kitelepített parancsnokságokon a logisztika vezetését.

Alap folyamatok

- A NATO-nak és a hozzájáruló nemzeteknek békében-, válság- és konfliktus idején egyaránt biztosítaniuk kell a logisztikai erőforrásokat a NATO erők számára. Ennek megfelelően a logisztikai tervezés célja, hogy a szükséges személyi állomány-, felszerelés- és az egyéb anyagok megfelelő időben és mennyiségben rendelkezésre álljanak;
- Az információ áramlás a művelet tervezési és végrehajtási fázisában kétirányú. A végrehajtási fázis valós eseményei eltérhetnek a tervezési fázis során meglévő logisztikai helyzettől, ezért a valós információkat a végrehajtás sikere érdekében az újratervezés során fel kell használni;
- A logisztika a műveletek minden részére hatást gyakorol. Ahhoz, hogy a műveletben résztvevő erők sikeresen hajtsák végre küldetésüket, a logisztikai támogatás minden formáját alkalmazni kell. Ennek megfelelően a logisztikához kapcsolódó külső területeket (CIMIC, Befogadó Nemzeti Támogatás, Egészségügyi támogatás, Pénzügyi támogatás) hozzá kell rendelni a logisztikai feladatok végrehajtásához.

Végrehajtói folyamatok

- A NATO műveleti támogatási láncnak biztosítania kell a műveletek végrehajtása szempontjából kritikusnak minősülő logisztikai erőforrások teljes láthatóságát;
- Az anyagi- és szállító eszközök nyomon követése a honi bázisoktól a hadszíntérig hozzájárul a logisztikai erőforrások láthatóságának fenntartásához (AAP-51A¹³);
- A műveletekben résztvevő erők folyamatos kapcsolatot tartanak fenn a gyártó- és ellátó szervezetekkel az ellátás folyamatos biztosítása érdekében;

⁸ Logistics Committee

⁹ Military Committee

¹⁰ North Atlantic Council

¹¹ Standardisation Agreement

¹² Összhaderőnemi Logisztikai Törzs

¹³ NATO Asset Tracking to be Business Model , NATO Standardization Agreement, 21.01.2010

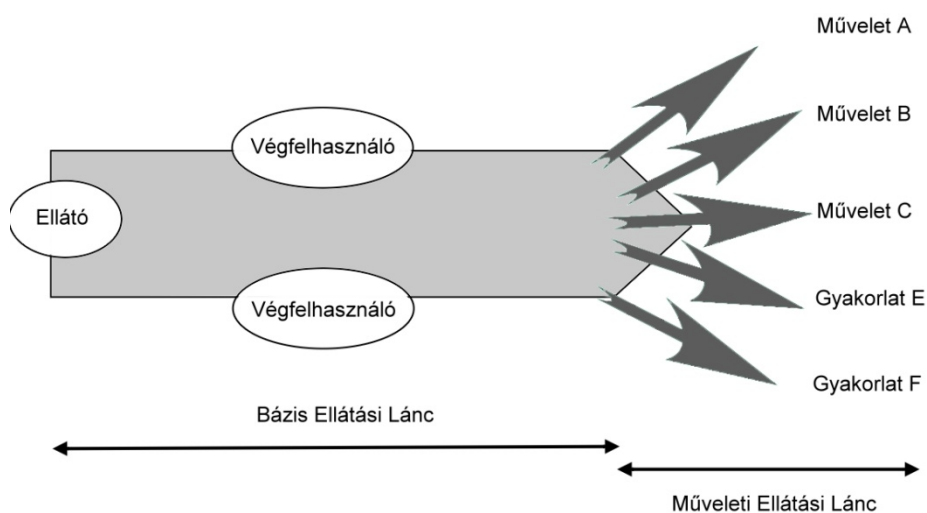
- A készletek képzése és tárolása magába foglalja a művelet végrehajtásához szükséges készletek megalakítását, tárolását, szinten tartását és leltározását.

ÖSSZHADERŐNEMI ELLÁTÁSI LÁNC KONCEPCIÓ [7]

Néhány NATO tagállam már átültette a NATO műveleti támogatási lánc menedzsment koncepcióban megfogalmazott elveket a gyakorlatba. Ebben a folyamatban Nagy Britannia kiemelkedő szerepet töltött be. Az általuk alkalmazott Összhaderőnemi Ellátási Lánc modell bizonyította hatékonyságát az elmúlt időszakban végrehajtott- és a jelenleg is folyó koalíciós műveletek során.

Az Összhaderőnemi Ellátási Lánc tulajdonképpen a védelmi szféra által ellenőrzött anyag- és eszköz fogadó-, tároló-, elosztó- és továbbító csomópontok hálózata, mely biztosítja a gyors, valósidejű információk, szolgáltatások és az anyagi készletek áramlását a honi bázisok és a végfelhasználók között a műveleti képesség kialakítása, fenntartása érdekében.

Az Összhaderőnemi Ellátási Lánc működése szempontjából több szintet különböztet meg és különböző tervezési időskála alapján működik. Az úgynevezett alap- vagy bázis ellátási lánc azokat az Összhaderőnemi Ellátási Lánc tevékenységeket foglalja magába, melyek célja nem egy meghatározott katonai művelet támogatása, hanem a csapatok általános ellátására használt erőforrások kezelésére irányulnak, továbbá azoknak az infrastrukturális elemeknek és erőforrásoknak a biztosítási feladatait látja el, melyek a katonai művelet végrehajtása során nem kerülnek kitelepítésre a műveleti területre, de a műveleti ellátási lánc szempontjából meghatározó jelentőségűek. Ezek az erőforrások általában a honi bázison találhatók. A műveleti ellátási lánc tevékenysége az adott műveletben résztvevő erők támogatására irányul. A hosszú távú ellátási lánc-tervezés a szükséges tőke ráfordítás, erőforrás tervezés szempontjából 20 éves időtartamra tekint előre. Ez a folyamat az Összhaderőnemi Ellátási Lánc legmagasabb szintje, mely a stratégiai szintű logisztikai és védelmi tervezési feladatokat foglalja magába.



3. ábra. Hosszútávú ellátási lánc tervezés

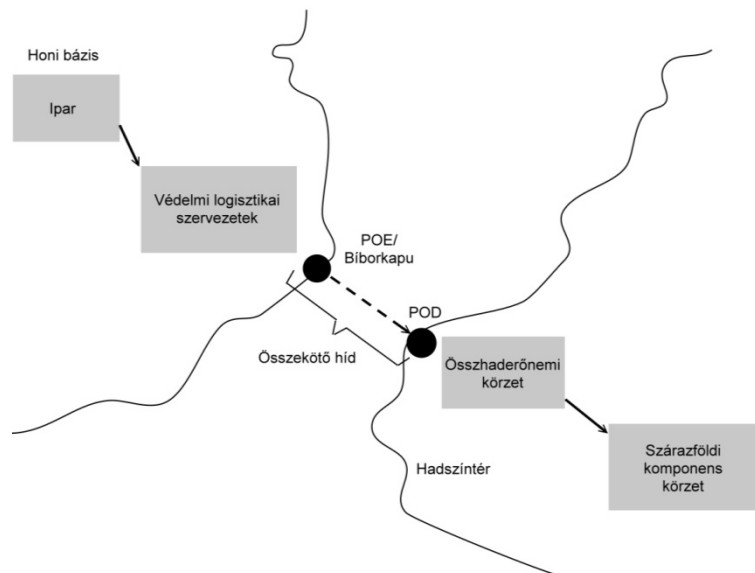
(Forrás: Royal Logistic Corps Operational Handbook, Army Code 71845, Issue 1.0 2007, p. 3-3. Fordította: A szerző)

A műveleti ellátási lánc a frontvonalai parancsnokságok (FLCs)¹⁴ és a honi területen működő ipari létesítmények, illetve a Védelmi Minisztérium és annak különböző szervezetei között működik, és kialakítása során fontos követelmény, hogy zökkenőmentesen integrálja

¹⁴ Front Line Commands

magába a külső és az úgynevezett függő támogatási lehetőségeket,¹⁵ biztosítsa a közvetlen anyagszállítás lehetőségét az ipari partnerek által a frontvonalai parancsnokságokhoz, számoljon egy hatékony inverz logisztika működtetésével, működése során legyen hatékony és erősítse a műveletekben résztvevő személyi állománynak az ellátási lánc megbízhatóságába vetett hitét.

Az ellátási láncot úgy tervezik és építik fel, hogy az megfeleljen az adott katonai művelet sajátosságainak és alapvetően a művelet fenntartási fázisára koncentrál, melyet a helyszínrre telepített logisztikai csapatok (RLC)¹⁶ hajtanak végre.



4. ábra. Az Összhaderőnemi Ellátási Lánc strukturális felépítése (Forrás: Royal Logistic Corps Operational Handbook, Army Code 71845, Issue 1.0 2007, p. 3-11. Fordította: A szerző)

Az ábra azokat a kulcsfontosságú érintkező felületeket mutatja be, melyek minden anyagosztály biztosítási feladataira hatással vannak a honi területen elhelyezkedő ipari létesítményektől a hadszíntérig bezárólag. A készletek biztosítása nem minden esetben a honi bázison elhelyezkedő ipari létesítményekből történik. Egyes esetekben a műveleti területhez közelebb eső, illetve közvetlenül az ott elhelyezkedő forrásból szerződés alapján kerül biztosításra. Erre jó példa az üzemanyag, amely leggyakrabban a befogadó nemzet által, szerződés alapján kerül kiszállításra.

A továbbiakban fontosnak ítélem bemutatni azokat a kulcsfolyamatokat, amelyek az Összhaderőnemi Ellátási Lánc működtetése során meghatározó jelentőséggel bírnak.

A műveletben résztvevő kontingens ellátása a feladatra biztosított készletek, illetve a kontingens által igényelt szükségletek alapján történik. Az első esetben a készletek a nélkül kerülnek kiutalásra illetve kiszállításra az adott kontingenshez, hogy az formálisan leigényelné azt. Ezeket a készleteket a műveleti parancsnokok határozzák meg és a műveleti területen jelenlévő logisztikai csapatok alakítják meg, tárolják és adják ki. A szükséglet alapján történő ellátás az ellátásnak egy általánosabb forrása, melynek során a kontingens készleteinek a pótlása a második lépcsőben elhelyezkedő logisztikai szervezethez benyújtott igénylés alapján történik. A logisztikai szervezet az általános elsőbbségi kód (SPC)¹⁷ és a

¹⁵ Magukba foglalják a Befogadó Nemzeti Támogatás, a szerződéseken alapuló logisztikai támogatás, az állami hivatalok, a nem állami szervezetek és a koalíciós erők által nyújtott támogatást.

¹⁶ Royal Logistic Corps

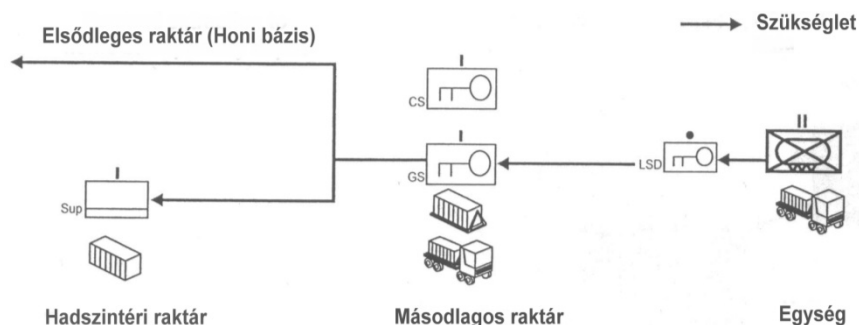
¹⁷ Standard Priority Code

kiszállítási határidő (RDD)¹⁸ figyelembevételével végzi a hiányzó készletek pótlását. Az ellátási lánc nyolc elsőbbségi kódot különböztet meg, melyek közül négyet békeidőszakban, négyet pedig a műveletek végrehajtása során alkalmaznak. A műveletek végrehajtása során az 1-es kóddal ellátott szükséglet (SPC 1) kielégítése azonnali prioritást élvez a felmerülő költségek teljes figyelmen kívül hagyásával. Ilyen esetben a RAF¹⁹ gépein kívül polgári repülőgépek is végezhetik a kiszállítást a műveleti területre és egyéb ügynökségek, szervezetek is igénybe vehetők az anyagoknak a honi raktárakból, légi kirakó pontokról való összegyűjtésére és kiszállítására. Egyéb esetekben a készletek pótlása a kiszállítási határidő figyelembevétel a leggazdaságosabb módon történik.

A műveleti területen tevékenykedő minden egység mellé egy RLC alegység van rendelve, melynek feladata az adott egység szükségleteinek feldolgozása és biztosítása. Az RLC alegység úgy van kialakítva, hogy képes legyen a készletlépcsőzési előírásoknak megfelelően a készletek letárolására az úgynevezett másodlagos raktárban. Mikor az egységtől beérkezik az igénylés, az RLC alegység megállapítja, hogy rendelkezik-e a szükséges anyagokkal és eszközökkel. Amennyiben azok nem állnak rendelkezésre a saját raktárában, továbbítja az adott igénylést a hadszíntéren jelenlévő, más egység érdekében tevékenykedő másodlagos raktárakhoz. Ha azok sem képesek a szükséges anyagi eszközöket rendelkezésre bocsátani, továbbítja az igényt a hadszíntéri raktárhoz vagy azon keresztül tovább a honi bázison elhelyezkedő raktárhoz. A hadszíntéren elhelyezkedő másodlagos raktárak közötti szoros együttműködés jelentősen növeli az ellátási lánc hatékonyságát, a gazdaságos felhasználást, csökkenti a szállítási feladatokat a honi bázis és a hadszíntér között és végső soron megakadályozza az anyagok és eszközök indokolatlan felhalmozását.

A műveleti területen működő RLC logisztikai dandár szervezetszerű alegységei, köztük a támogató ezred a harmadik lépcsőben helyezkedik el és feladata a hadszíntéri tartalékok tárolása és kezelése a hadszíntéri raktárban. A logisztikai csapatok jelenlegi struktúrája nem teszi lehetővé az összes anyagosztályból megalakított készletek tárolását a harmadik lépcsőben. Amennyiben a szükséglet nem elégíthető ki a hadszíntéri raktárban tárolt készletekből, továbbításra kerül a honi bázison elhelyezkedő Védelmi Logisztikai Szervezethez (DLO)²⁰.

Összefoglalva az ellátási lánc kulcsfolyamatait megállapítható, hogy az ellátás a feladatra biztosított készletek biztosításával (Push) illetve az igényelt szükségletek biztosításával (Pull) történik. Szükséges azonban megjegyezni, hogy a műveletek kezdeti fázisában (kitelepülés), illetve a magas intenzitású műveletek végrehajtása során a harctevékenységekhez szükséges készletek (CSups)²¹ biztosítása a „Push” – elvnek megfelelően történik.



5. ábra. A szükséglet alapján történő ellátás

(Forrás: Royal Logistic Corps Operational Handbook, Army Code 71845, Issue 1.0 2007, p. 3-12. Fordította: A szerző)

¹⁸ Required Delivery Date

¹⁹ Royal Air Force

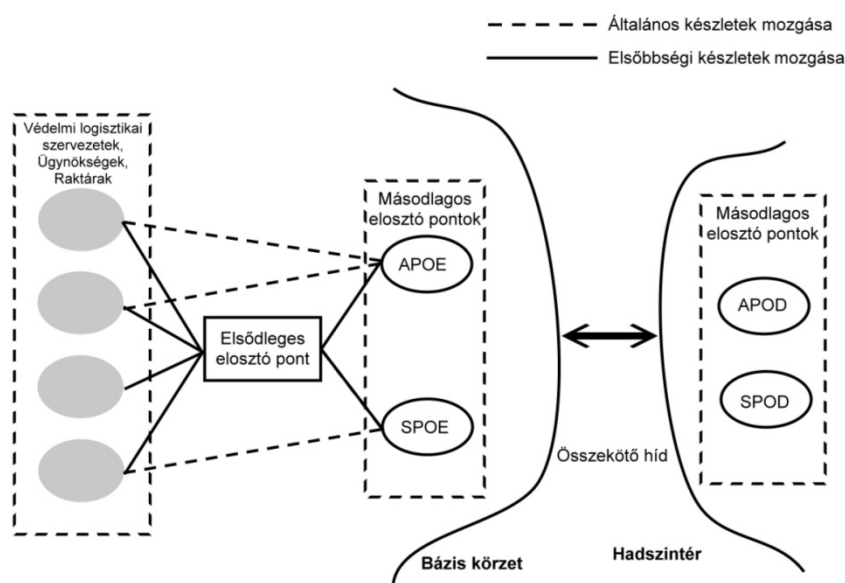
²⁰ Defence Logistic Organisation

²¹ Combat Supplies

Irányítás tekintetében az Összhaderőnemi körzetben települő Összhaderőnemi Logisztikai Komponens (JFLogC)²² az Összhaderőnemi Műveleti Főnöknek (CJO)²³ van alárendelve és fő feladata a szárazföldi-, haditengerészeti- és a légierő komponensek logisztikai biztosításának koordinálása, irányítja a tengeri- és légi kirakó pontokon tevékenykedő logisztikai szervezetek munkáját. Bár a szárazföldi komponens körzetben²⁴ tevékenykedő logisztikai dandár nem tartozik a közvetlen alárendeltségébe, a művelet különböző fázisaiban átcsoportosíthatja a rendelkezésre álló logisztikai erőforrásokat a logisztikai támogatás hatékonyságának növelése érdekében. A logisztikai dandár felel a Szárazföldi komponens körzetében tevékenykedő csapatok közvetlen logisztikai támogatásáért a művelet fenntartási fázisában és a Szárazföldi komponens parancsnokának (LCC)²⁵ van közvetlenül alárendelve.

Az Összhaderőnemi Ellátási Lánc strukturális felépítésében²⁶ kiemelt szerepet tölt be az úgynevezett „Bíbor kapu” és az „Összekötő híd”. Ezeket nem szükséges minden esetben valós fizikai körzeteknek tekinteni, inkább úgy tekintenek rájuk, mint azokra a folyamatokra, melyek segítségével a készletek, a felszerelés és a személyi állomány eljut a honi bázisokról a hadszíntérre.

A „Bíbor kapu” egy olyan, a védelmi logisztikai szervezetek által irányított folyamat, mely szabályozza anyagok belépését, és azok mindkét irányban történő áramlását az Összhaderőnemi Ellátási Láncban belül. Ezeknek a folyamatoknak a teljes felügyelete egy kifinomult, minden haderőnemi logisztikai támogatási feladatait magába foglaló informatikai rendszer működtetését teszi szükségessé. Tény, hogy a műveletek fenntartásához szükséges készletek már akkor beérkeznek a hadszíntérre, mikor még tart a művelet kitelepítési fázisa. A „Bíbor kapu” pontosan meghatározza, hogy a kimenő készletek a művelet fenntartási fázisához vagy kitelepítéshez szükségesek. A „Bíbor kapu” feladatait az elsődleges és a másodlagos „Bíbor kapu” elosztó pontok működtetésével valósítja meg.



6. ábra. Elsődleges és másodlagos „Bíbor Kapu” elosztó pontok (Forrás: Royal Logistic Corps Operational Handbook, Army Code 71845, Issue 1.0 2007, p. 3-17. Fordította: A szerző)

²² Joint Force Logistic Component

²³ Chief of Joint Operations

²⁴ Lásd 4. sz. ábra

²⁵ Land Component Commander

²⁶ Lásd 4. sz. ábra

Az anyagok csomagolása és előkészítése a védelmi logisztikai szervezetek és ügynökségek raktáraiban történik, ahonnan átkerülnek az elsődleges elosztó pontra, a Bicesterben található Védelmi Elosztási és Raktározási Központba (DSDC)²⁷. Az elsődleges elosztó ponton az anyagokat előkészítik a szállítmánykövető informatikai rendszerbe történő belépéshez és az elsőbbségi kód, illetve a szállítókapa-
citás függvényében továbbítják a megfelelő tengeri és légi berakó pontokra vagy tovább tárolják. A tengeri és légi berakó pontok körzetében található másodlagos elosztó ponton (honi bázis) az elsőbbségi kóddal rendelkező anyagokat nem tárolják, a szállítmánykövető logisztikai informatikai rendszeren történő átvezetés után átszállítják a hadszíntérre. A hadszíntéri másodlagos elosztó ponton az anyagok újraregisztrálásra kerülnek a szállítmánykövető rendszerben és az adott elsőbbségi kód alapján továbbszállítják az igénylőhöz. A hadszíntéri elosztó pont tevékenységét az Összhaderőnemi Logisztikai Komponens Parancsnoksága (JFLogC HQ) felügyeli és ellenőrzi.

Az SPC 1 elsőbbségi kóddal ellátott készletek a Védelmi Logisztikai Szervezetek raktáraiból az elsődleges elosztó pont kihagyásával is beérkezhetnek berakó pontokra. Ebben az esetben a készletekkel kapcsolatos minden olyan művelet, melyet az elsődleges elosztó pont hajtott végre, a honi bázison található másodlagos elosztó pontra hárul. Mindkét esetben a „Bíbor kapu” műveletek a készletek láthatóságára helyezik a hangsúlyt.

Az „Összekötő híd” folyamat segítségével valósul meg az anyagok és a műveletben résztvevő egységek fizikai értelemben vett átszállítása a berakó pontokról a hadszíntérre. A végrehajtás nem tisztán logisztikai feladat, abban a szárazföldi-, haditengerészeti- és a légierő komponens kijelölt csapatai és szervezetei is részt vehetnek. Erre jó példa, mikor a szállítmány olyan hajózási útvonalon halad, amely nem biztonságos. Ebben az esetben a haditengerészeti komponens kijelölt kötelékei fogják ellátni az erők védelmét.

ÖSSZEGZÉS

A katonai támogatási lánc elméleti és gyakorlati alapjai a polgári szférában az ellátási láncok kialakulásával már megteremtődtek, a problémát az jelentette, hogy miként lehet a civil ellátási láncok alapfogalmait, elveit átültetni a NATO logisztikai rendszerébe. Ezeket a fogalmakat és elveket illetve a gyakorlati alkalmazásra vonatkozó tapasztalait a NATO önálló tanulmányokban tette közzé „Supply Chain Management developments in NATO Nations” és „Recommendations for a NATO Support Chain Management Concept” címekkel.

Sok NATO tagállam már megpróbálta a gyakorlatba is átültetni a NATO műveleti támogatási lánc koncepcióban megfogalmazott elveket. Ezek közül az országok közül a Nagy Britannia által alkalmazott Összhaderőnemi Ellátási Lánc modell már bebizonyította hatékonyságát a korábban- és jelenleg is folyó NATO műveletek során.

Felhasznált irodalom

- [1] Horváth Attila - Vélemény Szabó Mihály „Új sztár tudomány a «logisztika»” című cikkéhez. Nemzetvédelmi Egyetemi Közlemények, 3. évf. 2. szám. 2000, 262-272 o.
- [2] Báthy Sándor: A katonai logisztikai új kihívásai. Hadmérnök. Budapest, 2006. 7 p.
URL cím: <http://hadmernok.hu/kulonszamok/logisztika/bathy.pdf>
- [3] NATO Logisztikai Kézikönyv
- [4] Gáspár Tibor – A TERVEZÉSTŐL A MŰVELETEKIG A katonai logisztika, ZMNE kiadvány, Budapest 2008

²⁷ Defence Storage and Distribution Centre

- [5] MC 319/2 NATO Logisztika alap- és irányelvek, határozati dokumentum
- [6] Baranyai Virgil – A NATO műveleti támogatási lánc koncepció megvalósulása napjainkban, Katonai Logisztika, 15. évf. 3. szám, 2007, 78-107 o.
- [7] Royal Logistic Corps Operational Handbook, Army Code 71845, Issue 1.0, 2007

VII. Évfolyam 4. szám - 2012. december

Balogh Péter

balogh.peter@knbsz.hu

A MAGYAR HONVÉDSÉG ISTAR (ISR) KÉPESSÉGEI, A FEJLESZTÉS LEHETSÉGES IRÁNYAI, KÜLÖNÖS TEKINTETTEL AZ ELEKTRONIKAI HADVISELÉSRE

Absztrakt

Kétség nélkül állítható, hogy minden katonai tevékenység alapja a megfelelő felderítés. Megbízható és pontos adatok, információk nélkül biztos kudarccal jár. A Magyar Honvédség is törekszik modern, a jelenkor kihívásainak megfelelő felderítő szervezetek kialakítására. Az ISTAR (ISR) képesség megteremtése minden jövőt érintő haderő fejlesztési dokumentumban szerepel. Ebben az írásomban javaslatokat fogalmazok meg lehetséges változat kialakítására, különös tekintettel az elektronikai hadviselési képességekre.

There is no doubt that the basis of every military action is intelligence. Without reliable and accurate data and pieces of information there is no success at all. The Hungarian Defence Forces have been struggling to set up modern intelligence structures to meet future challenges. The concept of ISTAR (ISR) capabilities can be found every pieces of document dealing with military developments. In this paper I would like to draw a possible version to create an organisation focusing on Electronic Warfare solutions.

Kulcsszavak: ISTAR (ISR), Magyar Honvédség, Elektronikai Hadviselés, ~ ISTAR (ISR), Hungarian Defence Forces, Electronic Warfare.

BEVEZETÉS

A hadviselés változásai folyamatosak és ez a közhelyszerű megállapítás minden, a hadtudományban résztvevőt arra ösztönöz, hogy nézeteit, álláspontját a kor követelményeinek megfelelően felülvizsgálja és új tudományos válaszokat keressen.

A rendszerváltást követően a Magyar Honvédség erői számos átalakításon mentek keresztül. A „reformok” által megcélzott korszerűsítések, a szervezetek racionalizálása és a párhuzamosságok megszüntetése jól csengő szlogenjeiből jórészt a létszámcsökkentés és szervezeti kultúrák leépítése szintig mindig eljutottunk. A következő lépések az építkezés, a képességteremtés, a bővítés kérdéseiben már nem voltunk ennyire sikeresek és ennek okai csak részben pénzügyi természetűek. Megváltozott a haderő feladatrendszere is, az ország védelemtől a missziós tevékenység felé tolódott a hangsúly. A Magyar Honvédség erői több kontinensen, számos békeműveleti misszióban vesznek részt, melyben a nemzeti felderítő képesség birtoklása létszükségletté vált, különösen a balkáni és afganisztáni hadszíntéren, ahol nagyobb létszámú kontingensünk állomásozik. Meggyőződésem, hogy ez a tevékenység létfontosságú volt a Magyar Honvédség erői, eszközei korszerűsítésében, e nélkül még a jelenlegi színvonalat sem értük volna el. Nem is beszélve a nélkülözhetetlen harci tapasztalatokról, amelyet katonáink szereztek különböző beosztásokban tevékenykedve.

Minden progresszió és a nemzetközi példák ellenére ez a folyamat korántsem sikertörténet még. Valamennyi katonai tevékenység a felderítéssel kezdődik és ezen a területen is sok a tennivalónk. Az általánosan megfogalmazott hírszerző, felderítő alkalmazási elvek mellett még nincsenek olyan széles körben elfogadott elvi és műszaki ajánlások, amellyel elérhető volna, hogy a hírszerzésben-felderítésben feladatot végrehajtók tevékenysége harcászati, hadműveleti, hadászati szinten is az összadatforrású felderítés és a fúziós adatfeldolgozás felé mutassanak. A felderítő erőknél, valamennyi INT-nek¹ egymást kiegészítő, támogató megoldásokat kell találniuk. Itt elsősorban nem csak a state-of-the-art² technológiák alkalmazására gondolok, hanem a meglévő erőforrásaink, képességeink legteljesebb ismeretére, a nemzeti és a szövetségi képességek integrálására a célok elérése érdekében. Korábban a „hagyományos” felderítő szakmai kultúrák képviselői nem láttak túl az általuk üzött tevékenység korlátaiban, így nem voltak befogadóak a többi, szintén a felderítésben tevékenykedő munkája iránt. Emiatt korlátozottan voltak képesek rendszerben gondolkodni. Ez érezhetően, jól felfoghatóan változik. Véleményem szerint ez egyértelműen annak köszönhető, hogy számos tiszt és altiszt kollégánk kapott lehetőséget arra, hogy ismereteit hazai és külföldi katonai intézményekben, modern tananyagok elsajátításával bővítse. A feladatot végrehajtó katonai kötelék parancsnoka, régebben nem tapasztalt természetességgel igényli a SIGINT³ és IMINT⁴ támogatást is, holott erre korábban csak a HUMINT⁵ erővel számolt. Több fiatal tisztünk tollából születtek tanulmányok a Magyar Honvédség különleges műveleti és ISTAR⁶ képessége megteremtése témakörében. Ehhez a munkához kívánok hozzájárulni SIGINT szakemberként néhány gondolattal.

Munkámban felmérem az ISTAR képesség nemzeti megteremtésének körülményeit, a vonatkozó szövetségi és fellelhető hazai dokumentációk alapján. Megvizsgálom a korábban e területen dolgozók javaslatait és megosztom saját tapasztalataimat, amelyet az Elektronikai hadviselésben (továbbiakban EHV) és a rádióelektronikai felderítésben szereztem az elmúlt

¹ INT- Intelligence: felderítés-hírszerzés.

² state-of-the-art: legkorszerűbb (technika).

³ SIGINT- Signals Intelligence – A magyar terminológiában jelenleg rádióelektronikai felderítést jelent, de a definíció korszerűsítése az elektronikai területen bekövetkezett változások miatt hamarosan szükséges.

⁴ IMINT- Imaginery Intelligence- képi felderítés.

⁵ HUMINT –Human Intelligence- emberi erőforrással végrehajtott felderítés.

⁶ ISTAR- Intelligence, Surveillance, Target Aquisition and Reconnaissance.

majdnem két évtizedben. Ezek ismeretében értékelem a Magyar Honvédség ISTAR képességének megteremtésére készített tervezeteket, saját javaslatokkal kiegészítve.

AZ ISTAR KÉPESSÉG

Az ISTAR egy mozaik szó, amely néhány éve jelent meg a hadtudományi terminológiában és hamarosan nagy teret nyert a magyar katonai gondolkodásban is.

„Intelligence: Idegen nemzetekre, ellenségre, a potenciális ellenséges erőkre és elemeire, vagy a potenciális műveleti területre vonatkozó információ feldolgozásának eredménye. Az információ feldolgozó tevékenységre és a végrehajtókra is használatos ez a kifejezés. (A gyűjtött információ feldolgozása, tájékoztatás és az abban érintett állomány és eszközök.)

Surveillance: A légtér, a felszín, a felszín alatti területek, helyek, személyek és dolgok rendszeres, vagy folyamatos megfigyelése különböző – vizuális, akusztikus, elektronikus – eszközökkel. (Az információ gyűjtés folyamata, a gyűjtő eszközök és állomány.)

Target Acquisition⁷: A célpont (célobjektum) felismerése, azonosítása, és helyének pontos meghatározása, olyan részletességgel, hogy lehetőség nyíljon a fegyverek leghatékonyabb alkalmazására. (Egy bizonyos célról – lehet ez egy terület, egy szervezet, személy, objektum, stb.- minden nemű információ gyűjtése, annak érdekében, hogy ellene a legmegfelelőbb fegyver, a legmegfelelőbb módon kerüljön alkalmazásra.)

Reconnaissance: Információ gyűjtése az ellenség, a potenciális ellenség tevékenységéről, erőforrásairól, illetve egy meghatározott területre vonatkozó meteorológiai, vízrajzi és földrajzi jellemzőiről vizuális, vagy egyéb felismerési módszerekkel. (Egyfajta információgyűjtés, és a gyűjtő szervezet.) Valójában az ISTAR-t használjuk egy képesség (ami több alképességből tevődik össze) és szervezet megnevezésére is. Arra a szervezetre, amely rendelkezik e képességgel (képességekkel).”⁸

AZ ISTAR KÉPESSÉG MEGTEREMTÉSÉT SZABÁLYOZÓ DOKUMENTUMOK

Az AJP 2.1 NATO felderítő doktrínája⁹ leírja, hogy a felderítést a nemzeti felelősség kategóriájába sorolja. Tehát a tagállamoknak önállóan kell gondoskodniuk a felderítő tevékenység megtervezéséről, megszervezéséről, végrehajtásáról. Nemzeti felelősség a szervezetek felállítása erői-eszközeinek biztosítása és a tevékenységet szabályozó dokumentumok elkészítése.

⁷ Target Acquisition: célmegjelölés (esetleg célkijelölés). Egyelőre nem létezik hivatalosan elismert fordítása az angol terminológiában gyakran emlegetett kifejezésnek. Tartalmában a Target Acquisition: a célok érzékelése, azonosítása és pozíciójuk meghatározása olyan részletességgel, amely eredményeképpen ellenük halálos, vagy nem halálos ellentevékenységi formák alkalmazhatók. (saját meghatározás)

Egy másik meghatározás alapján: *Target Acquisition*: A felderítő és megfigyelő eszközök alkalmazásával új célok és létező célokban történő jelentős változások detektálása, helyzetük meghatározása, azonosítása, elemzése, valamint csapás utáni értékelése. Az elemzések eredményeinek (sebezhetőség) összegzése adatbázisban (target folder), melyek iránymutatást adnak az esetleges ellenük való tevékenység (felderítés, INFOOPS, EW, PSYOPS, csapás) eredményes végrehajtásához; Dr Horváth Zoltán mk. ezredes: Az összhaderőnemi műveletek ISTAR támogatása, Seregszemle különszám, 2012. június, 88. oldal

⁸ Dr. Horváth Zoltán mk. ezredes (a cikk megírásakor még alezredes): Egy lépés az ISTAR képességek fele – új felderítő eszköz a Magyar Honvédségben, VIII. évfolyam, 2. szám, 2010. április-június 49. o. Internet: http://www.hungariandefence.com/container/files/attachments/28301/s_sz_2010_2.pdf letöltve: 2012.10.12). Az AAP-06 NATO Glossary of Terms and Definitions (English and French) 2012 (2) kiadásában meglehetősen általános, leegyszerűsített magyarázatok vannak, így a meghivatkozott cikk jobban adja vissza az ISTAR tartalmiságát.

⁹ AJP 2.1 (Allied Joint Publications) 1. fejezet, IX. rész, 114. pont.

A nemzeti szabályozásban az ISTAR képesség kialakítása először a NATO lisszaboni csúcstalálkozóval közel egy időben került elfogadásra és a „*Miniszeri Irányelvek a védelmi tervezéshez (2012-2021)*” címmel, melyet a honvédelmi miniszter adott ki. A dokumentumban megfogalmazott irányelvek a fegyveres erő fejlesztésével és képességekialakításával kapcsolatos követelményeket fogalmazza meg.¹⁰ Ebben a dokumentumban hangsúlyos helyen szerepel a Magyar Honvédség felderítőrendszerének fejlesztése és az ISTAR képesség kialakítása.

Az AJP-2.7¹¹ NATO dokumentum a következőképpen határozza meg az ISTAR eljárás lényegét:

„Az ISTAR egy olyan eljárás, mely összekapcsolja (integrálja) a megfigyelő, a felderítő és a célokról adatot szerző (célfelderítő) rendszereket valamint érzékelőket a műveletek és a csapásmérő eszközök irányítása érdekében. Magában foglalja az információgyűjtést, a műveleti és felderítő információk menedzsmentjét, helyzetjelentést, illetve helyzetértékelést biztosít a parancsnok és törzse részére a hadműveletek vezetése és a célmegjelölő eljárások támogatása érdekében. A műveleti felderítő tevékenység integrálja és szinkronizálja a tervezést, a felderítő eszközök és érzékelők alkalmazását, az információ feldolgozását és felhasználását, valamint a célmegjelölő és tájékoztató rendszereket közvetlenül támogatva a folyamatban lévő és jövőbeli műveleteket.”¹²

A hazai szabályozás alapvető pillére az új Nemzeti Katonai Stratégia, amely már jelenlegi tervezetében is tartalmaz az ISTAR képességgel is összefüggő feladatokat, így az abban foglaltak útmutatóként szolgálnak a tervezett lépéseink megtételéhez.

„A Magyar Honvédség alkalmazására jellemzően válságkezelő műveletekben kerül sor, sok esetben Magyarországtól jelentős távolságra, szélsőséges természeti és éghajlati viszonyok között, nehezen megközelíthető terepen, ahol csupán korlátozott mértékben vagy egyáltalán nem áll rendelkezésre befogadó nemzeti támogatás. A válságok kezelése során a *hálózatalapú hadviselés, a hírszerzés és a felderítés*, a precíziós fegyverek és modern technikai eszközök, a civil-katonai együttműködés, a pszichológiai hadviselés, valamint a különleges rendeltetésű erők széles körű alkalmazása szükséges. A válságkezelésre általában olyan, az alapfeladatát ellátni képtelen, gyenge államokban kerül sor, ahol irreguláris, félkatonai szervezetekkel, felkelőkkel, fegyveres csoportokkal, nemzetközi zsoldos és terrorista csoportokkal szemben kell a biztonságot megteremteni és fenntartani.”¹³

A Magyar Honvédség Összhaderőnemi Doktrínája 3. változatának (kiadásra tervezett 2012. 08. 29. verzió) megközelítése alapján.

Az összhaderőnemi műveletek végrehajtása megköveteli a műveletek végrehajtásához szükséges képességek meghatározását. Egy összhaderőnemi művelet végrehajtásához a következő főbb területek igényelnek kiemelt figyelmet, amelyek nemzetközi környezetben hangsúlyosan jelentkeznek:

- hírszerzés, felderítés és megfigyelés;

¹⁰ Honvédelmi Minisztérium Védelempolitikai és Védelemtervezési Helyettes Államtitkár. nyt sz.: 503-34/2010 számú dokumentum. Honvédelmi Minisztérium 1-9. oldalak.

¹¹ AJP 2.7 -Allied Joint Doctrine for Reconnaissance and Surveillance dated 7 July 2009

¹² Gulyás Attila: A nemzeti különleges műveleti erők felderítő támogatása, Hadmérnök VII. évfolyam 3. szám 2012. szeptember, 135-136 o.

¹³ Magyarország Nemzeti Katonai Stratégiája (tervezet) 41. pont, megtalálható Internet: http://www.kormany.hu/download/d/ac/a0000/Nemzeti%20Katonai%20Strat%C3%A9gia_tervezet.pdf, letöltve 2012.11.04.

- légtér feletti ellenőrzés kívánt szintjének elérése és megtartása;
- manőver és tűz összehangolása;
- elektromágneses spektrumban fölény kialakítása;
- irányítás és vezetés;
- információs műveletek;
- stratégiai kommunikáció;
- logisztikai támogató rendszer felépítése, fenntarthatóság;
- erők megóvása;
- civil-katonai együttműködés (CIMIC).

Ezek tehát azok az alapidokumentumok, amelyek alapján a HVK J2 Felderítő Csoportfőnökség (és jogelőd szervezetei) megtervezte a Magyar Honvédség ISTAR képességének megteremtését.

A kiadásra tervezett új összhaderőnemi doktrína az új kihívások tükrében újraértékeli a kiemelt figyelmet igénylő területeket beleértve az AJP 2.7 NATO dokumentumban fajsúlyosként jelentkező ISTAR lényegi elemeit.

Az ÖHD tervezet fenti felsorolása felöleli valamennyi ISTAR területet, kiegészítve az információs műveletek, a stratégiai kommunikáció, a logisztikai támogató rendszer, az erők megóvása és a CIMIC tevékenységekkel. Mindezt áthatja a hatásalapú műveletekre való felkészülés gondolata.

„A hatásalapú műveletekben a korábbi felfogáshoz képest komolyan figyelembe veszik azt a láncreakcióhoz hasonló elvet, miszerint a kezdeti közvetlen hatással – első csapással – törvényszerűen további közvetett károsító, korlátozó hatásokat lehet elérni, amely a teljes rendszerre különböző mértékű negatív hatást fejt ki. Az előidézett hatások eredőjének, vagyis az összhatás eredményének elemzése és értékelése képezi a hatásalapú műveletek lényegét. Ez az új műveleti felfogás a holisztikus elvű szemlélet alkalmazását igényli.”¹⁴

Elgondolkodtató a CIMIC felértékelődése az ÖHD tervezetében. Valamennyi információs művelettel, információs hadviseléssel foglalkozó dokumentum foglalkozik e területtel.

A NATO információs műveletek doktrínájának V. fejezete (Képességek, eszközök és technikák, amelyek az információs műveleteket támogatják) az alábbi tartalmi felsorolást adja:¹⁵

- pszichológiai műveletek (PSYOPS);
- hadműveleti biztonság (OPSEC);
- információ biztonság (INFOSEC);
- megtévesztés (Deception);
- elektronikai hadviselés (Electronic Warfare);
- fizikai pusztítás (Physical Destruction);
- kulcsfontosságú vezetőkkel történő tevékenységek (Key Leader Engagement);
- számítógép hálózati műveletek (CNO);
- polgári-katonai kapcsolatok (CIMIC).

Az AJP 3.10 NATO dokumentum és az ÖHD tervezetében leírtak összehasonlításából kitűnik, hogy a CIMIC szinte „túlnőve” az információs műveletek kategóriát, önálló életre kel. Az ÖHD tervezete (tévesen) megnevezi az információs műveleteket és a CIMIC-et, mint attól független, önálló fogalmat.

¹⁴ Dr Haig Zsolt mk. ezredes „Haig Zsolt, Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, 2005, ISBN 963 327 391 9, 176 o.

¹⁵ AJP 3.10 Allied Joint Doctrine for Information Operations (2009), Internet: <http://info.publicintelligence.net/NATO-IO.pdf>, letöltve 2012.10.10.

A jelenlegi és a korábbi doktrínákban megfogalmazottak szerint az információs műveletek végcélja az információs fölény elérése. Ennek fontos, de nem kizárólagos összetevője a CIMIC és az elmúlt években kissé túlhangsúlyoztuk a többi fontos elem kárára. A Magyar Honvédség Civil-katonai Együttműködési és Lélektani Műveleti Központ (CKELMK) felelős a CIMIC és PSYOPS tevékenységért és felvállalta a Magyar Honvédség Információs műveletek doktrínájának kidolgozását 2014-ig. 2012-ben megszületett Összhaderőnemi Parancsnoksági kiadványa, az INFOOPS Parancsnoki útmutató, amely tartalmaz minden lényegi elemet az alkotó részek egymásra épüléséről, feladatairól, kölcsönhatásairól stb.

A Magyar Honvédségben jelenleg két INFO OPS beosztás van. Az ÖHP Parancsnok 2012. évi írásos feladatszabása alapján az INFOOPS feladatokat még 2012-ben integrálni kellett az MH CKELMK feladatrendszerébe.¹⁶

Véleményem szerint ez a NATO szabályzatok teljes figyelmen kívül hagyása és további tévedéseket generál majd. Fontos megérteni, hogy az INFOOPS **nem egyenlő** a CIMIC-kel.

Szükségszerű, hogy a többi alkotó elem egymásra épülő hatásait erősítő módon érhük el a végcéljainkat, valamint a szemben álló fél ilyen jellegű tevékenységeinek hatását a lehető legnagyobb módon csökkentsük.

Figyelemreméltó, hogy az ÖHD tervezete fontossági sorrendjében számol a hírszerzés, felderítés és megfigyelés kiemelt prioritásával, a tevékenységben résztvevő szervezetek technikai eszközeinek fejlesztésével.

Ennek fontos megvalósítási lehetősége a NATO ajánlások figyelembevételével történő ISTAR képesség megteremtése.

A fent leírt definíciók, ajánlások alapján szükséges, hogy egy korszerű fegyveres erő rendelkezzen ilyen képességgel. A legtöbb NATO tagország már kialakította, vagy a rendelkezésre álló anyagi eszközei figyelembevételével folyamatosan teremti meg ISTAR képességeit. Ez alól a Magyar Honvédség sem kivétel.

Egy változat szerint a Magyar Honvédség 5/24 „Bornemissza Gergely” felderítő zászlóalj bázisán, annak átalakításával kerülne felállításra az ISTAR zászlóalj.

AZ MH 5/24 „BORNEMISSZA GERGELY” FELDERÍTŐ ZÁSZLÓALJ JELENLEGI FELÉPÍTÉSE ÉS KÉPESSÉGEI

A zászlóalj, amely néhány éve került átdiszlokálásra Egerből Debrecenbe, az átcsoportosítás során elvesztette kiképzett állományának közel 50%-át és a technikai eszközei vonatkozásaiban (különösen az elektronikai hadviselési eszközök) a 60-as, 70-es évtizedek technikai színvonalát képviselik.¹⁷

Az elmúlt évek alatt az állomány létszáma elérte az elvárható szintet és ami még fontosabb, kiképzettségében, összekovácsoltságában rengeteget fejlődött. Számos missziós tevékenységben, vagy hazai és külföldi gyakorlatokon fejlesztették tudásukat.

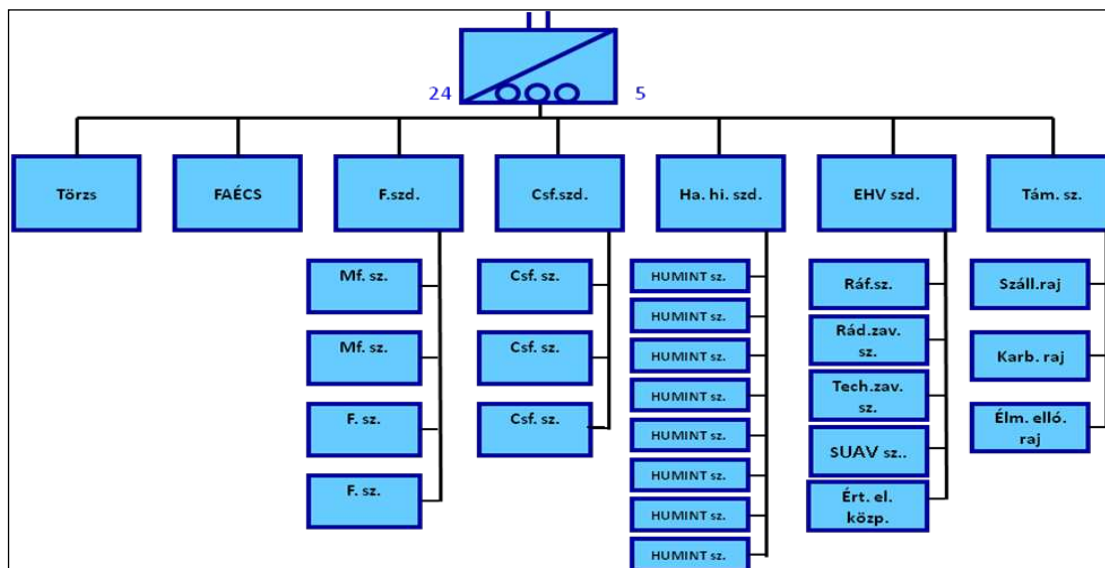
A zászlóalj jelenlegi szervezete:

- zászlóalj parancsnokság,
- felderítő-adatértékelő csoport,
- csapatfelderítő század,
- felderítő század,
- harcászati hírszerző század,

¹⁶ Szilágyi Csaba ezredes: Információs műveletek (INFOOPS), Seregszemle különszám, 2012. június, 131. oldal

¹⁷ Forrás: Felderítők Társasága 2012. 12. 04. ülés, Kovács József altábornagy tájékoztatója.

- elektronikai hadviselés század,
- támogató szakasz
felépítéssel hajtja végre feladatait.



1. ábra: Az MH 5/24 „Bornemissza Gergely” felderítő zászlóalj jelenlegi szervezete¹⁸

A szaktechnikai eszközök vonatkozásában komoly elmaradás mutatkozik. Az elektronikai hadviselés század - különösen annak rádiófelderítő eszközei - teljesen, vagy részlegesen elavultak, így alkalmazásuk erősen korlátozott és gyakorlatilag csak hagyományos, analóg adatforrások felderítésére képesek.

A jelenleg rendszeresített zavaróeszközök is csak egy speciális feladatra alkalmasak (rádióvezérelt, házi készítésű improvizált robbanóeszközök ellen) és semmiképpen sem elegendők az elvárható, teljes spektrumú elektronikai ellentevékenységhöz.

Az R-1378 rövidhullámú rádiófelderítő (továbbiakban: RH) állomás (FLÓRA), a PRIZMA RH felderítő és zavarórendszer utolsó, még rendszerben tartott eleme. Alkalmas az RH (1,5-30 MHz) frekvenciatartományban üzemelő hagyományos rádióforgalmazások harcászati, hadműveleti-harcászati mélységben történő felfedésére, lehallgatására, illetve az információ rögzítésére táviró és távbeszélő üzemmódban. A négy felfedő-lehallgató és az egy parancsnoki munkahely képes 4-6 elsőrendű, 8-12 másod-harmadrendű, periodikusan üzemelő rádióforgalmi rendszer figyelésére, lehallgatására.

¹⁸ Forrás: a szerző. Az ábrában szereplő rövidítések; FAÉCS: Felderítő és Adatértékelő Csoport, F.szd: felderítő század, Mf.sz: mélységi felderítő szakasz, F.sz: felderítő szakasz, Csf.szd.: csapatfelderítő század, Ha.hi.szd.:harcászati hírszerző század, HUMINT cs. : HUMINT csoport, EHV szd.: elektronikai hadviselés század, Ráf sz.:rádiófelderítő szakasz, Rád. zav. sz.: rádiózavaró szakasz, Tech. zav. sz.: technikai zavaró szakasz, SUAV sz.: harcászati pilótanélküli felderítő szakasz, Ért. el. közp: értékelő elemző központ, Tám sz. támogató szakasz.



1. kép: Az R-1378 állomás telepítve és belső kialakítása.¹⁹

Az URH/F RÁF állomás egy Zil-131 alvázra, KF-1 konténerre felépített ultrarövidhullámú felderítő állomás, mely alkalmas a 20-100 MHz (VHF) frekvenciatartományban üzemelő hagyományos szárazföldi URH rádióforgalmazások felfedésére, lehallgatására, illetve távbeszélő üzemmódban az információ rögzítésére harcászati (30-40 km) mélységben. A négy munkahely alkalmas 4-6 elsőrendű, 8-12 másod-harmadrendű, periodikusan üzemelő rádióforgalmi rendszer felfedésére, lehallgatására, információ rögzítésére.



2. kép: Az URH RÁF állomás (szárazföldi) telepítve és belső kialakítása.²⁰

Az URH/L RÁF állomás egy Zil-131 alvázra, KF-1 konténerre felépített ultrarövidhullámú felderítő állomás, mely alkalmas a 100-500 MHz (VHF-UHF) frekvenciatartományban üzemelő hagyományos, főként légiirányító URH rádióforgalmazások felfedésére, lehallgatására, illetve távbeszélő üzemmódban az információ rögzítésére harcászati (40-60 km) mélységben. A három munkahely alkalmas 3-5 elsőrendű, 6-9 másod-harmadrendű, periodikusan üzemelő rádióforgalmi rendszer felfedésére, lehallgatására, információ rögzítésére.

A század felderítő képessége gyakorlatilag ennyiben ki is merül. Jelentős hiányossággként jelentkezik az eszközök korlátozott száma, az eszközök méretei, korszerűtlensége (csak analóg adatforrások felderítésére alkalmas). Legsúlyosabb kifogásként említhető a rádiótechnikai felderítő eszközök,²¹ valamint az iránymérő-, helymeghatározó képesség teljes

¹⁹ Forrás: a szerző felvételei.

²⁰ Forrás: a szerző felvételei.

²¹ A rádiótechnikai felderítő (ELINT) tevékenységgel a szembenálló fél fegyverirányítási rendszereiben működtetett célobjektumok, mint pl. a földfelszíni-, vagy repülőfedélzeti felderítő és tűzvezető radarok, légvédelmi, vagy rakéta csapatok felderítő eszközei stb. észlelhetők. Korábban a század állományában RPSZ-5 (RPSZ-6) típusjelű, GAZ-66 alvázra épített rádiótechnikai felderítő eszközök voltak rendszeresítve. (jelenleg még hadrendben vannak, de üzemképtelenül központi telephelyen állnak, felújításuk hosszabb távon sem várható)

hiánya. A korszerűsítés elmaradása miatt az alegység csak rendkívül korlátozott rádiófelderítő képességgel rendelkezik



3. kép: Az URH RÁF állomás (légi) telepítve és belső kialakítása.²²

Az elektrooptikai felderítő eszközök tekintetében az 5/24 felderítő zászlóalj, elektronikai hadviselés százada valamivel jobban áll az izraeli Skylark I LE SUAV-ok beszerzése kapcsán. Az eszközök az ISTAR ajánlás LAME²³ kategóriájába tartoznak és eredményesen vizsgáztak az afganisztáni hadszíntéren, ahol a PRT²⁴ felderítő biztosításában kerültek alkalmazásra. A rendszer hiányossága, hogy csak a látható és éjszakai fény tartományban képes tevékenykedni, amely az IMINT tevékenység végrehajtásához szükséges, azonban SIGINT függészménye nincs.

A Magyar Honvédség az elmúlt években néhány, az L3 cég által gyártott egyéni és kollektív rádió zavaróeszközt²⁵ szerzett be, melyek programozhatóak és alkalmasak az Afganisztánban gyakorta használt RCIED²⁶-k indítóeszközeinek (rádióberendezés, GSM, CDMA telefonok) zavarására. Ezek csak elégséges képességek, hiszen e speciális eszközök (egyetlen célra rendszeresített) csak korlátozott frekvenciasávban és teljesítménnyel és természetesen hatótávolsággal használhatók. Az elektronikai ellentevékenységekben szereplő zavarás terminológia tartalma, ennél tágabb értelmű kategória.

Tehát látható, hogy a jelenlegi szervezetben meglévő technikai eszközök csak részben elégítik ki az ISTAR ajánlásokat.

A csapatfelderítő alegységek számára szükséges a BTR modernizációs programban megfogalmazott képességeknek megfelelő eszközök beszerzése, valamint a modern lövészfegyverek biztosítása.

A mélységi felderítő alegységek részére jelenleg nem állnak rendelkezésre megfelelő könnyű páncélozott szállító eszközök, az egyéni éjjellátó berendezések és lézer célmegjelölő eszközök, valamint a könnyű és nehézbúvár felszerelések vonatkozásban is elmaradásban vagyunk. Nem szabad természetesen megfedkezni a nagy hatótávolságú, titkosított adatátviteli eszközökről, és a szükséges túlélő felszerelésekről sem.

²² Forrás: a szerző felvételei.

²³ LAME -Low Altitude Medium Endurance: kismagasságú, közepes hatótávolságú.

²⁴ PRT- Provincial Reconstruction Team: tartományi újjáépítő csoport.

²⁵ A TMP 0512 (URH), TMP 0512/EB (GSM) zavaró berendezések katonai hátizsákban kerültek málházásra, míg a WBS 2500 eszközök MB G250, illetve BTR-80-ba kerültek beépítésre.

²⁶ RCIED- Radio Controlled Improvised Explosive Device: rádióvezérlésű házilagosan előállított robbanóeszköz.

A MAGYAR ISTAR KÉPESSÉG MEGVALÓSÍTÁSA

A Magyar Honvédség 2005 óta foglalkozik mélyebb szinten a NATO ISTAR²⁷ követelményeknek történő megfeleléssel és az ehhez szükséges képesség kialakításával, amely az alábbi összetevőket-elemeket foglalja magába:

- C2,²⁸ később C4I²⁹ képesség a felderítő elemek irányítására, minősített adattovábbításra;
- műveleti értékelő-elemző képesség, amely képes közel valós idejű értékelt adatok szolgáltatására a saját és a szövetséges megerősítő csapatok számára;
- csapatfelderítő képesség;
- mélységi felderítő képesség, amely földi, légi és vízi úton is kijuttatható erőket foglal magában;
- harcászati hírszerző (HUMINT) képesség;
- földi mozgócél-felderítő képesség;
- földi és légi EHV támogató képesség;
- távirányított rögtönzött robbanóeszközök elleni védelem (RC-IED);
- SIGINT képesség amely COMINT, ELINT és értékelő képességgel rendelkezik;
- IMINT képességen belül MALE³⁰ UAV³¹ alegység és harcászati UAV szakasz (LAME team);
- célfelderítő képesség (ez az elem a tüzér alegységeknél jelenik meg).

A Honvédelmi Minisztérium Haderőtervezési Főosztály, Haderőtervezési és Modernizációs Osztálya által 2007 novemberében ismertetett elképzelés alapján a lövészdandár felderítő támogatása érdekében az alábbi **ISTAR zászlóalj** szervezettel számolt.

- zászlóalj parancsnokság;
- törzstámogató szakasz;
- HUMINT század;
- 1-2 felderítő század;
- elektronikai hadviselés század;
- felderítő támogató század;
- logisztikai alegységek.

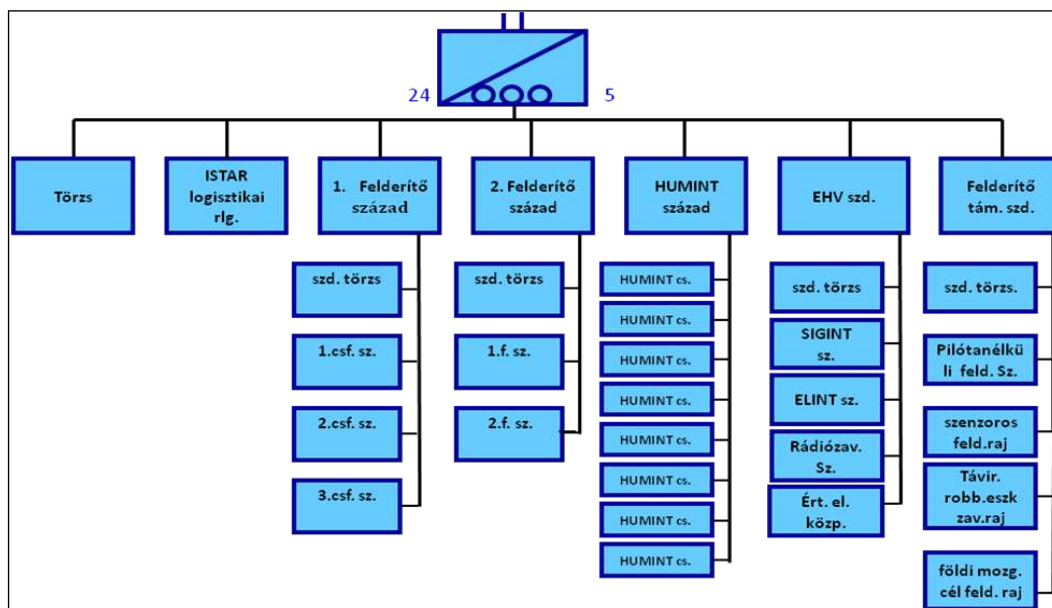
²⁷ EL 0583 – NATO 2006 force proposals for Hungary 2006 – 2016.

²⁸ C2 -Command and Control: vezetés és irányítás.

²⁹ C4I -Command Control Communication Computer and Intelligence: vezetés, irányítás, híradás, informatika és felderítés.

³⁰ MALE -Medium Altitude Long Endurance: közepes magasságú, nagy hatótávolságú.

³¹ UAV –Unmanned Aerial Vehicle: pilótánélküli repülőeszköz.



2. ábra. Az ISTAR zászlóalj szervezete (egy változatban)

Az elképzelés alapján a HUMINT század nyolc HUMINT csoport felállításával számolt, csoportonként 9-9 fővel.

A felderítő századok három, illetve kétszakaszos szervezésben lefednék a hagyományos csapat és mélységi felderítő tevékenységet.

Az ISTAR zászlóalj *elektronikai hadviselés* százada az alábbiak szerint épülne fel:

- századtörzs;
- rádiófelderítő (SIGINT) szakasz, 1-3 rádiófelderítő állomással;
- elektronikai (ELINT) felderítő szakasz, 1-3 elektronikai felderítő állomással;
- rádiózavaró szakasz, 1-2 zavaróállomással;
- értékelő központ.

Mint látható, a tervezet elkészítésekor több logikai hibát vétettek és összemossák, összekeverik a SIGINT (Signals Intelligence) és EW (Electronic Warfare), a magyar nyelvben elektronikai hadviselés, terminológiát, ezért a felsorolásban szándékosan az eredeti elnevezést hagytam meg. A hiba, tapasztalataim alapján abból ered, hogy nem ismerik pontosan a két elnevezés tartalmát.

A SIGINT, mint a rádióelektronikai felderítő tevékenység magában foglalja a rádió- (COMINT) és a rádiótechnikai felderítést (ELINT). Tehát a rádiófelderítő szakasz eleve nem viselhetné a SIGINT jelzőt. Helyesen COMINT elnevezés volna megfelelő, ha nem elektronikai hadviselés századról beszelnénk. A SIGINT csak passzív tevékenységet végez, míg az EHV aktív összetevőkkel is rendelkezik.

Az elektronikai hadviselés³² tartalma és összetevői:

- elektronikai támogatás (Electronic Support Measures-ESM);
- elektronikai támadás (Electronic Attack- EA),³³
- elektronikai védelem (Electronic Protection- EP).

Az EHV század szervezetében a fent felsoroltaknak megfelelően az ESM és EA tevékenység jelenhet meg.

³² FM 3-36 alapján (Internet), <http://usacac.army.mil/cac2/Repository/FM336/FM336.pdf>, letöltve 2012. 09. 24.

³³ Korábban az elektronikai támadás helyett elektronikai ellentévékenység (Electronic Counter Measures-ECM) elnevezést használták, de az FM 3-36 2009. évi kiadása már egyértelműen ezzel a terminológiával számol.

Az ESM hasonlóan a SIGINT-hez a szemben álló fél által használt elektromágneses spektrumból nyeri az információit, vagyis a kisugárzott elektromágneses és más kisugárzások detektálásával, azonosításával foglalkozik. Az MH. elektronikai hadviselési doktrínája szerint: „Az elektronikai támogatás az elektronikai hadviselés azon területe, amely az ellenség helyzetére vonatkozó tájékozottság és a fenyegetés késedelem nélküli felismerés céljából magában foglalja az elektromágneses kisugárzások kutatását, felfedését és azonosítását, valamint a kisugárzók helyének meghatározását.”³⁴

Tehát az elektronikai támogatás feladatai, különösen harcászati szinten átfedést, azonosságot mutatnak a SIGINT-tel. A különbség az információgyűjtés céljában kereshető. Természetesen az ESM is hozzájárul a felderítő információgyűjtő tevékenységhez, de alapvető célja a fenyegetések azonnali felismerése, azonosítása. Összefoglalva az ESM fő feladata az önvédelem és a célmegjelölés. Tehát az ESM olyan harci információkat szolgáltat, amely alapján elektronikai támadást (pl. zavarást), vagy fizikai pusztítást, tűzcsapást lehet és kell kiváltani, vagy a csapatok manőverei által kitérni a fenyegetések elől.

Ezt mindenképpen fontosnak tartottam tisztázni, hiszen a terminológiai tartalom és a tevékenység céljának ismerete szüksége ahhoz, hogy az EHV század felállításához szükséges alkalmazói követelményeket megfogalmazhassuk.

Tehát a szervezetben, helyesen, az elektronikai felderítést végző (ESM) alegységeket rádió-, illetve rádiótechnikai felderítő szakaszoknak célszerű elnevezni. A zavarószakasz elnevezése megfelelő.



4. kép: Egy lehetséges megoldás rádiófelderítő feladatokra, a „Proféta” (Prophet)³⁵

Ami a felderítő támogató századot illeti, a Magyar Honvédség az alábbi alegységekkel számolt:

- század törzs;
- pilótánélküli felderítő (PNF) szakasz;
- szenzoros felderítő szakasz;
- távirányítású robbanóeszköz zavarószakasz;
- földi mozgócélfelderítő szakasz.

³⁴ Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrína. 2004.

³⁵ Forrás: www.14cav.org/w3-d-intro.html. A Prophet SIGINT eszközt általános rádióelektronikai felderítő eszközként, széleskörűen használják az USA szárazföldi erőinél és a tengerészgyalogságnál. A Magyar Honvédség számára hasonló, nagy mozgékonyssággal és páncélvédelemmel rendelkező eszközök rendszeresítése javasolt.

A pilótanélküli eszközökből a Magyar Honvédség jelenleg, az izraeli gyártmányú Skylark-I LE típusú SUAV-okkal rendelkezik, amelyek a Tartományi Újjáépítő Csoport, képi felderítő-támogatását (IMINT) hajtják végre. A NATO ajánlások alapján célszerű mind a LAME, mind a MALE UAV-kat célszerű az ISTAR képesség megteremtése érdekében rendszeresíteni.

Az utóbbi (MALE) pilótanélküli felderítő eszközöket (közepes magasságú, nagy hatótávolságú) általában 24-48 órás szolgálati idővel és 3000-10000 méter magasságban alkalmazzák. A hasznos terhelhetőségük kb. 500-800 kg.³⁶

A Nemzeti Katonai Stratégiában megfogalmazottak alapján, a Magyar Honvédség jövőbeni várható alkalmazási területei és feladatai figyelembevételével kiemelkedő felderítő képességre tehetnénk szert ilyen eszközök beszerzése esetén, amelyekkel nem csak a nemzeti, hanem szövetségi információszerző igények is kielégíthetők volnának.

Fejlesztési irányként fontos, hogy a későbbi beszerzésre, rendszeresítésre tervezett UAV eszközeink alkalmasak legyenek SIGINT, EHV, ABV,³⁷ SAR/MTI,³⁸ stb. függesztmények (payload) hordozására is. Ezen felderítő eszközök, szenzorok általában MALE UAV-k payloadjaiba vannak beépítve, a nagyobb méret és komolyabb harcászati-technikai paraméterek miatt.

A HM EI Zrt. által a közelmúltban bemutatott „Bora” és „Ikran” repülőeszközök is csak IMINT feladatok végrehajtására alkalmasak (jelenleg) és legfeljebb a már rendszerben lévő pilótanélküli repülőeszközöknek jelentenek hazai alternatívát.



5. kép: A Magyar Honvédségben rendszeresített Skylark SUAV.³⁹

A szenzoros felderítő szakasz technikai eszközei kiválasztása érdekében célszerű lenne tanulmányozni az USA hadsereg harctéri érzékelő rendszereivel szerzett tapasztalatait. A legismertebbek egyike a REMBASS⁴⁰ és az IREMBASS⁴¹ rendszerek, melyek felügyelet nélküli passzív infravörös, mágneses szeizmikus és akusztikus szenzorokból és adatátviteli eszközökből állnak.

³⁶ A MALE kategóriában leggyakrabban használt eszközök: Aeronautics Defense Dominator (Izrael), IAI Heron (Izrael), TAI Anka (Törökország), EADS Harfang (a franciák az izraeli IAI Heron licensze alapján fejlesztették), MQ-1 Predator (USA), Scaled Composites Model 395 (USA), Chengdu Pterodactyl I (China), EADS Talarion (Európai Unió és Törökország) és a DRDO Rustom (India). A szakemberek az USA, izraeli és a török gyártmányokat tartják a kategória legjobbainak.

³⁷ ABV: atom, biológiai, vegyi.

³⁸ SAR/MTI- Synthetic Aperture Radar (szintetikus apertúrájú lokátor)/ Moving Target Indicator (mozgócéli indikátor).

³⁹ Forrás: www.honvedelem.hu/cikk/35023_fotisztek_a_bocskai_dandarnal

⁴⁰ REMBASS -Remote Battlefield Sensor System (AN/GSQ-187).

⁴¹ IREMBASS -Improved Remote Battlefield Sensor System (AN/GSQ-187).



6. kép: REMBASS felügyelet nélküli szenzorok.⁴²

Szakmailag a legnagyobb dilemmát a *távírányítású robbanóeszközök elleni tevékenységre* létrehozni tervezett szakasz ötlete, illetve annak a felderítő támogató század szervezetébe történő létrehozása jelenti.

Mint ismeretes az IED-k⁴³ okozzák a legtöbb veszteséget a XXI. századi aszimmetrikus hadviselési területeken. Ezek speciális formái a RCIED-k⁴⁴, amelyek rádió-, gyakran GSM, vezérléses elven működtethetők el. Ezen eszközök elleni tevékenységre (rádiózavarás) lenne alkalmas a szakasz. Tartalmában ez, semmiben sem különbözik az elektronikai ellentevékenységtől (leggyakrabban zavarás), ezért az elektronikai hadviselés század szervezetében van a helye. Ez a század felelős a zavaróeszközök használatra való felkészítéséért, felprogramozásáért, a frekvenciamenedzsmentért (zavarásra kijelölt frekvenciák, vagy sávok, tabufrekvenciák stb.) és az eszközök alkalmazás utáni kiértékeléséért. Így a zavarótevékenységnek egy kézben, egy alegységben kell összpontosulnia, nem külön szervezetbe allokálni, forrásainkat szétaprózva.

Véleményem szerint a 2007-ben megfogalmazott elveket meghaladta az idő érdemes lenne azokat újragondolni. Elgondolásom azon a tapasztalaton alapul, hogy a hadszíntereken tevékenységet végrehajtó, gyakorlatilag valamennyi harc és gépjármű rendelkezik egyéni zavaró-berendezésekkel, amelyek védelmet biztosítanak és a feladat, valamint a felderítési információk alapján programozhatóak, így nem célszerű erre külön alegységet, szervezetet működtetni. Továbbra is ez volna a célszerű megoldás, így plusz alegység felállítása nem indokolt. Az elektronikai hadviselés század zavarószakaszt kell alkalmassá tenni az előre nem látható feladatok végrehajtására.⁴⁵

⁴² Forrás: www.defense-update.com/products/r/rembassII.htm.

⁴³ IED -Improvised Explosive Device: improvizált (házilagosan előállított) robbanóeszköz.

⁴⁴ RCIED -Radio Controlled IED: rádióvezérlésű (indítású) improvizált robbanóeszköz.

⁴⁵ A gép és harcjárművekbe épített zavaróeszközök (jammerek) inkább egyéni, mint kollektív zavaróeszköznek tekinthetők. Az elektronikai hadviselés elvei alapján kollektív zavaróeszköznek minősülnek azok, amelyek több eszköz, vagy kötelékek oltalmazására alkalmasak.



7. kép: Az L3 cég által gyártott szélessávú háton szállítható zavaró berendezés.⁴⁶

A földi *mozgócélfelderítő* szakasz esetében 1-3 raj rendszeresítésével számol a tervezet, amely egy, a Magyar Honvédség rendszerében már meg nem lévő képesség helyreállítását jelentené. A korábban a BMP-kel felszerelt lövészalegységek szervezetében volt rendszeresítve a PSZNR-5 földi mozgócélfelderítő lokátor, jelenleg ilyen képességünk nincs.



8. kép: Egy lehetséges megoldás, az LRAS3 lézeres target acquisition rendszer.⁴⁷

VÁLTOZAT EGY LEHETSÉGES ISR ZÁSZLÓALJ KIALAKÍTÁSÁRA

Az előző fejezetekben kifejtetteknek megfelelően kiviláglik, hogy a 2007-ben született ISTAR (ISR) zászlóalj koncepciója revízióra szorul. Természetesen ez összefüggésben van az eltelt idővel, az azóta megszerzett hazai és nemzetközi tapasztalatokkal és a politikai és honvédelmi vezetés, a Magyar Honvédség alkalmazását illető, elképzelésének megváltozásával.

Az alaphelyzet teljesen világos: szükséges és fontos megteremteni az ilyen irányú képességünket. Középtávon gondolkodva ezt a szervezetet továbbra is az MH. 5/24 felderítő zászlóalj bázisán kell úgy kialakítani, hogy az alkalmas legyen (kötelékben, vagy önállóan) egy dandárerejű szervezet (honi vagy szövetséges környezetben) harcászati-hadműveleti felderítő igényeinek kielégítésére.

⁴⁶ Forrás: www.defense-update.com/products/b/broadshield.htm.

⁴⁷ Forrás: www.defense-update.com/20100907_lras3_liteye_monocular_displays.html.

Ezért nem értek egyet azon elképzelésekkel, amelyek egy önálló Különleges műveleti ezred (KME) felállítását javasolják úgy, hogy abba a jövőbeni ISTAR (ISR) zászlóalj beintegrálását célozzák meg.⁴⁸

Az ötlet szülőatyja kétségtelenül alaposan és módszeresen körbejárja a lehetséges változatokat, de egy sajátos és szűk értelmezésű változatot javasol, amely nem állja meg a helyét stratégiai környezetben.

A különleges műveleti erők a NATO AJP.3.5 (Allied Joint Doctrine for Special Operations) szerinti feladatai:

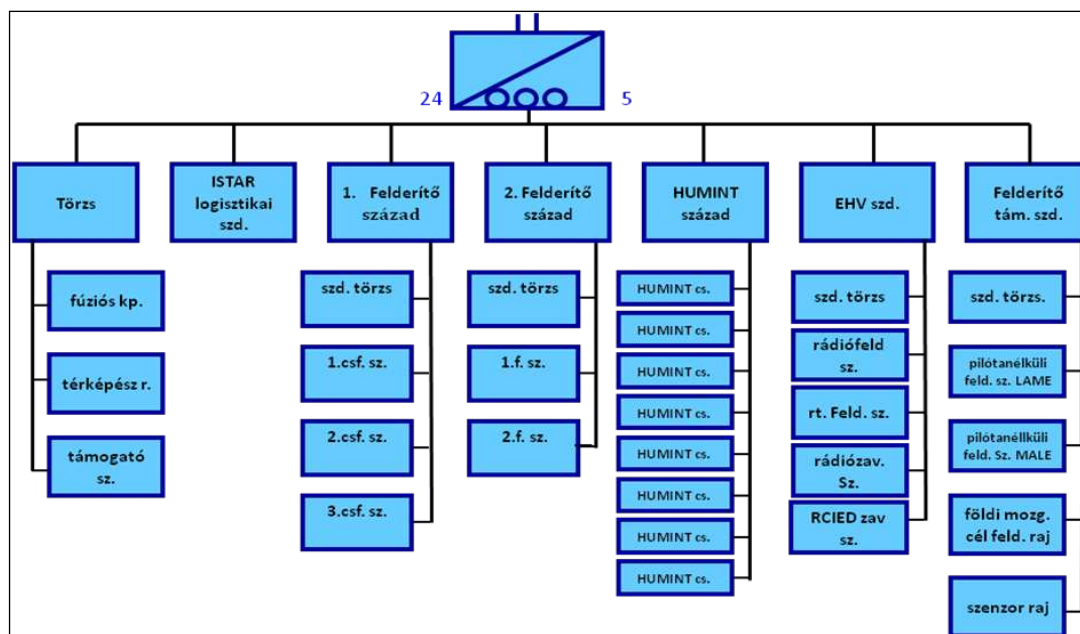
- különleges felderítés (KF)
- közvetlen művelet (KM)
- katonai segítségnyújtás.

A hivatkozott dokumentum és az abban felsorolt feladatok világosan jelzik, hogy a különleges műveleti erők csak egy részfeladata a KF és ez szinte kizárólag a KM érdekében történik. Habár a jelen hadszínterek pl. Afganisztán is bizonyítja, hogy egy harcászati információnak hadászati hatása is lehet, a különleges műveleti erők harcászati tevékenységet hajtanak végre. Habár ezek az alegységek rendelkeznek önálló felderítő eszközökkel, az ISTAR (ISR) támogatásukat egy magasabb törzs végzi más szervezetekben rendszeresített technikai eszközök alkalmazásával (ISTAR mátrix).

A másik fontos megállapítás, ami miatt hibás az a következtetés, hogy saját ISTAR (ISR) zászlóaljrendszeresítése volna indokolt a jövőbeni KME állományába, annak ténynek a megértése, hogy a felderítés **nem** egyenlő a különleges műveleti tevékenységgel.

Bármilyen jó a szándék a szakma jobbítására a magyar ISTAR (ISR) zászlóaljnak úgy kell felállnia, hogy az modulrendszerűen alkalmas lehessen már szervezetek támogatására is, de mindenképpen egy dandárerejű egység harca érdekében.

Mindenesetre Gulyás Attila százados munkájában felvázolt ISTAR (ISR) zászlóalj szervezetével alapvetően egyetértek. A felderítő és hírszerző századok szervezetére vonatkozó megállapításai támogathatóak, de az elektronikai hadviselés és az egyéb felderítő támogatásban résztvevő erők tekintetében néhány észrevételt teszek. Az 3. számú ábra egy lehetséges változatot ábrázol.



3. ábra. Az ISTAR (ISR) zászlóalj javasolt szervezete⁴⁹

⁴⁸ Gulyás Attila mk. százados: Gondolatok a nemzeti különleges műveleti erők fejlesztéséről. Honvédségi szemle 2012/4. szám, HU ISSN 2060-1506

A zászlóalj törzs valamennyi NATO vezetési elemet tartalmazna (S1, S2, S3, S4, S6, S7). Szükséges egy térképészeti támogató elem (raj) rendszeresítése, amely a hagyományos és digitális, térinformatikai megoldásokon alapuló alkalmazásokat biztosítaná, kezelné.

A támogató szakasz volna felelős a zászlóalj vezetési pontjának működtetéséért, különösen önálló tevékenység végrehajtása esetén.

Javaslatom alapján az összadatforrású fúziós központ (All Source Analysis Center) is a törzsben kapna helyet. A különböző adatszerző elemektől (HUMINT, EW, IMINT, OSINT,⁵⁰ RADINT⁵¹, szenzorok) származó anyagokat dolgoznák fel és itt teljesítenének szolgálatot az együttműködő szervezetek (pl. légierő, SOF,⁵² KNBSZ⁵³ stb.) összekötői is.

A törzs tevékenységét a parancsnok kritikus információ igényei (CCIRM⁵⁴), az elsődleges hírszerzési igények (PIR⁵⁵), az információ (hírszerző) terv (ICP⁵⁶) és a felderítő információigények alapján (RFI) hajtana végre az előljáró G2/J2 szakmai koordinálásával. Biztosítani kell, hogy a központ hozzáférhessen a nemzeti és szövetséges, nyílt és minősített hálózatokhoz, mindezt az összadatforrású fúziós adatfeldolgozás érdekében.

A végrehajtó erőket illetően (amely megegyezik a Honvédelmi Minisztérium Haderőtervezési Főosztály, Haderőtervezési és Modernizációs Osztálya által 2007-ben ismertetett elképzeléssel) kettő felderítő századdal számolnánk. A háromszakaszos század a „hagyományos” csapatfelderítő erőket, míg a kétszakaszos az ejtőernyős és bűvárlegységeket foglalná magába.

A HUMINT század állományában továbbra is nyolc (8) HUMINT csoport kerülne rendszeresítésre.

Az elektronikai hadviselés (EHV) század ötszakaszos változatban kerülne felállításra. A rádiófelderítő (RÁF) szakasz állományába mind gép, vagy harcjárműbe épített felderítő- és hordozható eszközök rendszeresítésre kerülnének.⁵⁷ Nem szükséges külön rádióíránymérő alegység rendszeresítésre, hiszen a modern RÁF eszközök már biztosítják ezek a funkciókat.

A szembenálló fél vezetési és fegyverirányítási rendszereiben működtetett nem kommunikációs eszközök (pl. radar, IFF, telemetriai stb.) felderítésére felállításra kerülne egy rádiótechnikai felderítő szakasz.

A rádiózavaró szakasz állományába kell rendszeresíteni a kollektív (alegységek védelmére szolgáló) elektronikai ellentevékenységi (pl. zavaró) eszközöket, amelyek a szembenálló fél elektrooptikai és rádiófrekvenciás kisugárzáson alapuló eszközeinek működését gátolná.

Mivel logikailag is ebbe a tevékenységi körbe tartozik, az EHV század állományába kell szervezni a rádiófrekvenciás vezérlésen alapuló improvizált robbanóeszközök (RCIED) elleni tevékenységre beszerzett zavaróberendezéseket, önálló szakaszként.

A felderítő támogató század alapvetően IMINT feladatokat hajtana végre LAME és MALE UAV-k⁵⁸ használatával. Itt kapna helyet a felügyelet nélküli harctéri szenzor és a földi mozgócél felderítő szakasz is. Az utóbbi alapvetően felderítési és nem célmegjelölési, (célkijelölési) feladatokat hajtana végre és hordozható, vagy harc és gépjárműből könnyen kitelepíthető eszközökkel lenne felszerelve.

⁴⁹ Forrás: a szerző javaslata

⁵⁰ OSINT- Open Source Intelligence: nyílt adatforrású felderítés.

⁵¹ RADINT- Radar Intelligence: radar alapú felderítés.

⁵² SOF- Special Forces: különleges műveleti erők

⁵³ KNBSZ: Katonai Nemzetbiztonsági Szolgálat

⁵⁴ CCIRM-Commander Critical Information Requirement Management.

⁵⁵ PIR- Priority Intelligence Requirements.

⁵⁶ ICP-Information Collection Management.

⁵⁷ Ezek 1-2 főből álló gyalogos rádiófelderítő járőrök, az LLVIT-k (Low Level Voice Interception Team), vagy LEWT-k (Light Electronic Warfare Team) felszerelését képeznék.

⁵⁸ Ez alapvetően megegyezik Gulyás százados javaslatával, de ő SUAV (Short Range UAV) és MUAV (Medium Range UAV terminológiát használ.

A mindenoldalú biztosításhoz szükséges egy logisztikai század felállítása is.

Mivel a célmegjelölés (célkijelölés), a magyar döntés értelmében a tűzérési erőkhez kerül allokálásra, így a jövőbeni zászlóalj ISR zászlóaljnak célszerű továbbiakban nevezni.

ÖSSZEFOGLALÁS

A 2007-ben megvalósításra tervezett ISTAR zászlóalj szervezete számos, a NATO ajánlásoknak megfelelő javaslatot tartalmazott. Sajnos a költségvetési források nem tették, nem teszik lehetővé az elképzeléseknek megfelelő ütemezésű kialakítását az MH 5/24 „Bornemissza Gergely” felderítő zászlóalj bázisán. A képességek megteremtése rendkívül lassan halad, de szerencsére számos tiszt és altiszt kollégánk foglalkozik e képesség elméleti-gyakorlati kutatásával, így elképzeléseik, javaslataik útmutatók lehetnek.

Az elmúlt években alapvetően sokat változott maga az ISTAR koncepció is. Az elképzelések alapján az ISR képesség maradna zászlóalj szervezetben, míg a célmegjelölés (célkijelölés) a tűzérési erőkhez kerülne beintegrálásra.⁵⁹ Jelenleg az alegység elégséges HUMINT, megfelelő IMINT és minimális EHV képességekkel (elégtelen felderítő és kizárólag egyéni zavaróeszközök) rendelkezik, de lassú fejlődés mindenképpen kimutatható. Mivel az elektronikai támogatás és a SIGINT **harcászati** szinten gyakorlatilag egymást átfedő feladatokat hajt végre (csak a tevékenység céljában van különbség), így kézenfekvő, hogy a Katonai Nemzetbiztonsági Szolgálat, támogatást nyújtson a különleges jogrend, vagy a missziós feladataink végrehajtása során. Ez a technikai eszközök biztosításában, vagy a személyi állomány felkészítésében, képzésében, valamint közös feladat végrehajtásban is manifesztálódhat.

Figyelemreméltó fejleményként kell megemlíteni a 2012. májusi chicagói NATO csúcserőkezelést, amelyen többek között egy olyan ISTAR/ISR témájú javaslat került elfogadásra, amely JOINT képességekkel ruházná fel a Szövetséget. Az Allied Ground Surveillance System (AGS)⁶⁰ a Líbia elleni hadműveletek tapasztalatait felhasználva biztosít majd, várhatólag 2017-re komoly felderítő képességet. Az aláíró 13 NATO ország 5 Global Hawk UAV-t és a hozzátartozó rendszert vásárolja meg és az AWACS⁶¹ és HAW⁶² flottához hasonlóan üzemeltetik majd.

Örömmel hallani, hogy valamennyi, a képességfejlesztéssel foglalkozó konferencia, rendezvény kiemelten foglalkozik a felderítés korszerűsítésével, annak prioritásaival. Azonban az Összhaderőnemi Parancsnokságon 2012. 11. 08-án kapott tájékoztató alapján nem túlságosan biztató, hogy főleg költségvetési okokból, az ISTAR (ISR) képességhez tartozó konkrét lépések csak (a jelenlegi helyzet szerint) 2016-tól kezdődhetnek. Éppen ezért lenne fontos átgondolni újra a megvalósításra váró feladatokat, a tapasztalatok feldolgozásából származó új igényeket (Kosзовó, Irak, Afganisztán, Líbia stb.), hogy a NATO csúcstalálkozókon meghirdetett Európai Unió Pooling and Sharing, valamint a NATO Smart Defence elvekhez igazodjunk. Mindenképpen úgy kell képességeket kialakítani, hogy az működhessen nemzeti és nemzetközi (szövetséges) környezetben is. Ezért fontos az eszközeink, alrendszereink, rendszereink interoperabilitása.

⁵⁹ MH Összhaderőnemi Parancsnokság, Felderítő Főnökség FEF/8-19/2011. nyt. számú ügyszerződés, 2011. március. A Fegyvernemi Állandó Munkacsoport (FÁM) ajánlása alapján. Számos nemzetközi példa is igazolja ezt az elképzelést pl. a 2006-ban Ausztráliában felállított 20th Surveillance and Target Acquisition ezred, ami a tűzéréshez tartozik.

⁶⁰ http://www.nato.int/cps/en/natolive/topics_48892.htm

⁶¹ AWACS - NATO's Airborne Early Warning & Control System (NAEW&C)

⁶² HAW –Heavy Airlift Wing: Nehéz szállító repülőezred (Pápa)

A katonai alkalmazás szempontjából nem lehet elsőrendű, de mindenképpen fontos kritérium, hogy a Magyar Honvédség jövőbeni képességei (képességmoduljai) civil feladatokra (katasztrófa-elhárítás, természeti csapások esetén) is használható legyen.

„Magyarország fegyveres ereje a Magyar Honvédség. A Magyar Honvédség alapvető feladata Magyarország függetlenségének, területi épségének és határainak katonai védelme, nemzetközi szerződésből eredő közös védelmi és békefenntartó feladatok ellátása, valamint a nemzetközi jog szabályaival összhangban humanitárius tevékenység végzése.⁶³

Ennek megfelelően kell megtennünk a következő lépéseinket. A közhasznúság és a katasztrófavédelmi feladatok napjainkban történő túlhangsúlyozása ugyanúgy káros folyamatokat indíthat el, mint annak alábecsülése. Meg kell találni az egyensúlyt a feladatok között, hogy a Magyar Honvédség teljesíthesse alaprendeltetésű feladatait a jövőben is. Ehhez azonban forrás kell, a humán erőforrás, a szürkeállomány már rendelkezésre áll. Úgy kell döntenünk, hogy azok eredményei előremutatóak és relevánsak lehessenek.

Ahogy Churchill ezt korábban megjegyezte „Uraim, a pénzünk elfogyott, ideje gondolkodnunk”.

Felhasznált irodalom

- [1] Dr. Horváth Zoltán mk. ezredes: Az összhaderőnemi műveletek ISTAR támogatása, Seregszemle különszám, 2012. június, 88. oldal,
- [2] Dr. Horváth Zoltán mk. ezredes: Egy lépés az ISTAR képességek fele – új felderítő eszköz a Magyar Honvédségben, VIII. évfolyam, 2. szám, 2010. április-június 49. o. Internet: http://www.hungariandefence.com/container/files/attachments/28301/s_sz_2010_2.pdf letöltve: 2012.10.12),
- [3] AAP-06 NATO Glossary of Terms and Definitions (English and French) 2012 (2),
- [4] AJP 2.1 (Allied Joint Publications) 1. fejezet, IX. rész, 114. pont,
- [5] Honvédelmi Minisztérium Védelempolitikai és Védelemtervezési Helyettes Államtitkár. ny. sz.: 503-34/2010 számú dokumentum. Honvédelmi Minisztérium 1-9. oldalak,
- [6] AJP 2.7 -Allied Joint Doctrine for Reconnaissance and Surveillance dated 7 July 2009,
- [7] Gulyás Attila: A nemzeti különleges műveleti erők felderítő támogatása, Hadmérnök VII. évfolyam 3. szám 2012. szeptember, 135-136 o.,
- [8] Magyarország Nemzeti Katonai Stratégiája (tervezet) 41. pont, megtalálható Internet: http://www.kormany.hu/download/d/ac/a0000/Nemzeti%20Katonai%20Strat%C3%A9gia_tervezet.pdf, letöltve 2012.11.04.,
- [9] Haig Zsolt, Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, 2005, ISBN 963 327 391 9, 176 o.,
- [10] AJP 3.10 Allied Joint Doctrine for Information Operations (2009), Internet: <http://info.publicintelligence.net/NATO-IO.pdf>, letöltve 2012.10.10.
- [11] EL 0583 – NATO 2006 force proposals for Hungary 2006 – 2016.,
- [12] FM 3-36. Internet, <http://usacac.army.mil/cac2/Repository/FM336/FM336.pdf>, letöltve 2012. 09. 24.,
- [13] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrína. 2004.,

⁶³ Magyarország Alaptörvénye 45. cikk, megtalálható: www.kozlonyok.hu/nkonline/mkpdf/hiteles/mk11043.pdf

- [14] MH Összhaderőnemi Parancsnokság, Felderítő Főnökség FEF/8-19/2011. nyt. számú ügyszerabja, 2011. március.
- [15] Gulyás Attila mk. százados: Gondolatok a nemzeti különleges műveleti erők fejlesztéséről. Honvédségi szemle 2012/4. szám, HU ISSN 2060-1506.
- [16] Coalition Interoperable ISTAR System, Concept of Employment, Working Paper version 1.0, MAJIIC Operations Working Group (OWG), The Hague 2007. Internet: <http://info.publicintelligence.net/NATOistarconemp.pdf>. letöltve: 2012. 10.21.
- [17] NATO AJP.3.5 (Allied Joint Doctrine for Special Operations) dated 27 Jan 2009. Internet: <http://infostore.saiglobal.com/store/details.aspx?ProductID=1128193>. letöltve: 2013. 01. 10.
- [18] Magyarország Alaptörvénye 45. cikk, Internet: <http://kozlonyok.hu/nkonline/mkpdf/hiteles/mk11043.pdf> Letöltve: 2012. 11. 10.

STRUKTÚRA ÉS FUNKCIÓ A HÁLÓZATALAPÚ HADVISELÉSBEN

Absztrakt

Olyan számítógépes modell elvi és gyakorlati megvalósításáról számol be a cikk, amely alkalmas a Nemzeti Közzolgálati Egyetem több szakmai területének, így a honvédelemnek, a rendvédelemnek és a közigazgatásnak a segítésére, miközben a funkcionális fenntarthatóságot előnyben részesíti a merev struktúrához való ragaszkodással szemben. A modell jelen formájában is képes a valóságos harc modellezésén kívül különféle civil problémák megjelenítésére és a küzdelmi dinamika tanulmányozására. A modell egy új paradigmát mutat be: Külön-külön intelligencia nélküli, de egymással kommunikálni képes részekből olyan szervezet áll össze, amely külső beavatkozás nélkül védelmi intelligenciát fejleszt ki magának.

The present paper gives an account on the theoretical and practical realization of a computer model, which is capable of supporting several professional fields of the National University of Public Service, such as national defence, law enforcement and public administration, while it prefers functional sustainability to insistence on a rigid structure. The model in its present form can, apart from modeling actual fight, display different civil problems and study combat dynamics. The model introduces a new paradigm. Separate parts, which have no individual intelligence but can communicate with one another, can form an organization, which develops for itself, without external intervention, some sort of defence intelligence.

Kulcsszavak: *hálózat-alapú hadviselés, logikai kockázatelemzés, közigazgatás modellezése, sejtautomata, GMO ~ network-centric warfare, logical risk analysis, public administration modeling, cellular automaton, GMO*

BEVEZETÉS

A különböző szaktudományok fejlődésével természetes módon együtt jár a differenciálódás, vagyis a korábbi részterületekkel foglalkozó új szaktudományok kialakulása, és az integrálódás, vagyis a szaktudományok módszereinek és eredményeinek egyesítése új diszciplinák kialakítása érdekében.

Ezt a tendenciát követi a hadtudomány is, amelynek eredeti, klasszikus tárgykörét a reguláris hadseregek nyílt összecsapásával kapcsolatos stratégiai-taktikai problémák alkotják. Napjainkban a nagyhatalmak közvetlen katonai konfrontációjának esélye erősen lecsökkent, ami a hadtudományt is új kihívások elé állítja. Ezért a tárgykör fokozatosan bővülni kezdett: először a nem hagyományos hadviselés irányában, l. Kiss (2011), majd megjelent a polgári alkalmazások iránti igény is. Ebbe a tendenciába illeszkedik a jelen cikk. Mint Zsigovits (2011) rámutat: „...célszerű a hadtudományt a legszélesebb értelemben felfogni, és ebből leszármaztatni a nem fegyveres küzdelem megvívásának tudományos megalapozását, így a rendvédelem, rendészet, államigazgatás területeken is.”

A hadviselés fogalmának szokásos értelmezése olyan aktusok sorozatát jelenti, amelyek egy másik fél erejének lerombolására vagy meggyengítésére irányul. A jelen cikkben hadviselésen két fél küzdelmét értjük, ahol legalább az egyik fél célirányosan és alkotórészeinek valamilyen egymást befolyásoló működésével cselekszik. Szándékosan nem kívánjuk meg a tudatosságot egyik féltől sem, mert bármelyik küzdő fél lehet valamilyen jelenség, élőlények vagy gépek csoportja is. A célirányos cselekvést azonban legalább az egyik félről feltételezzük. Ez az értelmezés lehetővé teszi a természeti jelenségek által okozott károk elkerülésének és rehabilitációjának elemzését is.

HÁLÓZATALAPÚ HADVISELÉS – A STRUKTÚRA VAGY A FUNKCIÓ ELLEN?

A hálózatalapú hadviselés koncepcióját korábbi publikációnkban (Bukovics-Fáy-Kun, 2011) ismertettük, itt csak röviden összefoglaljuk. Eszerint a haderőket hálózatukkal együtt, azzal összefüggésben szemléljük. A hadviselési elv az anyagi eszközök struktúráját kívánja rombolni, és a rombolás valószínű, de bizonytalan következményeként várja az ellenség harcképességének csökkenését.

Lényegét az a felismerés képezi, hogy a csapásmérés hatékonysága csekély, ha nem a hálózati szemléleten alapszik. A hálózat, mint működési mód figyelembe vétele mind a saját, mind az ellenséges erők esetében kulcsfontosságú.

Ezt a koncepciót most némileg finomítjuk. A korábbi megközelítést kiegészítve, hangsúlyozzuk, hogy a támadás valódi veszélyét a funkció sérülése jelenti, ami természetesen előállhat – bár nem kizárólag – a struktúra sérülésén keresztül. Amit tehát elsősorban védeni – és sérülése esetén helyreállítani – kell, az a funkció. Természetesen a módosult struktúrának is alkalmasnak kell lennie az eredeti funkció ellátására.

A jelen publikációban éppen arra mutatunk példát, hogy a funkció fenntartható vagy legalábbis helyreállítható az eredeti struktúra helyreállítása nélkül.

GERILLA-HADVISELÉS

A gerilla-hadviselés valaha élt egyik legnagyobb szakértője, Ernesto „Che” Guevara 1961-ben írt tanulmánya szerint (Guevara, 1998) az alábbiakban jelöli meg ennek legfontosabb jellemzőit:

- *Mozgékonyság, meglepetés*, A gerilla-stratégia nem változtatja meg a felek erőviszonyait, mégis lehetővé kell tennie a csaták túlélését. Ennek alapvető módja a csatatér összezsugorítása, ahol a gerilla is kerülhet időleges fölénybe.

- *Gyors visszavonulás*, A gerillának nincsenek erőforrásai, tartalékai a pozíció megtartásához, ezért nem habozik elhagyni a helyét, hogy azután a legváratlanabb helyen bukkanjon fel. Ha lehetőséget lát, azonnal támad, de ha veszét érzi, rugalmasan kisiklik az egyenlőtlen harcból.
- *Alkalmazkodóképesség, megtévesztés*. A gerilla-parancsnok nem tekintheti saját csapatait egyenlő ellenfélnek egy reguláris hadsereggel szemben. A közönséges számtant kell kihasználnia. Például a vietnami háborúban az amerikai csapatok kevesebb, mint 20 %-a harcolt, a többiek ellátó, támogató katonák voltak. Ha a Vietkong az amerikaiak harcmodorát alkalmazza, akkor biztosan elveszíti a háborút.

Robert Taber amerikai szakértő az alábbi módon jellemezte a kubai gerillaháborút (Taber, 1965): „A bolha csíp, ugrik, aztán újra csíp fürgén elkerülve a lábat, mely el akarja taposni. Nem törekszik arra, hogy egy csapásra megölje ellenfelét, de mindig belemar és ő maga abból táplálkozik, csapásokkal sújtja és bosszantja ellenfelét. Ha szükséges, kikelt újabb bolhákat... az ellenfél hadereje pedig a kutya hátrányával szenved; túl nagy védekezni, támadója pedig túl kicsi és mozgékony ahhoz, hogy fogást találjon rajta.”

Mao Ce-tung pedig a kínai „népi háború” stratégiáját írta le a következőképpen (Mao Tse-tung, 1989): „Az ellenség előrenyomul, mi visszavonulunk; az ellenfél letáborozik, mi fárasztjuk zaklatásainkkal; az ellenfél elfárad, mi támadunk; az ellenfél visszavonul, mi üldözzük.”

A gerilla-hadviseléshez meglepően hasonló módon harcoltak annak idején a magyarok, lásd (Zólyomi, 2011):

- *Mozgékonyosság*. Váratlan helyen, időben és irányokból végrehajtott támadás, mely adott esetben akcióképtelenséget váltott ki az ellenség soraiban.
- *Megtévesztés*. A magyar lovasság menekülést színlelt, mire az ellenség biztos győzelmének tudatában üldözőbe vette a menekülő könnyűlovasságot, mely ekkor visszafordulva a felbomlott hadrendű üldözők erőit egyenként felmorzsolta.
- *Manőverezés*. Előszeretettel alkalmazták azt a taktikát is, amikor az üldözőket csapdába csalva tartalékban várakozó nagyobb erők gyűrőjébe vezették. Ugyancsak bevett gyakorlat volt az ellenség zaklatása távolról végrehajtott rajtaütésekkel, nyílzáporral, aminek hatására az ellenség hadrendje felbomlott és a megnyíló résekbe a könnyűlovasság behatolt, ily módon kivégeztetve az ellenség főerőit.

LOGIKAI KOCKÁZATELEMZÉS

A logikai kockázatelemzés alapfogalmait korábbi publikációnkban (Bukovics-Fáy-Kun, 2011) ismertettük, itt csak röviden összefoglaljuk a legfontosabb fogalmakat.

- *Kockázati rendszer, esemény, állapot*. Ezek olyan alapfogalmak, amelyek szemléletes tartalma magától értetődő.
- *Hibafa*. A nemkívánatos esemény (főesemény, top event, explikátum) bekövetkezése szükséges és elégséges konjunktív-diszjunktív feltételrendszerének megjelenítése, modellezése.
- *Primesemény*. Saját hatáskörünkben lévő esemény.
- *Explikáns*. Bármely esemény szükséges és elégséges konjunktív-diszjunktív feltételrendszerének megjelenítése, modellezése.
- *Franklin-paraméterek*. Költség- illetve időigény.
- *Esemény aktív és passzív állapota*. Ez is alapfogalom.
- *Rendszerállapot*. Primesemények állapotösszessége.

A KÖZIGAZGATÁS HADTUDOMÁNYI ELEMZÉSE ÉS MODELLEZÉSE

A közigazgatás jogtudományi hátterének kidolgozása már évszázadokkal ezelőtt megtörtént, de önálló tudományként való kezelésének igénye a XX. század első felében merült fel, l. Willoughby (1927), Dahl (1947). Bukovics (2012) előadásában bemutatta a közigazgatás tudomány előzményeit, fogalmát, helyét és szerepét, továbbá javaslatot tett tudományos paradigmájára.

A közigazgatás hadtudománnyal való kapcsolatának kidolgozása, a közös diszciplináris problémák felismerése napjainkban is folyik, mint azt a korábban említett (Zsigovits, 2011) tanulmány mutatja.

A közigazgatást olyan küzdelemnek foghatjuk fel, ahol az egyik fél – akár emberi cselekvéseken keresztül, akár természeti jelenségként – „hozza” a napi szinten megoldandó gondokat, a másik fél – a közigazgatási apparátus – pedig igyekszik megoldani a gondokat, lépést tartva azok felmerülési ütemével. Ha ez a lépéstartás sikerül, az apparátus saját kapacitásának mozgósításával reagál a kihívásra, ami a struktúra részleges megváltozását jelenti (igazgatási kapacitások átcsoportosítása az igényeknek megfelelően), ez pedig nem egyéb, mint a struktúra részleges feláldozásával a funkció fenntartása. Katonai szóhasználatban ez azt jelenti, hogy az ütőképességet a rendelkezésre álló erők megfelelő átcsoportosításával tudjuk fenntartani.

A HADVISELÉS SEJTAUTOMATA-MODELLJE

Szinte bármely rendszer folyamatosan ki van téve különféle külső hatásoknak (támadásoknak) a szó legáltalánosabb értelmében. Ezeket a hatásokat valamilyen mértékben tolerálja, és *immunitási képességétől* függően *túléli*.

Az adott esetben a modellezéshez standard sejtautomatát használunk, kombinálva a hibafelmódszer logikai (determinisztikus) verziójával. A sejtautomata-rendszer determinisztikus elvek szerint működik. A sejtautomatával kapcsolatos fogalmakra nézve lásd (Bukovics, 2007).

In silico kísérletek bizonyítják, l. (Bukovics, 2007), hogy megfelelő átmeneti szabályok minden további modellfeltevés nélkül egyfajta *mesterséges immunitás* kialakulásához vezetnek. A vizsgálat célja nem az immunitás leírása vagy szimulációja, hanem egy olyan szabályrendszer keresése, amely biztosítja egy komplex, mesterséges, adaptív rendszer védekező képességének sikerességét.

Az immunitást kifejleszteni képes sejtautomata-rendszer neve *AIM-SORS* (Artificial Immunity Model – Self Organizing Raiding System = Mesterséges Immunitási Modell, Önszervező Támadó/Védelmi Rendszer). Ez egy olyan sejtautomata (sejttér, *CellSpace*, röviden *CS*), amely kétféle sejtől áll, ezek a *védő* és *védett* egységek (örsejtek és közsejtek). Más szóval, speciális „örsejtekről” beszélünk, melyek feladata „védeni” a többi (köz-) sejtet.

A „védeni” szónak itt speciális jelentése van, amit a „funkciót helyreállítani” kifejezés fejez ki. Jelen szövegösszefüggésben a „rehabilitálni” szót javasoljuk.

A közsejt egy színhely (mint például egy ország) földrajzi körzeteiként interpretálható. Emellett elméletileg egyéb interpretációk is lehetségesek, amelyek a modell megállapításának érvényességét nem érintik.

A modellben minden sejtnak négy szomszédja van, a konkrét alkalmazásnál ennek megfelelően végezzük el a földrajzi körzetek kialakítását. A közsejteknek kétféle állapota van. A közsejt lehet „virtuális” (azaz potenciálisan lehetséges), vagy „valós” (azaz ténylegesen bekövetkezett) veszélyállapotban.

Az állapot-átmeneti algoritmus teljes leírását terjedelmi okokból mellőznünk kell. Legfontosabb alapelveit azonban az alábbiakban közöljük.

Állapot-átmenet vagy két szomszédos sejt kölcsönhatásának, vagy külső támadásnak az eredményeképpen történhet.

Az állapot-átmeneti szabályrendszer két célt szolgál.

- Virtuális állapotok esetében biztosítja a sejtter globális állapotának *állandó ciklikus átmenetét*, vagyis a természetes ingadozás modellezését.
- Valós állapotok esetében biztosítja a helyszínek támadás alatti és azt követő (kívánatos vagy célravezető) viselkedésének és a védekezési folyamatnak a modellezését.

Ha egy állapot-átmenet szomszédos sejtek kölcsönhatása folytán megvalósul, akkor a következő típusok egyike lehet. Elsőnek a változó sejt kiinduló állapotát, azután zárójelben a befolyásoló szomszéd sejt állapotát, majd a változó sejt végállapotát tüntetjük fel. Végül a változás jellege szerepel.

- | | |
|--|---|
| – Reális közsejt (Reális közsejt) Reális közsejt | <i>Fenyegetés, veszélyfokozás</i> |
| – Virtuális közsejt (Reális közsejt) Reális közsejt | <i>Fertőzés, veszélyeztetés</i> |
| – Örsejt (Reális közsejt) Örsejt | <i>Készültségfokozás</i> |
| – Reális közsejt (Virtuális közsejt) Reális közsejt | <i>Fenyegetés</i> |
| – Virtuális közsejt (Virtuális közsejt) Virtuális sejt | <i>Fenyegetés</i> |
| – Örsejt (Virtuális közsejt) Örsejt | <i>Éberségfokozás</i> |
| – Reális közsejt (Örsejt) Virtuális sejt | <i>Fenyegetés virtualizálása</i> |
| – Virtuális közsejt (Örsejt) Virtuális sejt | <i>Éberségfokozás</i> |
| – Örsejt (Örsejt) Örsejt | <i>Ellenőrzésfokozás, készültségfokozás</i> |

PÉLDA: GMO

Az illusztrációs példa tárgya a genetikai módosítással keletkező gyomirtó-tűrő gyomnövény (angolul: Herbicide Tolerant Weed, rövidítve HTW) terjedése elleni védekezés, rehabilitáció. A HTW kockázatának kitűnő elemzését adja (Hayes, 2003).

A gyomirtó-tűrő gyomnövény lényegében a gerilla-stratégiát „követve”, kiszámíthatatlan helyen és ütemben „támad”. Így az ellene való védekezés is olyan, mint egy gerillaháború.

A védekezésben a hálózat-alapú hadviselés elveit követjük: a döntések a megfelelő helyen, a „hadszíntéren”, a támadásra vonatkozó információk birtokában születnek. Ezért a példa jól illusztrálja egy valóságos hadszíntér dinamikáját.

A küzdelem pillanatnyi állásától függően a védekező erők struktúráját (vagyis a védekezési kapacitások földrajzi eloszlását) feláldozzuk a védekezés funkciójának eredményes fenntartása érdekében.

A példa kapcsolódik a közigazgatás korábban említett küzdelmi felfogásához is, hiszen a GMO probléma kezelése hatósági beavatkozást igényel, vagyis az erre alkalmas kapacitás térben és időben megfelelő elosztásának megtervezését annak a célnak megfelelően kell megoldani, hogy a közigazgatás fel tudja számolni a veszélyt, azaz rehabilitálhasson.

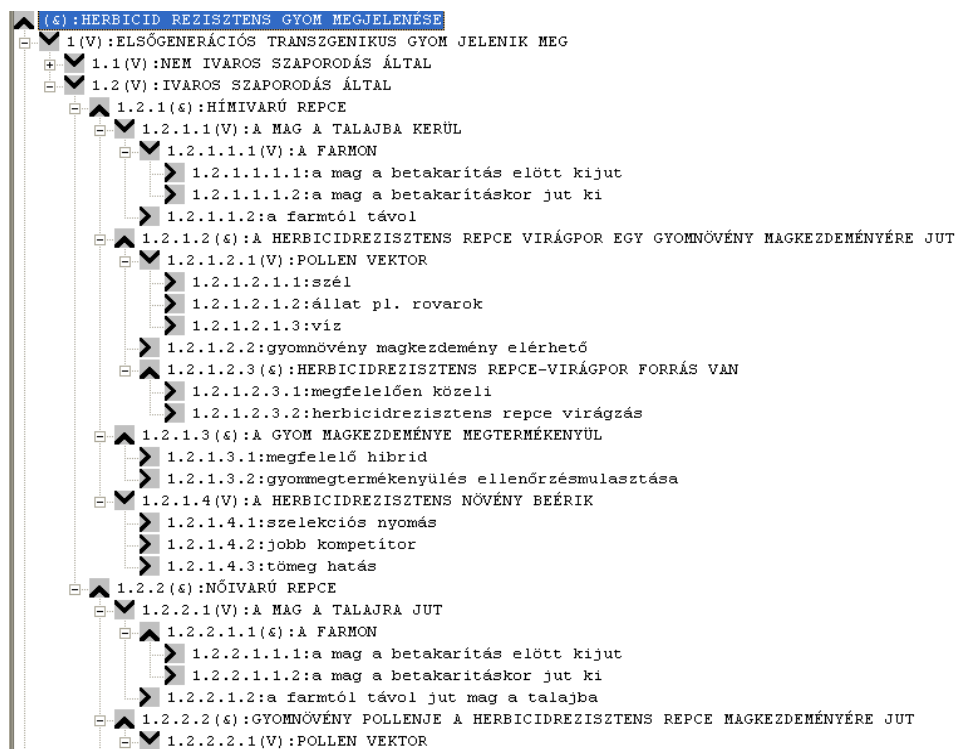
A fentieket a Profes+4 szoftver képernyőképeivel illusztráljuk. (A szoftver a PROFES Környezetbiztonsági Programiroda Kft, <http://www.profes.hu> terméke.)

A hibafa jelölései:

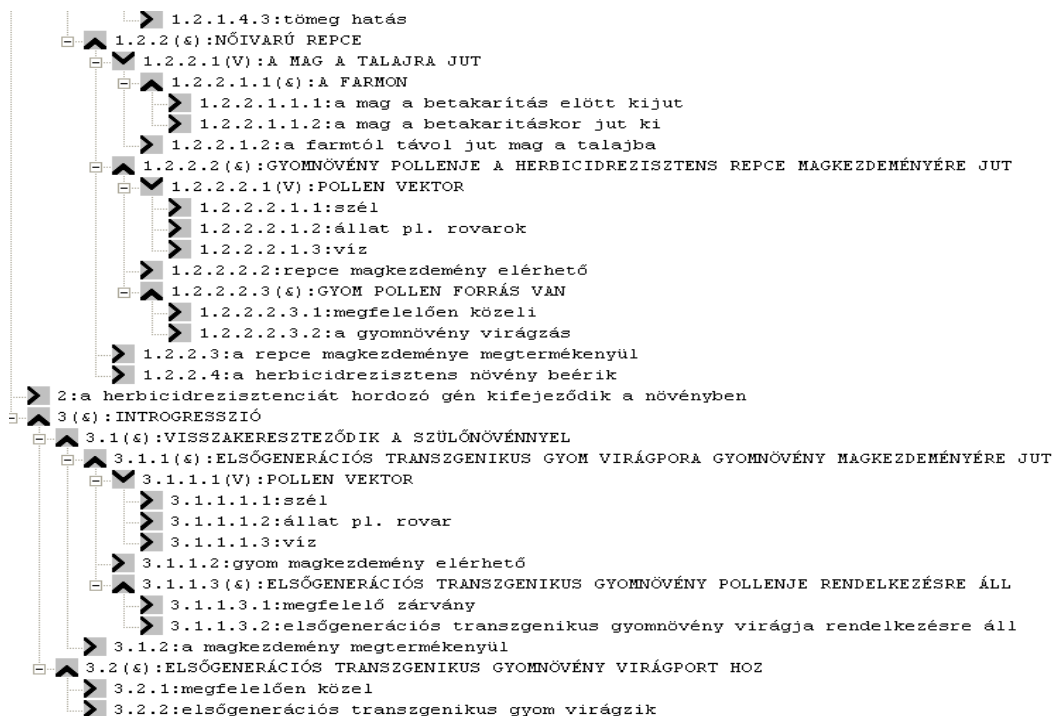
- Az **Λ** és (&) szimbólumok egy összetett esemény sorát jelöli, amelynek kibontása a következő sorokban található. Szóban „és”-nek illetve „et”-nek szokás ejteni.
- A **V** és (V) szimbólum egy összetett esemény sorát jelöli, amelynek kibontása a következő sorokban található. Szóbeli ejtése: „vagy”, a szó megengedő értelmében, tehát mint „legalább az egyik”. Ez nem tévesztendő össze a mindennapi nyelvben használt „kizáró vagy”-gyal, amit a „vagy-vagy” fejez ki.

- A ► szimbólum egy prímesemény sorát jelöli. (Szóbeli ejtésére nincsen kialakult szokás.)
- Az ▲, ▼ és ► szimbólumok mögötti, többnyire pontokkal tagolt számok az események *rendszámai*. Ezek (az események jelentésétől függetlenül) megmutatják, hogy melyik esemény melyiknek a következménye. Ennek akkor van jelentősége, amikor a kockázatelemzőnek titkos anyagból kell dolgoznia.

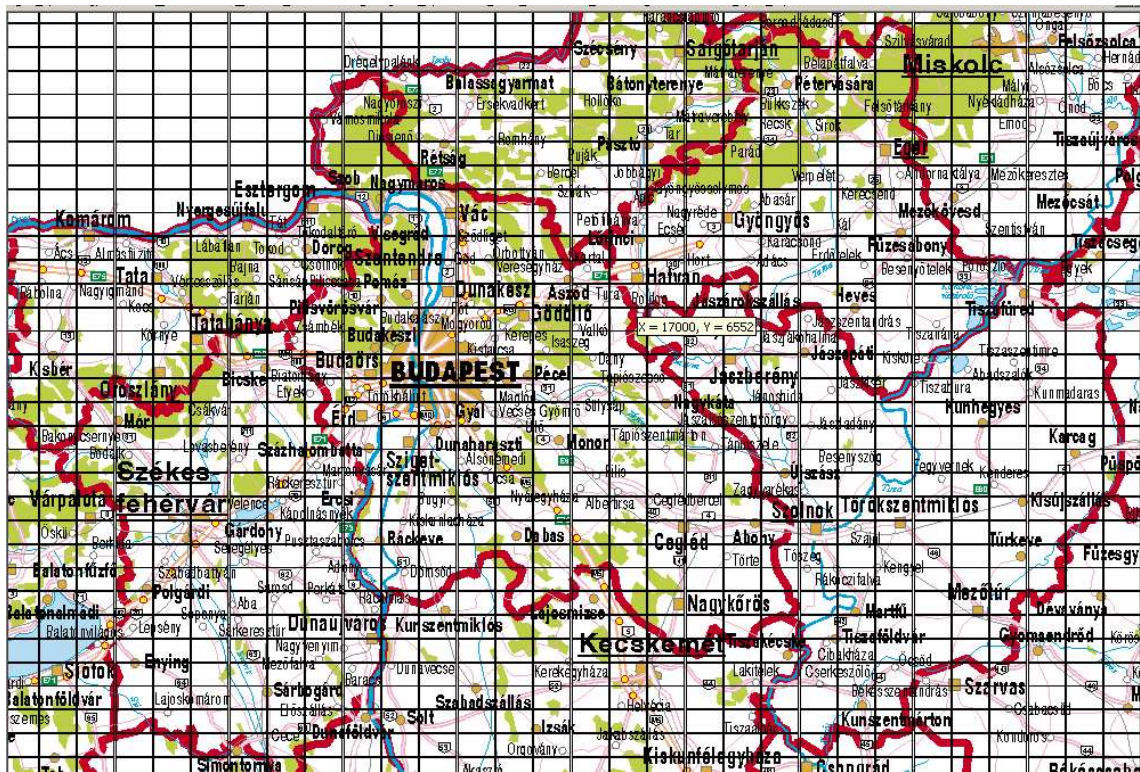
Nézzük először a HT Weed probléma hibafáját, amelyet Hayes (2003) közölt.



1. ábra. A GMO hibafa első része (Profes+4 program képernyőképe)



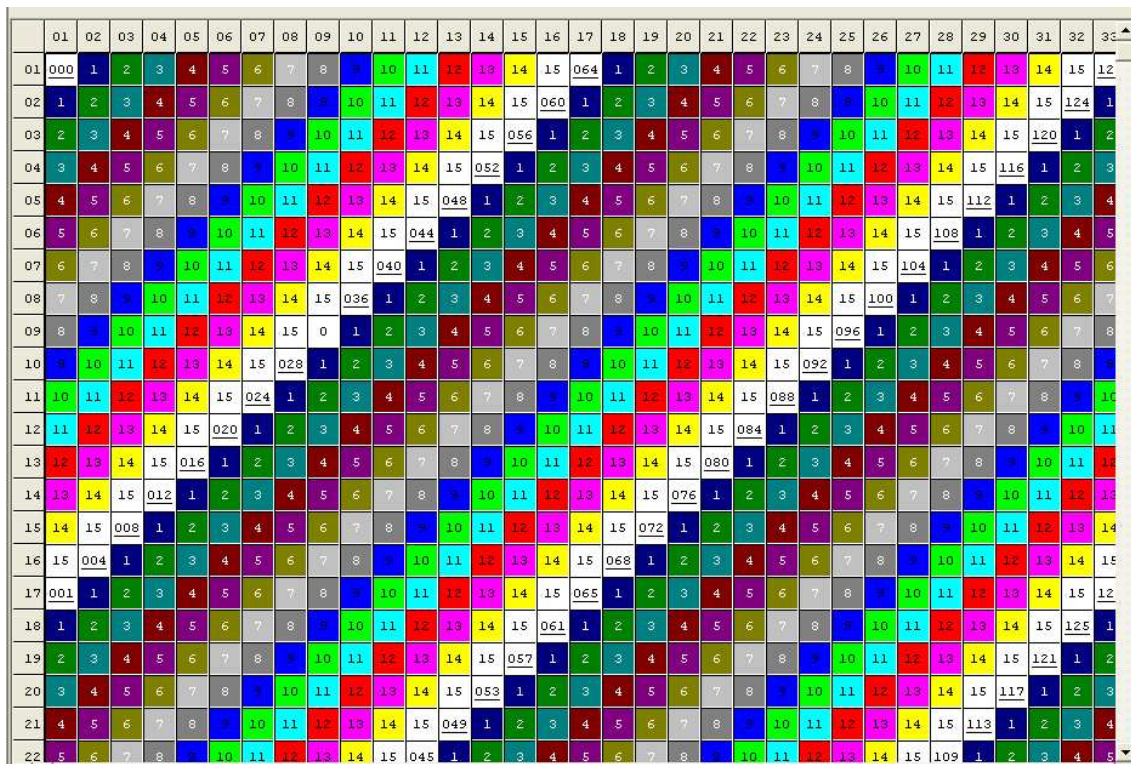
2. ábra. A GMO hibafa második része (Profes+4 program képernyőképe)



3. ábra. Az AIM SORS sejtter egy részlete.

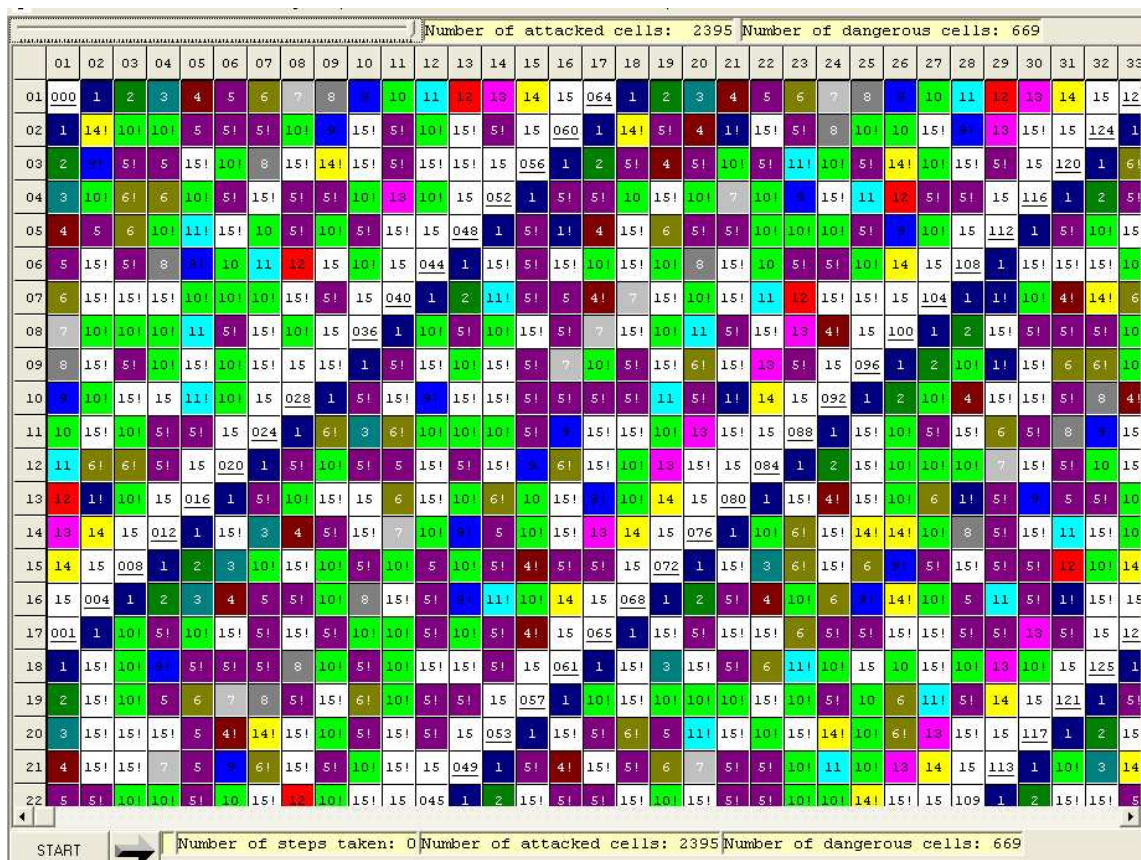
(Dr Zentai László, a térkép készítője engedélyével, <http://lazarus.elte.hu/gb/maps/mo-full.gif>)

A térkép a 2000-es állapotot mutatja. Magyarországot egy $64 \times 64 = 4096$ négyzetből álló négyzetháló fedi le. Minden helyszínhez tartozik egy hibafa. Azonos típusú hibafa tartozhat több helyszínhez is.



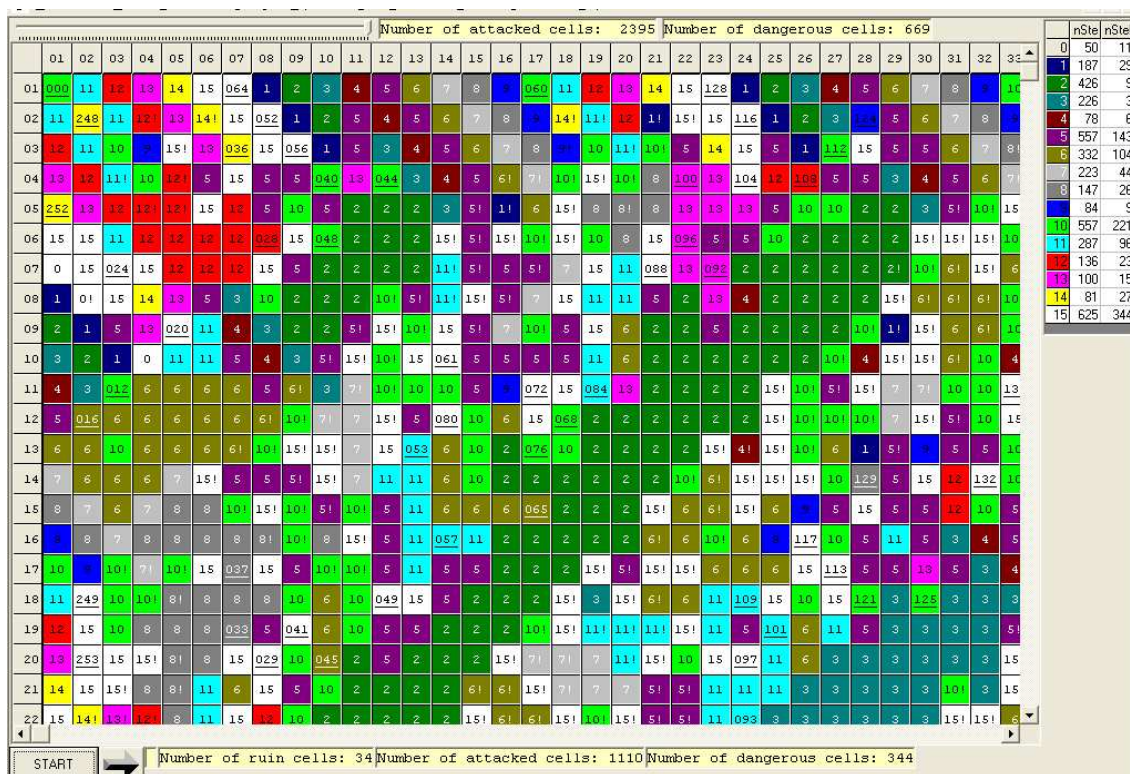
4. ábra. A sejtter eredeti globális állapota.
(Profes+4 program képernyőképe)

Jól látszik a kiinduló struktúra. A sejttér megjelenítő mátrix melléklátloín (balról jobbra felfelé) azonos állapotú sejtek vannak. 254 örsejt van. Az örsejteket aláhízott sorszám jelöli. A 32. sorszám nem szerepel az örsök között. Ennek programozástechnikai oka van.



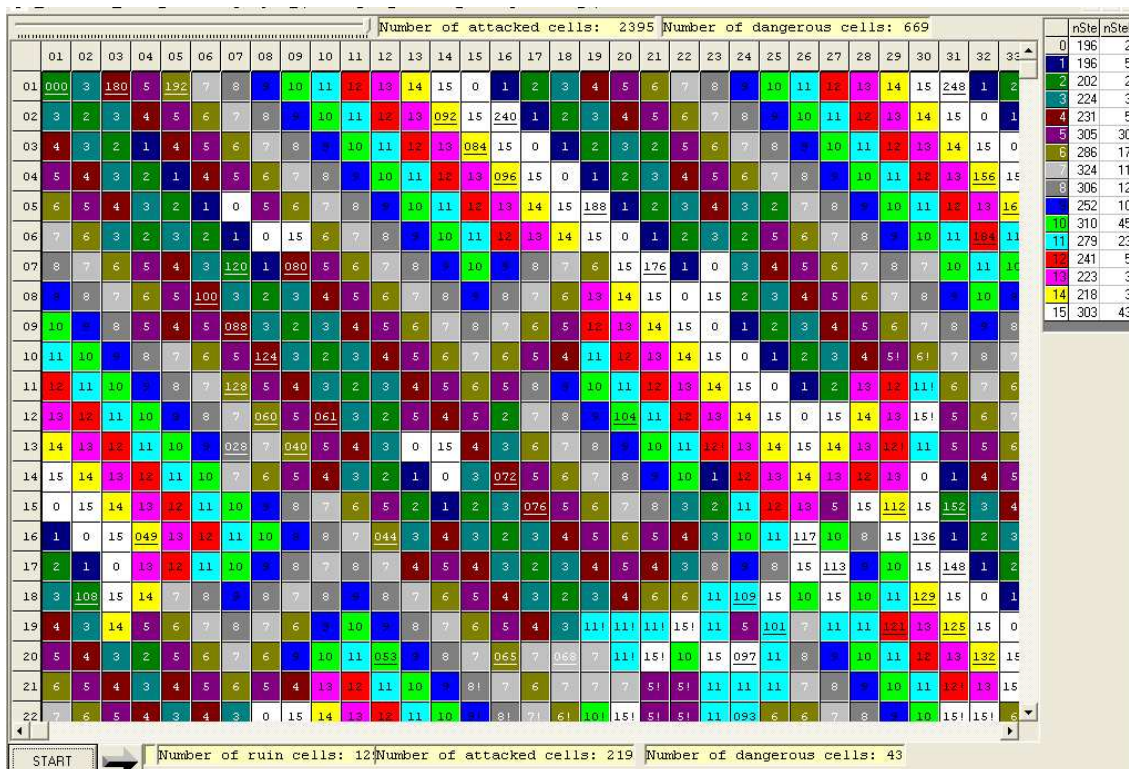
5. ábra. A sejttér közvetlenül a támadás után
(Profes+4 program képernyőképe)

Az eredeti struktúra nyomai alig láthatóak, új struktúra nem látszik. A ! jelzi a megtámadott (attacked) állapotot. Ekkor van aktív prímeseemény, vagyis a főeseemény bekövetkezésének kockázata megnövekedett, de még nem következett be ténylegesen a főeseemény, azaz még nem kelt ki a GMO mag. A 15! állapot a veszélyes (dangerous) sejttálapot, vagyis aktiválódott a főeseemény, kikelt a GMO mag.



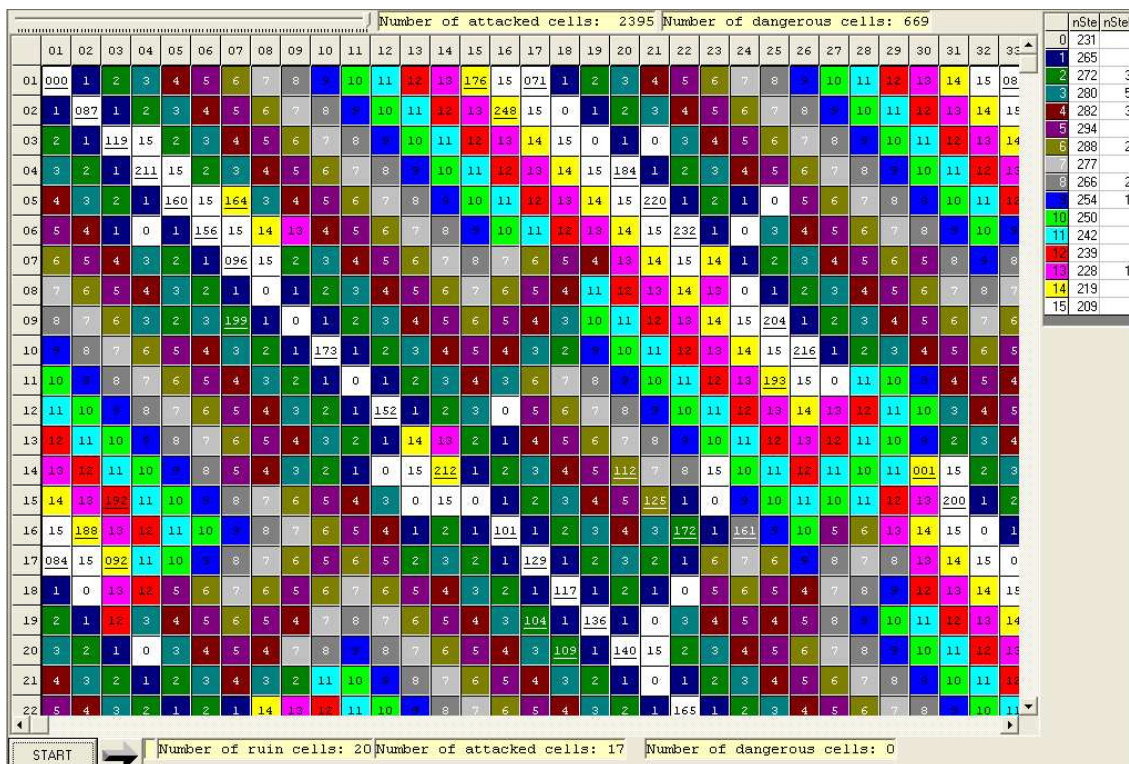
6. ábra. 10 lépés telt el a támadás óta.
(Profes+4 program képernyőképe)

Az eredeti struktúra nyomai még kevésbé látszanak, az új struktúra még egyáltalán nem érzékelhető. A jobboldali dobozban látszik az egyes állapotokban levő sejtek száma, külön a ! száma is. A !-es oszlop a reális állapot, a középső oszlopból a jobboldalit levonva a virtuális. Azonos sorszámú virtuális és reális állapot az átmenetfüggvénynél viselkedik azonosan, más azonosság nincs. A sejtterkép alatti sorban látható a romsejtek (ruin cells) száma. Ezek olyan megtámadott sejtek, amelyeknél a teljes rehabilitáció idő- és pénzigénye csekély.



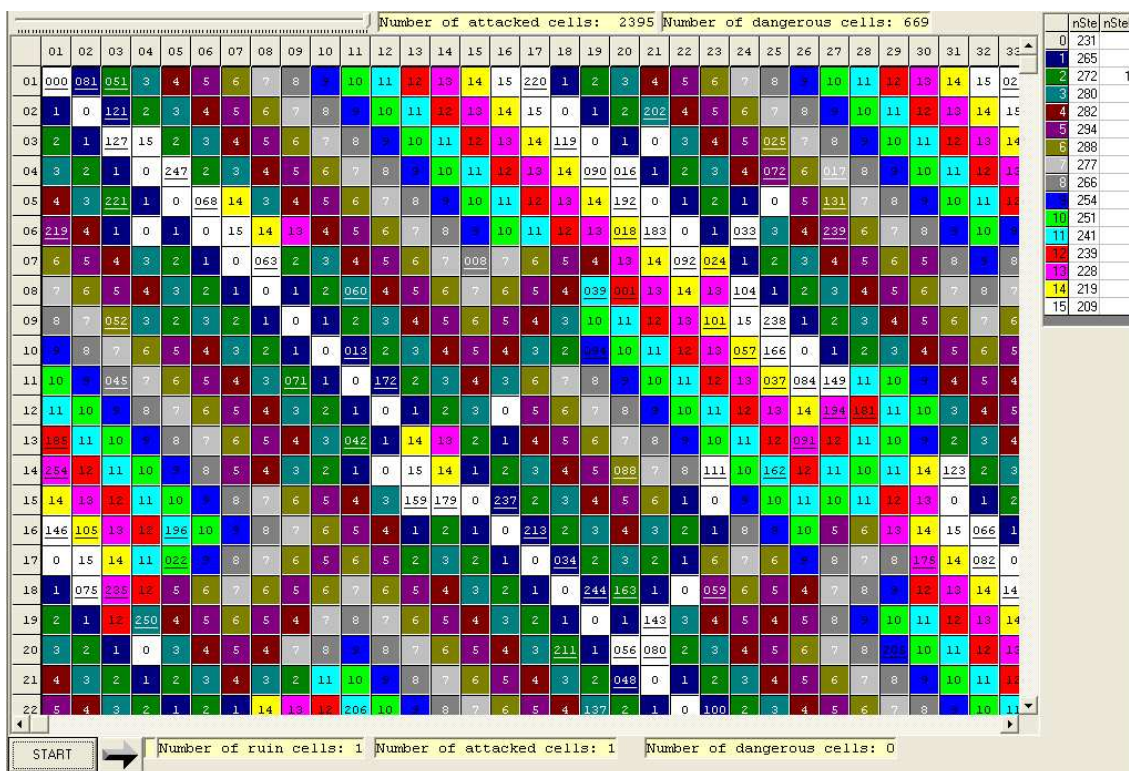
7. ábra. 50 lépés telt el a támadás óta
(Profes+4 program képernyőképe)

A struktúra kezd rendeződni, a sejtér-mátrix főátlóiban (balról jobbra lefelé) jellemzően azonos sejtállapotok jelennek meg. A veszélyes cellák száma erősen lecsökkent.



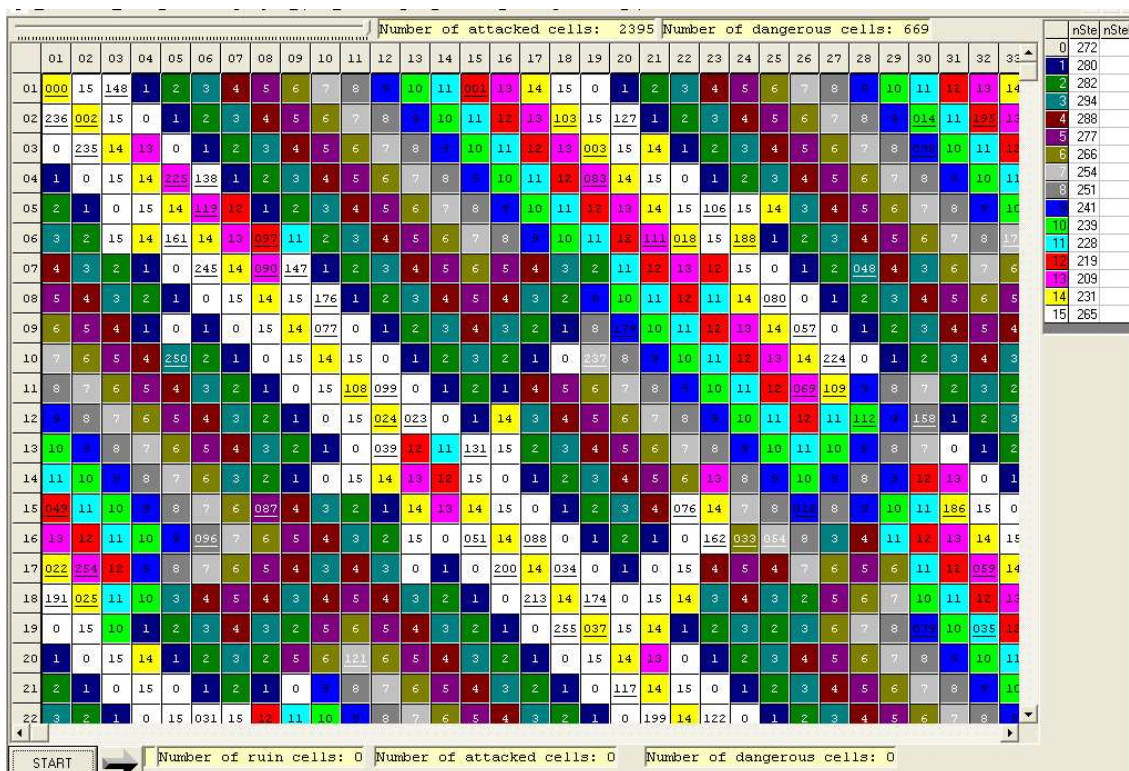
8. ábra. 80 lépés telt el a támadás óta (Profes+4 program képernyőképe)

Még inkább látható az új struktúra. A veszélyes cellák száma 0.



9. ábra. 368 lépés telt el a támadás óta; (Profes+4 program képernyőképe)

Az új struktúra erőteljesen kirajzolódott. Már csak 1 megtámadott sejt van. Csak 1 romsejt van (0 de veszélyes állapot).



10. ábra. 446 lépés telt el a támadás óta; (Profes+4 program képernyőképe)

Lassan, nagyon sok lépésben érte el célját a védekezés, de végül szépen strukturált lett a sejtter. Az őrsők viszont rendszertelenül helyezkednek el. Mindegyik, korábban megtámadott sejt állapota 0, vagyis eltűntek a támadás következményei.

FENNTARTHATÓSÁG

Az eddigiekben tárgyalt AIM-SORS modell két vonatkozásban kapcsolódik a fenntarthatóság problémaköréhez. Ennek vizsgálatához szükség van a fenntarthatóság fogalmának értelmezésére. Bukovics (2007) disszertációjában foglalkozik ezzel a kérdéssel. Megkülönbözteti a mesterséges, ember által létrehozott környezet funkcionális fenntarthatóságát a csak elméletileg létező érintetlen természeti környezet fenntarthatóságától, ami a Római Klub közismert fenntartható fejlődési koncepciója.

A funkcionális fenntarthatóság értelmében arról van szó, hogy a „támadás” után a funkció rehabilitálásra kerül, a „védő” fél funkcionálisan lényegében visszakerül a támadás előtti állapotába, esetleg a struktúra némi változásával. A GMO példában a támadás a gyomirtónak ellenálló gyomok megjelenését jelentette, a funkcionális rehabilitáció ugyanezeknek a gyomoknak a kiirtását, vagyis a korábbi állapot visszaállítását jelenti.

A fenntartható fejlődés elvéhez kapcsolódó értelmezése szerint a fogalom az adott esetben a természetkárosítás felszámolását jelenti. Ennek is teljes mértékben megfelel a tárgyalt modell, hiszen a génmódosuláson átment gyomnövény megjelenése természetkárosítást jelent, és ennek kiküszöbölése éppen a fenntartható fejlődést szolgálja.

A fenntarthatóság fogalmának mindkét értelmezése szerint egy közigazgatási probléma megoldásáról is szó van, hiszen a génmódosult, tehát a szokásos gyomirtási eljárással kezelhetetlen gyomnövény eltüntetése csak szervezett közigazgatási intézkedésekkel lehetséges.

KÖVETKEZTETÉSEK

Az AIM-SORS GMO sejtter eredeti struktúrája megváltozott, új struktúra alakult ki. A védekező szervezet (az őrs sejtek) struktúrája rendezetlenné vált, vagyis az eredeti struktúrát a rendszer feláldozta. Viszont az eredeti funkció (a GMO-mentesség) helyreállítása sikerült, tehát a támadást a rendszer vissza tudta verni.

Olyan, sejtautomatán alapuló védelmi rendszerre látunk példát, amely közvetlen, lépésenkénti emberi beavatkozás nélkül, csak saját működési elvére támaszkodva önvédelmi-öngyógyító képességet, azaz valamiféle intelligenciát képes kifejleszteni és azt alkalmazni.

A MODELL TOVÁBBFEJLESZTÉSI LEHETŐSÉGE

A modell jelenlegi formájában szomszédságként a közvetlen földrajzi szomszédság jellemzőire épít.

A valóságban a mai körülmények között a sejtek földrajzi szomszédság nélkül is könnyen kapcsolatba kerülhetnek egymással, vagyis egy emberi cselek vagy egy természeti jelenség hatása könnyen és gyorsan áterjedhet egyikről a másikra. Példaként gondoljunk egy humán fertőző betegség terjedésére. A „támadás” ebben az esetben egy adott sejtről egy földrajzi értelemben távol fekvő másik sejtre is közvetlenül áterjedhet, hiszen a fertőzést repülőgépen utazó fertőzött utasok vihetik magukkal.

Ezért a szomszédsági viszonyt valamilyen, az egyik sejtről a másikra történő közvetlen (azaz egyszerű és gyors) eljutás lehetőségéhez célszerű kötni, aminek esetleg nincs köze a földrajzi közelséghez.

KITEKINTÉS

Zsigovits (2011) tanulmányában, mint már említettük, teljesen indokoltan a honvédelmi, rendvédelmi és közigazgatási problémák közötti hasonlóságok megkeresésére és ezek kihasználására helyezi a hangsúlyt.

További mérlegelés után azonban józan paraszti ésszel is belátható lényeges különbség mutatkozik e szakterületek között.

Egy katonai jellegű támadást annak közvetlen célpontjában kell elhárítani, és a támadás tovaterjedése esetén is mindig lépéselőnyben van a támadó, hiszen rajta múlik a következő célpont kijelölése.

Közigazgatási jellegű támadás esetében azonban gyakran lehetséges a „támadást” eredeti célpontjától eltéríteni egy olyan új célpontba, amely a védő számára jobban megfelel. Ha például a közigazgatási támadás valamilyen adminisztrációs igény hirtelen, nagy tömegben történő megjelenése, akkor ezeket számítógépes hálózaton keresztül át lehet küldeni az éppen szabad feldolgozó kapacitással rendelkező sejtekbe. Az AIM-SORS modellben ennek az felel meg, hogy a megtámadott sejt a támadást tovább küldheti egy nem, vagy alig támadott sejtbe. Ez az elméletileg csekélynek látszó, de gyakorlatilag létfontosságú különbség jelentheti a modellnek közigazgatási problémákra való alkalmazhatóságát, ugyanakkor rávilágít a szakterületek közötti hasonlóságokra és különbségekre.

Felhasznált irodalom

- [1] Bukovics, I. (2007): A természeti és civilizációs katasztrófák paradigmatisztikus elmélete: MTA doktori értekezés.
- [2] Bukovics, I. (2012): Fenntartható közigazgatás. „A tudomány szerepe a hazai közszolgálat fejlesztésében” tudományos-szakmai konferencia, Nemzeti Közszolgálati Egyetem, Budapest, 2012. november 7.
- [3] Bukovics, I., Fáy, Gy., Kun, I. (2011): Logikai hadviselés – kritikus pontok harca. Hadmérnök, VI. évfolyam 4. szám, 189-203.
- [4] Dahl, R. A. (1947). The Science of Public Administration: Three Problems. Public Administration Review, Winter:1-11.
- [5] Guevara, E. (1998): Guerrilla Warfare (1961) University of Nebraska Press, Lincoln NE.
- [6] Hayes, K. R. (2003): Robust methodologies for ecological risk assessment, Final report: Inductive hazard analysis for GMOs, Centre for Research on Introduced Marine Pests, CSIRO Division of Marine Research, Hobart, Tasmania, Australia.
- [7] Kiss, Á. P. (2011): A negyedik generációs konfliktusok jellemzői és tapasztalatai. Doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem Kossuth Lajos Hadtudományi Kar, Hadtudományi Doktori Iskola, Budapest.
- [8] Mao Tse-tung (1989): On Guerilla Warfare, , US Marine Corps, Quantico VA.
- [9] Taber, R. (1965): The War of the Flea – A Study of Guerilla Warfare Theory and Practice, Paladin, St. Albans.
- [10] Willoughby, W. F. (1927): Principles of Public Administration. Brooking Institution, Washington D.C.
- [11] Zólyomi, Zs. (2011): Magyar harcmodor az Árpád-korban bizánci források alapján, Hadmérnök, VI. évfolyam 1. szám, 320-339.

- [12] Zsigovits, L. (2011): Az új Nemzeti Közszolgálati Egyetem K+F+I és pályázati tevékenységének lehetséges irányai, Hadmérnök, [VI. évfolyam 2. szám, 287-300.](#)

Csuka Antal

antal.csuka@hotmail.com

A FÉNY SZABADTÉRI TERJEDÉSÉNEK ELMÉLETI ÉS GYAKORLATI VIZSGÁLATA

Absztrakt

A továbbiakban a fény terjedésének elméleti és gyakorlati vizsgálatát mutatom be. Nagy hőmérsékletű sugárzók környezetében a levegő törésmutatója véletlenszerűen változik, ami egy könnyen reprodukálható és megfigyelhető jelenség, ellentétben azokkal a természetben előforduló teljes visszaverődéssel kapcsolatos jelenségekkel, amelyek földön vagy vízen figyelhetők meg. A jelenség leírására a törésmutató és a levegő állapotjelzői közt olyan lineáris egyenletek nem használhatók, mint amilyenekkel a geometriai optikában gyakran találkozunk, mert a jelenség téves leírását, vagy alkalmazását eredményezheti. A levegő összetevőinek hatása és a törésmutató megváltozása közti összefüggés feltárását végezhetjük mérésel, gázszenzorok segítségével. Olyan monokromatikus sugárzás, mint amilyen a lézerek által előállított fény terjedésének irányváltozásának meghatározásához jól használhatók a levezetett differenciál egyenletek.

Theoretical and practical study of light propagation in nonlinear media is described. High temperatures and thermal radiation of sources causes random variation of refraction index in optical media. This is an easy notable and reproducible phenomenon compared to most of natural phenomenon visible on land or at sea. A linear relationships used in geometrical optics between the indicators and refraction index of gases may cause improper application and description of studied phenomena. The influence of components on the variation of refraction index can be measured using gas sensors. Using differential equations or functions instead of empirical relation, the deviation of light produced by monochromatic sources such as laser sources can be calculated relatively easy.

Kulcsszavak: optika, lézer, fény refrakció, törésmutató, adatátvitel ~ optics, laser, refraction of light, refraction index, data transmission

BEVEZETÉS

A rádiófrekvenciás sávok telítettsége, ezzel egyidejűleg az RF szennyezettség (poluáció) gyorsuló ütemben nő. A frekvenciasávok túltelítettsége miatt egyre sürgetőbb új műszaki megoldások megtalálása és kidolgozása, amivel az adat-, és információátvitel tovább fejleszthető, sebessége tovább növelhető. Amennyiben a szükséges biztonsági feltételek adottak, vagy megteremthetők a zavartalan kapcsolat kiépítéséhez és fenntartásához, szabadtéri optikai csatorna létesítésével, olyan nagy kapacitású és nagy sávszélességű adatátvitel létesíthető rövid idő alatt és viszonylag egyszerű optikai eszközökkel, amivel biztosíthatók a csapatok és vezetési pontok közti összeköttetés. Biztonsági intézkedések alatt azokat az eljárások, műszaki megoldásokat értem, amelyek ahhoz szükségesek, hogy az információs csatorna lehallgathatatlan legyen. Különféle modulációs és kódvédelmi eljárások mellett szükség lehet a szabadtéri optikai forrás elrejtésére, álcázására. [1] Ott, ahol lehallgató berendezések folyamatosan pásztázzák, kémlelik a rádiófrekvenciás hullámok tartományát, egy kis nyílásszöggel sugárzó középteljesítményű infra-lézerforrással, kedvező időjárási viszonyok közepette, de még akár gyenge ködben is, olyan optikai csatorna létesíthető, amire az ellenfél nem biztos, hogy azonnal felfigyel.[2]

A hadviselés történetében leleményes megoldásokra több olyan példát is találunk, amikor meglepően egyszerű eszközökkel, megoldások egész sorával a veszteségeket hatékonyan sikerült csökkenteni, emberéletet és technikai eszközöket megvédeni a pusztulástól, megsemmisítéstől. [3]

A fényvezetéssel kapcsolatos első megfigyelések és alkalmazásuk első kísérletei az 1800-as évek közepén kezdődtek. A korabeli kísérleteknek eredményeire alapozottan fejlődött a vezetékes optikai adatátvitel azzá, amilyennek ma azt ismerjük. A fény szabadtéri terjedésével kapcsolatos jelenségek megfigyelések és reprodukálásának hasonlóképpen több száz éves múltja van, de a szabadtéri adat-, és információátvitel ezzel szemben közel sem fejlődött olyan ütemben, mint a vezetékes. Ennek oka az, hogy az a közeg, amelyben a fény terjed, a Föld légköre, és az azt alkotó levegő egy olyan gázelegy, ami jellemzően egy inhomogén, kaotikusan változó, nemlineáris és anizotróp közeg. Szabad térben ennek a gázhalmazállapotú közegnek a jellemzői és állapotjelzői folyamatosan változnak, stabilitása úgy semmiképpen sem biztosítható, mint az optikai szálhoz hasonló szilárd halmazállapotú közeg esetében. A fényforrások fejlődésének ellenére a kommunikációnak ez a formája nem fejlődött, néhány kísérlet és egyedi alkalmazástól eltekintve, háttérbe szorult. Több mint fél évszázad telt el az óta, amióta az ember leküzdve a Föld gravitációs terét, kilépett abból és Föld körüli pályára állította a műholdjait. A Föld légkörét elhagyva, egyáltalán nem, vagy csak kisebb mértékben kell számolnia annak zavaró hatásával megbízhatóbb kapcsolat létesíthető, mint a földfelszín közelében. [4]

A lézerforrások a múlt század hetvenes éveitől kezdődően megtalálhatók különféle mérő-, és diagnosztikai eszközökben. Gyors ütemű fejlődésüknek köszönhetően a nagyteljesítményű változataik fegyver célú alkalmazásán túlmenően, felhasználhatók szabadtéri optikai átvitel létesítésére is. Amennyiben a lézerfény közegjellemzőkre gyakorolt hatása és terjedésének minden részletét sikerül tisztázni, elháríthatók azok az akadályokat, amelyek korábban a felhasználását, felhasználásának kiterjesztését és bővítését akadályozták.

A FÉNY LÉGKÖRI REFRAKCIÓJA

A fény légköri refrakcióját olyan egyszerűen megfigyelhető és ismert jelenségek igazolják, mint a fény teljes visszaverődése különböző hőmérsékletű vagy összetételű légrétegek határfelületéről, a délibáb, a látóhatár fölé emelkedő napkorong torzulása, a csillagok fényerejének periodikus változása, stb. A fény refrakciója egy érdekes hétköznapi, mondhatni mindennapos jelenség, ha a Nap felkeltére gondolunk, aminek első sugarait már akkor láthatjuk, amikor az még a látóhatár alatt van. Ez csak néhány példa mindazok közül, amelyeket a természetben szabad szemmel is megfigyelhetünk, amennyiben a jelenség létrejöttéhez szükséges feltételek adottak és a megfigyelés körülményei is kedvezőek. Mindemellett léteznek olyan refrakcióval kapcsolatos jelenségek is, amelyek csak mérőműszerekkel vizsgálhatók. Sajnálatos tény, hogy ezeknek a jelenségeknek a legnagyobb része nehezen, vagy csak kiegészítő, erre a célra kifejlesztett optikai eszközökkel, rögzíthetők, fényképezhetők. Ennek oka a légkör törésmutatója és állapotváltozása közti bonyolult függvénykapcsolat, amihez az is hozzájárul, hogy a levegő, mint optikai közeg és az emberi szem alkotja optikai rendszer és képrögzítő eszközök optikai rendszere (objektívje) közt alapvető különbségek vannak. [5]

Egy olyan kaotikusan változó közegben, mint amilyen a Föld légköre, az abban zajló folyamatok leírásánál gyakran találkozunk a geometriai optikában megszokott egyszerűsítésekkel és lineáris egyenletekkel, ami miatt okkal merül fel a kérdés, hogy azok vajon mennyire pontosak és megbízhatóak. Összetett folyamatok leírásánál, modellezésénél csak az egyszerűsítések vezetnek eredményre, hiszen a természetben zajló összetett folyamatok leírására szolgáló differenciál egyenleteink nagy része megoldhatatlan. A hő és áramlástanban tapasztalati összefüggések egész sorát kénytelenek vagyunk használni. Ott ahol lehetőség van rá, törekednünk kell arra, hogy minél pontosabb összefüggéseket nyerjünk. Amennyiben a fény refrakciójának vizsgálatát ki szeretnénk terjeszteni az ok-okozati összefüggések feltárására, mert többre vagyunk kíváncsiak, mint magára a jelenségre és annak egyszerűsített leírására, akkor olyan összefüggésekre van szükségünk, amelyekből a jelenség további vizsgálatához és eszközfejlesztésekhez szükséges adatok nyerhetők. Differenciálgeometriai módszerek felhasználásával levezethetők olyan egyenletek, megalkothatók olyan függvények, függvénykapcsolatok, amelyek esetenként kifejezőbbek és pontosabban írnak le egy jelenséget, vagy folyamatot. Ha erre nincs lehetőség, akkor mérések elvégzésével tapasztalati (empirikus) összefüggéseket kell alkotni. Az utóbbiak pontosságát viszont bizonyos időközönként ellenőrizni kell. A Föld légkörében lejátszódó folyamatok részben az emberi jelenlét, tevékenység és beavatkozás következtében, de sok más tényező hatására is, idővel megváltoznak. Ennek több jele is van és mérések egész sora igazolja, hogy több olyan állapotjelzőhöz kapcsolódó állandót is ismerünk, aminek értéke valójában nem állandó. Egy ilyenre példa a levegő hőegyenértéke, ami földrajzi helyhez kötött ugyan, de aminek értéke idővel megváltozik (pl. a légkör felmelegedésének hatására). Következménye a termikus gradiens értékének folyamatos csökkenése. [6]

GÁZOK TÖRÉSMUTATÓJÁNAK MEGVÁLTOZÁSA MAGAS HŐMÉRSÉKLETEN

A törésmutató megváltozásával kapcsolatos olyan jelenségek, amelyek többnyire magas hőmérsékleten jelentkeznek, könnyebben előállíthatók (reprodukálhatók) és gyakrabban figyelhetők meg, mint azok, amelyekről korábban szó volt és a természetben fordulnak elő. Erre egy szemléletes példa az 1. ábrán látható.

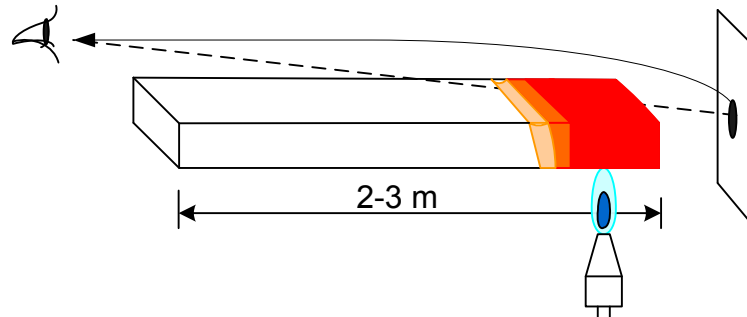


Mikoyan-Gurevich MiG-29OVT

1. kép. A repülőgép hajtóműből kiáramló meleg hatása [7]

A repülőgép hajtóművéből kilépő rendkívül magas hőmérsékletű gázok ($600 - 800^{\circ}\text{C}$) a környező levegő sűrűségét megváltoztatják. [8] A gázok sűrűsége eleve jóval kisebb, mint a környező levegőé. A háttérből, a képrögzítőbe érkező fénysugarak az alacsony sűrűségű térrészen áthaladva irányváltozást szenvednek. Magas hőmérséklet és turbulens áramlások a gázelegyet inhomogénné teszik, aminek a következtében az egyes térrészekben áthaladó és onnan kilépő elemi fénysugarak, az eltérő és folyamatosan változó törésmutató miatt nem maradnak párhuzamosak, a gáz áttetsző képessége (transzparenciája) csökken, aminek következtében a háttérkép elmosódottá válik. A törésmutató ilyen mértékű megváltozása akkor következik be, amikor a levegő (gáz) állapotjelzői (hőmérséklete, nyomása, sűrűsége, stb.) nagymértékben megváltozik. A jelenség megfigyelhető és előállítható jóval egyszerűbb eszközökkel is. Amennyiben a sugárhajtóműhöz hasonlóan, egy tárgy környezetében a felhevített levegő a törésmutató megváltozását idézi elő, akkor az hasonlóképpen jól megfigyelhető és vizsgálható, mint ahogy az 1. képen látható. Az ehhez szükséges kísérleti eszköz egyszerűsített vázlata az 1. ábrán látható. Egy hosszú fémtárgy, például egy rúd, vagy zártszelvény izzásig felhevített végének ($\text{kb. } 900^{\circ}\text{C}$) környezetében a levegő törésmutatójának olyan helyi (lokális) megváltozása következik be, ami a takarásban levő háttérkép eltolódásának egyszerű megfigyelését és vizsgálatát teszi lehetővé. Az ábrán látható ernyő és a rajta levő folt csak illusztráció. A törésmutató megváltozásának hatására a képen látható mértékű háttérkép eltolódást nem fogunk tapasztalni, ilyen megoldással ne is kísérletezzünk! Ez egy eltúlzott vázlat, ami a jelenség magyarázatára alkalmas. Ennél jóval finomabb felbontású háttérképre van szükségünk, például egy érdes felület, vagy köporral szórt falfelület. Ha az egyik szemünket behunyva, a másikkal a hosszú tárgy felülete mentén a háttérképre fókuszálunk, a háttérbe nem illeszkedő kép láthatóvá válik. Az elvi vázlatot

felhasználva megtervezhető olyan mérőeszköz, aminek segítségével a jelenség magas hőmérsékleten vizsgálható. A szemünk érzékenysége és felbontóképessége kellően nagy ahhoz, hogy a jelenséget megfigyeljük, de az említett háttérképben történő változásokat digitális fényképezőgéppel nem sikerült rögzíteni.



1. ábra. (A szerző rajza)

A FÉNYTERJEDÉS IRÁNYVÁLTOZÁSA GÁZHALMAZÁLLAPOTÚ KÖZEGBEN

Olyan egyszerű alapösszefüggésekből kiindulva, mint a Biot-Arago-Lorenz-, és Snellius-Descartes törvények:

$$\frac{n-1}{n_0-1} = \frac{p}{p_0} \cdot \frac{T_0}{T} = \frac{\rho}{\rho_0}, [9]$$

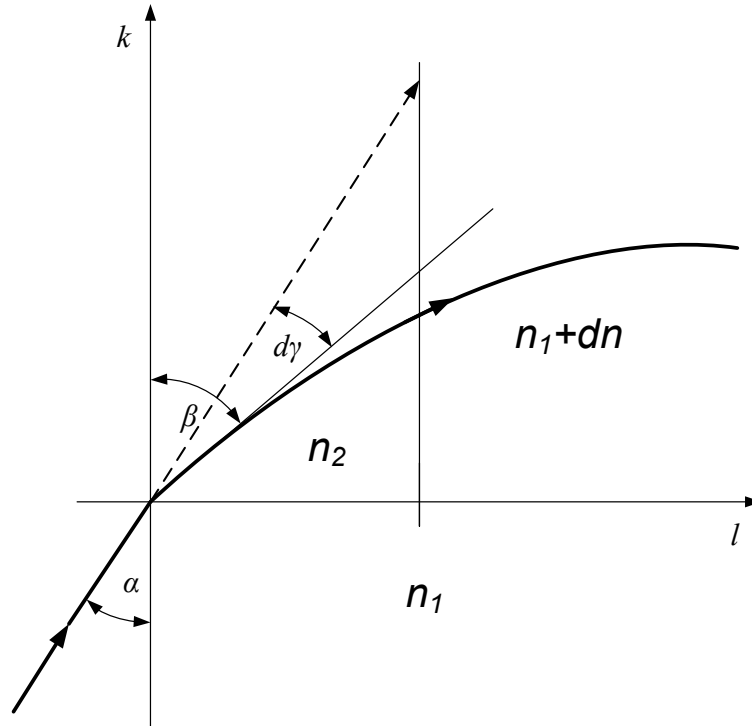
$$\frac{n_2}{n_1} = \frac{\sin \alpha}{\sin \beta}, [10] \quad (1)$$

levezethető az a differenciálfüggvény, amely pontosan leírja az inhomogén közegen áthaladó fénysugár $d\gamma$ szögeltérését, amint az a 2. ábrán látható.

Legyen a vizsgált gáznak n a törésmutatója, p a nyomása, T a hőmérséklete és ρ a sűrűsége, továbbá α és β a belépő és kilépő fénysugár a határfelület normálisával bezárt szöge,

Amennyiben monokromatikus zöld színű fényforrást használunk és veszünk alapul:

$$n_0 - 1 = 294 \cdot 10^{-6} [9]$$



2. ábra. (A szerző rajza)

Az (1)-be történő behelyettesítés és kiemelés után:

$$\sin \alpha = \frac{n_2}{n_1} (\sin \alpha + d\gamma \cdot \cos \alpha)$$

$$d\gamma \cdot \cos \alpha = \frac{\sin \alpha - \frac{n_2}{n_1} \cdot \sin \alpha}{\frac{n_2}{n_1}} = \left(\frac{n_1 - n_2}{n_1} \right) \cdot \sin \alpha,$$

A törésmutató megváltozását parciális differenciállal kifejezve:

$$n_1 - n_2 = \frac{\partial n}{\partial l} \cdot dl.$$

$$d\gamma \cdot \cos \alpha = \left(\frac{\frac{\partial n}{\partial l} \cdot dl}{n_1} \right) \cdot \sin \alpha = \left(\frac{\partial n}{n_1 \cdot \partial l} dl \right) \cdot \sin \alpha.$$

A hullám terjedésének irányszögének megváltozása a 2. ábrán látható koordinátarendszer l –el jelölt vízszintes tengelyének mentén:

$$d\gamma = \frac{\partial n}{\partial l} \cdot \operatorname{tg} \alpha \cdot \frac{l}{n_1} \cdot dl,$$

$\frac{\partial l}{\partial k} = \partial \operatorname{tg} \alpha = \frac{l}{\cos^2 \alpha}$ felhasználásával, és a láncszabály bevezetésével megkapjuk a törésmutató megváltozását a k tengely mentén:

$$\frac{\partial n}{\partial k} = \frac{\partial n}{\partial l} \cdot \frac{l}{\cos^2 \alpha}$$

Gázhalmazállapotú közeg esetében a törésmutató és a sűrűség közt az alábbi összefüggés írható fel:

$$n - 1 = (n_0 - 1) \frac{\rho}{3\rho_0} \left[1 - \frac{2}{3} (n_0 - 1) \left(1 - \frac{\rho}{\rho_0} \right) \right], [11]$$

A Michelson kísérletnél, fehér fény esetében meghatározott érték ($n=1,000225$). [10]

Normál állapotú levegőnél ($t = 20^\circ \text{C}$, $p = 1,013 \cdot 10^5 \text{ Pa}$), a törésmutatót $n=1,0003$ -nak szokás venni. Az inhomogén közeg határára érkező fénysugár szögeltérésére a következő parciális differenciál függvényt kapjuk abban az esetben, ha $\sin \alpha \cos \alpha \equiv \frac{\sin 2\alpha}{2} \approx \alpha - \frac{2\alpha^3}{3} \approx \alpha$, és lineáris közelítéskor $0 - 25^\circ$ -ig a relatív hiba 14% alatt marad:

$$d\gamma \approx \frac{(n_0 - 1) \left[1 + \frac{2(n_0 - 1)}{3\rho_0} \cdot (2\rho - \rho_0) \right] \cdot \frac{\partial \rho}{\partial k}}{3\rho_0 + (n_0 - 1)\rho \left[1 - \frac{2}{3} (n_0 - 1) \left(1 - \frac{\rho}{\rho_0} \right) \right]} \cdot \left(\alpha - \frac{2\alpha^3}{3} \right) dl \approx \frac{n_0 - 1}{3\rho_0} \left[1 + \frac{2(n_0 - 1)}{3\rho_0} \cdot (2\rho - \rho_0) \right] \cdot \frac{\partial \rho}{\partial k} \cdot \alpha dl$$

A γ szög megváltozását a k tengely irányában a sűrűség befolyásolja, a szög a dl -től, mint függő változótól függően egy négyzetes, parabolikus függvény szerint változik, úgy ahogy azt az a 2. ábrán vastag vonallal jelöltem.

A kapott függvény esetében alapul véve az $n = 1 + 0,000294 \cdot \frac{\rho}{\rho_0}$ (Biot–Arago–Lorenz törvényt), láthatjuk, hogy a k tengely mentén nagy sűrűségváltozás ($\frac{\partial \rho}{\partial k}$ - sűrűség gradiens) is csak nagyon kis γ szögeltérést eredményez.

A TÖRÉSMUTATÓ ÉS A GÁZÖSSZETÉTEL KAPCSOLATA

A levegő egy olyan gázkeverék, aminek az összetétele ismert és viszonylag állandónak tekinthető. Jellemzője, hogy a legtöbb összetevő százalékos aránya csak kismértékben változik az állapotjelzők megváltozásának hatására. Hő közléssel a levegő hőmérséklete és térfogata növekszik, sűrűsége csökken, törésmutatója a következő függvény szerint változik:

$$n - 1 = \frac{p}{101,32472} \cdot 10^{-3} \cdot \left(\frac{0,0002923}{1 + 0,00368 \cdot t} + 0,0000016 \cdot k \right) - 0,0004041 \cdot \frac{e}{760} \quad (2)$$

ahol; n - a levegő törésmutatója, t - hőmérséklete, p - nyomása, e - a páratartalom, és k - a szén-dioxid tartalom százalékos aránya. A nyomást a továbbiakban p -vel jelölöm. Az (1)-el jelölt összefüggést megjelölt forrásból átvett függvény átrendezésével,- és kiemeléssel kaptam. [5]

Az állapotjelzők, gázösszetevők hatását a függvény parciális differenciálásából nyert parciális differenciálegyenletből kapjuk. Az (2)-ből, a hőmérséklet szerinti parciális derivált a következő:

$$\frac{\partial n}{\partial t} = -0,7839 \cdot \frac{p}{t^2} \cdot 10^{-6},$$

A törésmutató nyomás szerinti parciális deriváltja:

$$\frac{\partial n}{\partial p} = \left(2,8848 + \frac{783,8858}{t} + 0,0158 \cdot k \right) \cdot 10^{-9} \quad (3)$$

ahol; p - a levegő nyomása Pa -ban,
 t - a hőmérséklete °C -ban,
 k – a széndioxid tartalom százalékos aránya.

Amikor a Föld légkörében, mint optikai közegben, olyan fényterjedéssel kapcsolatos jelenségeket vizsgálunk, amelyek a törésmutató megváltozásával valamiképpen összefüggnek, annak széndioxid tartalmának százalékos arányát és hőmérsékletét nem hagyhatjuk figyelmen kívül, azt mérni vagy számolni kell. Ilyen jelenség a fény terjedésének irányváltozása, azaz refrakciója is. Kézenfekvő megoldásnak tűnik tehát, hogy amennyiben a fény refrakcióját, avagy terjedésének irányváltozását szeretnénk meghatározni számítással és méréssel a hőmérsékletet, vagy a gáz komponenseinek, összetevőinek arányát vegyük figyelembe, vagy változtassuk meg.

Az általánosan elfogadott összetétel szerint a széndioxid koncentráció átlagosan 3000-7000ppm közt változik. Ezzel szemben a szénmonoxid aránya alig több, mint 20ppm-nek felel meg. A nitrogén - 78,084, az oxigén - 20,95, az argon - 0,93 térfogatszázaléknak megfelelő arányban van jelen a levegőben. Az utóbbiak kiugróan magas aránya annak téves látszatát keltheti, hogy inkább ezek arányát kellene vizsgálni, akkor, amikor a törésmutató mérését

szeretnénk elvégezni, vagy erre alkalmas mérési eljárást szeretnénk kidolgozni. Függetlenül, attól, hogy milyen térfogatarányban fordulnak elő az egyes összetevők, egyáltalán nem biztos, hogy a magasabb százalékarányt képviselő gázösszetevőt kell alapul venni, annak arányát vizsgálni és mérésére eljárást, módszert kidolgozni. Mindig az a gázösszetevő, avagy komponens, a meghatározó, amelyik megváltozása nagyobb hatással van a vizsgált jellemzőkre. Nem utolsó szempont az érzékelők mérési tartománya és linearitása sem. Ma alig van olyan egy, vagy kétatomos gáz, aminek a vizsgálatára ne lenne könnyen beszerezhető szenzor. [12] Az árak tekintetében nagyon nagyok lehetnek a különbségek. A levegőt alkotó gázok százalékos aránya és a mérésére alkalmas szenzorok árai közt nehéz felismerni valamilyen kapcsolatot. Míg egy szénmonoxid szenzor ára néhány ezer forint, addig egy széndioxid szenzor ára több tízezer forint is lehet. Ha a fényterjedés irányváltozásával kapcsolatos méréseket végezzük és az optikai közeg a levegő, akkor a (3) differenciálegyenlet figyelembevételével a levegő széndioxid tartalmának mérésére külön eljárást kell kidolgozni. A másik összetevő az oxigén, aminek megváltozását érdemes vizsgálni. A mérésére gyártott szenzorok ára magas, de érdekes összefüggések feltárásához járulhat hozzá.

ÖSSZEFOGLALÁS

A lézerforrások fejlődésével egyre több olyan alkalmazásról tudunk, ahol ezek a monokromatikus, koherens hullám-, és energiaforrásoknak egyre nagyobb szerepe van, legyen az irányított energiájú fegyver, vagy egy vegyi támadást ért terület biztonságos távolságból végzett vegyelemzése, lézerforrást használó mérőműszer segítségével. A fény légköri terjedésben bekövetkező hibák és pontatlanságok, ma még nem minden eszköz működésében okoznak számottevő hibát. Olyan nagy pontosságú mérések esetében azonban, ahol a fény hullámhosszával, vagy atomok-, molekulák méretével összemérhető eltérések a mérési eredményeket meghamisítják, a pontosságnak nagyon nagy szerepe van.

Az ismertetett összefüggések segítségével számolhatók a várható hibák, kidolgozhatók azok a mérési eljárások és megalkothatók azok a pontos mérőműszerek, amelyekkel tovább vizsgálható a jelenség és további összefüggések tárhatók fel.

Felhasznált irodalom

- [1] Csuka Antal.: Információvédelem, merre tovább?, ZMNE Kommunikáció 2008 Konferencia kiadványa 2008 október 7., ISBN 978-963-7060-57-1
- [2] Haig Zsolt- Kovács László- Makkay Imre- Seebauer Imre- Vass Sándor- Ványa László: Az információs társadalom veszélyforrásai, A kormányzat szerepe a védelem és ellentétekenység műszaki és szervezeti megoldásaiban, Tanulmány. MEH Informatikai Kormánybiztosság, 2002- Magyar Narancs- URL: <http://www.manacs.hu/index.php?gcPage=/Public/hirek/hir.php&id=14820>; (letöltve 2007.június 30.)
- [3] Bokor Imre: Rádióelektronikai harc korunk háborúiban, Zrínyi Katonai Kiadó, Budapest, 1989, 5-146 pp.
- [4] URL: <http://www.origo.hu/tudomany/20070216lezeres.html>; (letöltve: 2012.12.13)
- [5] Csuka Antal: A Föld légkörének hatása a lézernyaláb terjedésére és a továbbított fénytjeljesítményre, Szolnoki Tudományos Közlemények XV., 2011. nov. 10. URL: http://www.szolnok.mtesz.hu/sztk/kulonszamok/2011/cikkek/Csuka_Antal.pdf; (2012.07.01) ISSN 2060-3002,
- [6] Monks P.S.-Garnier C.: Atmospheric Composition Change-Global and regional air quality, Atmospheric Environment, 43, 5268-5350 (2009),

- [7] URL: <http://www.slideshare.net/inexplicable/russian-air-show-2007#btnNext>;
(2012.12.10)
- [8] URL: http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles6/vass_rw6.pdf;
- [9] Dr. Grúber J.-Ifj. Szentmártony T: Gázdinamika, Tankönyvkiadó, Budapest, 1952, pp 90-91
- [10] Dr. Ábrahám Gy.: Optika; Panem Kft kiadó Budapest, 1997; ISBN 963 545 144 X; p 26,29, 286, 292,
- [11] Prof.rer.nat.habil.W. Brunner: Wissenspeicher Lasertechnik, VEB Fachbuchverlag Leipzig, 1982, 28-29pp,
- [12] URL:
<http://www.figaro.co.jp/en/product/index.php?mode=search&kbn=1&type=30&id=213080>; (2012.12.10)

VII. Évfolyam 4. szám - 2012. december

Fleiner Rita - Munk Sándor

fleiner.rita@nik.uni-obuda.hu - munk.sandor@zmne.hu

KÖZIGAZGATÁSI ADATBÁZISOK ÖSSZEKAPCSOLÁSÁNAK BIZTONSÁGI KÉRDÉSEI

Absztrakt

Az államigazgatási szerveknek kötelessége a gazdaságra és a társadalmi folyamatokra kiható döntéseiket előzetesen mérlegelni és eredményeiket utólagosan vizsgálni. A költségvetési szervek által létrehozott adatbázisok nem csak adminisztratív célokra, hanem elemzések, hatásvizsgálatok és döntés előkészítés céljára is alkalmazandók. A vizsgálatokhoz szükség lehet a különböző adatbázisokból származó adatok együttes kezelésére, az adatbázisok összekapcsolására. A publikációban a közigazgatási adatbázisok összekapcsolásának biztonsági kérdéseit vizsgáljuk. Ennek keretében feltárjuk a közigazgatási adatbázisok összekapcsolásának szükségességét és célját, elemezzük az adatbázisok összekapcsolásának jogi és technikai korlátait, problémáit és bemutatjuk az összekapcsolást érintő magyarországi törvényi szabályozást.

It is the duty of the government to consider their decisions influencing the economy and the social processes beforehand and to examine their results posteriorly. Databases created by government agencies can be used not only for administrative purposes, but also for analyses, impact assessments and decision making processes. These examinations may need joint data from different databases, so the connection of databases must be performed. In the publication we examine the security aspects of connecting administrative databases. In this framework we reveal the necessity and the objective of connecting administrative databases, we analyse the legal and technical limitations and we present the Hungarian legal regulations concerning this issue.

Kulcsszavak: adatbázis, adatbázis összekapcsolás, elektronikus közigazgatás, adatvédelem, személyes adat ~ database, connecting databases, electronic government, data protection, personal data

BEVEZETÉS

Az elektronikus közigazgatás hatékony működésének egyik alapvető feltétele az adatok elektronikus tárolása, mely leggyakrabban adatbázisok segítségével valósul meg. A legfontosabb, szám szerint 23, a *nemzeti adatvagyon* körébe tartozó közigazgatási adatbázist az Országgyűlés által 2010-ben elfogadott CLVII. törvénye [1], illetve az ehhez kapcsolódó kormányrendelet [2] nevesíti meg. A nemzeti adatvagyon körében található többek közt a polgárok személyi adatait és lakcímét tartalmazó nyilvántartás, a központi úti okmány- és szabálysértési nyilvántartás, az egészség- és nyugdíjbiztosítási nyilvántartások, valamint a munkanélküliek ellátásával, a termőföldhasználattal kapcsolatos adatok és az államkincstár által vezetett szociális támogatások nyilvántartásai is.

A nemzeti adatvagyon mellett természetesen számtalan egyéb nyilvántartás segíti az elektronikus közigazgatás működését. A közigazgatás adatbázisainak vezetését, a nyilvántartott adatok körét mindig egy bizonyos szintű szabályozás határozza meg. A közigazgatás adatbázisainak vezetését, működését meghatározó jogszabály lehet törvény, rendelet (kormány, minisztérium, önkormányzat) vagy alacsonyabb szintű (például szervezeti) szabályozás. *Közigazgatási adatbázison* a továbbiakban olyan, a magyar közigazgatásban fellelhető adatbázist értünk, melyet valamely államigazgatási szerv a saját feladatai ellátása során hozott létre.

Bizonyos esetekben – például döntés előkészítés, statisztikai számítás, hatásvizsgálat elkészítése céljából - szükség lehet a különböző adatbázisok összetartozó sorainak összekapcsolására. *Adatbázisok összekapcsolásán* olyan új adatbázis létrehozását értjük, mely az eredeti adatbázisok azonos azonosítókkal vagy kapcsolati kóddal rendelkező sorainak adatait vagy azok egy részhalmazát tartalmazza. Kapcsolati kód egy olyan alfanumerikus azonosító, melyhez egyetlen entitás (például személy) azonosító adatait (pl. adóazonosító jel, TAJ szám, személyazonosító jel) rendeljük hozzá. Az adatbázisok összekapcsolásának feltételeit, módszerét és folyamatát a döntéselőkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló 2007. évi CI. törvény és az ehhez tartozó kormányrendelet szabályozza [3], [4]. Adatbázisok összekapcsolását csakis konkrét, előre definiált célhoz kötötten lehet végrehajtani.

A döntés előkészítők kérhetnek adatokat minden olyan nyilvántartásból, ami állami tulajdonú intézmény vagy szervezet kezelésében van. A legfontosabb közigazgatási nyilvántartások közérdekű adatokat, személyes adatokat és közérdekből nyilvános adatokat tartalmaznak. A *személyes adat* fogalmát az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban adatvédelmi törvény) [5] határozza meg. A törvény szerint érintettnek nevezünk bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személyt. Személyes adat pedig az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés.

Közérdekű adat az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret. Közérdekű adat így általában az adatkezelő szerv hatáskörére, illetékességére, szervezeti felépítésére, szakmai tevékenységére, eredményességére, a rögzített adatfajtákra és a működést szabályozó jogszabályokra, szerződésekre és a gazdálkodásra vonatkozó adat. Közérdekű adat például egy önkormányzati beruházás pénzügyi adata vagy egy vízközmű társulás szervezeti és működési szabályzata.

Közérdekből nyilvános adat a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli. Közérdekből nyilvános adat például a magánszemélyek vagy szervezetek közpénzek felhasználásával kapcsolatos adata vagy gazdasági tevékenységükkel kapcsolatos környezetvédelmi adatok, de e körbe tartozik a közszereplő személyek nyilvánosság számára megismerhető személyes adata is.

Közigazgatási adatbázisok esetén gyakran találkozunk az adatkezelés és adatfeldolgozás fogalmaival [6]. Adatkezelőnek nevezzük azt, aki az adatkezelés célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza, az adatfeldolgozó pedig elvégzi az adatkezeléshez kapcsolódó technikai műveleteket. Ezeket a műveleteket az adatkezelő maga is végrehajthatja, ekkor csak adatkezelőről beszélünk, és nincs adatfeldolgozó. Az adatfeldolgozónak a személyes adatokon végzett tevékenységére vonatkozó érdemi döntéseket az adatkezelő felelőssége meghozni. Az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért tehát az adatkezelő felelős. Az adatfeldolgozó az adatokat csak az adatkezelő rendelkezései szerint dolgozhatja fel. A megbízott adatfeldolgozó további alvállalkozót nem vehet igénybe. Az adatfeldolgozó tevékenységi körén belül, illetőleg az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért.

Jelen publikáció alapvető célja a közigazgatási adatbázisok összekapcsolásának biztonsági kérdéseinek vizsgálata. Ennek érdekében a publikáció

- feltárja a közigazgatási adatbázisok összekapcsolásának szükségességét és célját;
- elemzi az adatbázisok összekapcsolásának jogi és technikai korlátait, problémáit;
- bemutatja az összekapcsolást érintő magyarországi törvényi szabályozást.

ADATBÁZISOK ÖSSZEKAPCSOLÁSÁNAK SZÜKSÉGESSÉGE

A közigazgatási adatbázisok összekapcsolásának szükségességét a döntés előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló 2007. évi CI. törvény [3] is tárgyalja. Eszerint az államnak és az államigazgatási szerveknek kötelessége a gazdaságra és a társadalmi folyamatokra kiható döntéseiket előzetesen mérlegelni és eredményeiket utólagosan vizsgálni. Racionális és igazságos döntéseket az állami szervek csak a tények és a következmények alapos ismeretében képesek meghozni. A döntési alternatívák közötti választásban és a szabályozások előkészítése során empirikus kutatásokkal alátámasztott hatásvizsgálatokat és elemzéseket kell végezni. A törvény kimondja, hogy a költségvetési szervek által létrehozott adatbázisok nem csak adminisztratív célokra, hanem elemzések, hatásvizsgálatok és döntés előkészítés céljára is alkalmazandók.

A kutatásokban és elemzésekben mikroszintű adatokra van szükség. Mikroszintűnek nevezzük a természetes személyre vagy szervezetre vonatkozó adatot, melyet két további csoportba sorolunk be. Megkülönböztetjük a közvetlen vagy közvetett azonosításra nem alkalmas anonim (vagy névtelen) mikroszintű adatot az alanyukkal kapcsolatba hozható, személyes mikroszintű adatoktól.

A közigazgatás szervezetei feladataik ellátásához adatokat gyűjtenek természetes személyekről és gazdasági szervezetekről és ezeket adatbázisokban tárolják el. Ezek az adatbázisok elsősorban a szervezetek működéséhez szolgáltatnak adatokat, de másodsorban felhasználhatók - az előzőekben már felvázolt - kormányzati döntések meghozatalának előkészítéséhez, a döntések és intézkedések hatásainak utólagos vizsgálatához és statisztikai kutatásokhoz is. A vizsgálatokhoz, kutatásokhoz gyakran szükség van különböző adatbázisokból származó adatok együttes kezelésére, az összetartozó sorok (objektumok, entitások) egymáshoz rendelésére, vagyis az adatbázisok összekapcsolására.

Az adatbázisok összekapcsolásának folyamata kapcsán adatkérő szervnek nevezzük azt, aki az adatok átadását igényeli, vagyis aki számára az összekapcsolt adatok átadásra kerülnek. Az adatkezelő szerv vezeti az adott nyilvántartást, adatbázist. Az adatbázis létrehozásáért felelős szerv végzi el a különböző adatkezelőktől megkapott adatok összekapcsolását és adja át az összekapcsolt adatokat az adatkérő szerv számára.

Például hatásvizsgálatokban, döntés előkészítésben szükséges lehet a családoknak, háztartásoknak juttatott állami támogatások értékének, vagy annak változásának ismerete. Ezt úgy számolhatjuk ki, ha tudjuk, hogy milyen támogatásokban részesül az adott háztartás, illetve milyen adókat és járulékokat fizet. Ennek kiszámolásához adózási, társadalombiztosítási és államkinestári nyilvántartások adatait kell egyszerre vizsgálni, aminek része a különböző adatbázisok összekapcsolása is. Ha pedig azt akarjuk elemezni, hogy a táppénz szabályozása hogyan hat a munkakínálatra, akkor az Országos Egészségügyi Pénztár által nyilvántartott táppénz adatokat kell összekapcsolni az Országos Nyugdíjbiztosítási Főigazgatóság által nyilvántartott munkavállalásra vonatkozó adatokkal.

Diplomás pályakövető rendszer

A következőkben példaként bemutatjuk az adatbázisok összekapcsolására épülő Diplomás pályakövető rendszert (továbbiakban DPR), melyet 2008 óta működtet az Educatio Társadalmi Szolgáltató Nonprofit Kft [7]. A DPR a magyar felsőoktatásban végzett hallgatók végzés utáni életpályájáról szolgálat adatokat, ezáltal a felsőoktatási intézményekben szerezhető diploma munkaerő-piaci értékéről, a végzettek elhelyezkedési lehetőségeiről kaphatunk információkat. A DPR által lekérdezhetővé válnak egy adott felsőoktatási intézményben (és azon belül adott karon, szakon) végzett hallgatók elhelyezkedési adatai (például a végzettek jelenlegi és korábbi munkahelyének jellege, székhelye, ágazati besorolása, munkaköre, jövedelme).

A diplomás pályakövető rendszer esetében olyan adatbázisok összekapcsolása jön létre, melyek a végzett hallgatók felsőoktatási útját, valamint az őket érintő munkaerő-piaci eseményeket tárolják. Az integráció folyamán a Felsőoktatási Információs Rendszer (FIR), a Nemzeti Adó- és Vámhivatal (NAV), az Országos Egészségbiztosítási Pénztár (OEP) és a Foglalkoztatási és Szociális Hivatal (FSZH) adatbázisainak összekapcsolása valósul meg. A Felsőoktatási Információs Rendszerből a végzettek tanulmányi és demográfiai adatait, a NAV rendszeréből a járulékbemutató adatokat, az OEP adatbázisából a biztosítottak adatait, az FSZH-től pedig a munkaerő-piaci adatokat használja a DPR. A négy forrásadatbázis adatait a név, anyja neve, születési dátum azonosító paraméterek segítségével kapcsolják össze.

A Diplomás pályakövető rendszer hasznos lehet kormányzati döntéshozók számára felsőoktatás-kapacitási döntések meghozatalában, például támogatott képzések, szakok, keretszámok megállapítása során. A rendszer lehetővé teszi az állami támogatások hatásvizsgálatát, továbbá összevethetővé teszi a felsőoktatási intézményeket a munkaerő-piaci paraméterek mentén. Statisztikai elemzések, vizsgálatok számára adatokat szolgáltat a rendszer a felsőoktatásban végzettek munkaerő-piaci helyzetének alakulásáról (munkahelyi státusz, jövedelem, munkanélküliség, továbbtanulás). Végül pedig a DPR hasznos lehet a felvételizők számára az egyes diplomák (képzések és intézmények) munkaerő-piaci bevalásáról, a valós elhelyezkedési lehetőségekről való tájékoztatás által.

ADATBÁZISOK ÖSSZEKAPCSOLÁSÁNAK KORLÁTAI, PROBLÉMÁI

Adatbázisok összekapcsolásának jogi korlátai, problémái

Az adatbázisok összekapcsolására vonatkozó – publikációnkban tárgyalt – jogi előírások, korlátozások az adatbázisokban foglalt személyes adatok védelméhez kapcsolódnak. A jogi korlátozások alapvető rendeltetése, hogy biztosítsák a személyes adatok védelmét az összekapcsolás eredményeként bekövetkező jogosulatlan megismerés, illetve felhasználás ellen. Emellett meghatározzák a jogszerű összekapcsolás azon feltételeit, amelyek fenntartják a megfelelő szintű adatvédelmet. A következőkben röviden összegezzük a személyes adatok védelmének jogelméleti alapjait, a célhoz kötöttség elvének lényegét, az összekapcsolás adatvédelmi kockázatát, valamint a személyhez kötöttség megszüntetésének alapjait. A kérdések részletesebb elemzése megtalálható pld. a 2008-2011 közötti adatvédelmi ombudsman PhD értekezésében. [8]

A *személyes adatok* körébe azon adatokat soroljuk, amelyek egy természetes személlyel kapcsolatba hozhatóak, amelyekből az érintettekre következtetések vonhatóak le. Egy elemi adat tehát nem önmagában személyes, hanem más – a személyt azonosító – adatokkal fennálló kapcsolatában. Az egyes adatok az adatkezelés során mindaddig megőrzik ezen minőségüket, amíg kapcsolatuk az érintett személlyel helyreállítható. A személyes adatokhoz szorosan kapcsolódik az információs önrendelkezési jog, amely szerint ilyen adatokat csak az érintett beleegyezésével szabad felvenni és felhasználni, illetve követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját¹. Személyes adat kötelező kiszolgáltatását és felhasználását csak kivételesen és törvényben lehet elrendelni.

A *célhoz kötöttség elve* azt mondja ki, hogy személyes adatot feldolgozni csak pontosan meghatározott és jogszerű célból szabad. A meghatározott cél nélküli, előre nem megjelölt jövőbeni felhasználásra irányuló adatgyűjtés és –tárolás jogellenes. Személyes adatot harmadik személy számára hozzáférhetővé tenni csak akkor szabad, ha az erre konkrét törvényi felhatalmazással rendelkezik, vagy az érintett ehhez hozzájárulását adta.

Az *adatbázisok összekapcsolása* lényegében a kért adatok más számára történő rendelkezésre bocsátását jelenti. Ez a jogi korlátozások nélkül az egyes adatbázisok ezirányú kockázatainál jóval nagyobb mértékben veszélyezteti a személyes adatok biztonságát. A személyre vonatkozó adatok széles körének összességükben és összefüggéseikben történő megismerése kiszolgáltatja az érintetteket, átvilágíthatóvá teszi magánszférájukat, az eredeti összefüggésekből kiragadott adatokból összeállított "személyiségprofil" (amely nagy valószínűséggel torz is), különösen sérti a személyiségi jogokat. Az összekapcsolás lehetősége ráadásul kizárja az érintettet az adatáramlásból, korlátozza abban, hogy adatai útját és felhasználását ellenőrizze.

A személyes adatokat is tartalmazó adatbázisok közérdekű, vagy más jogszerű célra való felhasználásának jogi feltétele az *adatok személyességének megszüntetése*, az ún. anonimizálás. Az anonimizálás egy olyan eljárás, amelynek eredményeként az egyes adatsorok már nem kapcsolhatóak adott személyhez.

Az anonimizálás igénye már a statisztikai felmérések (köztük pld. népszámlálások), elemzések esetében felmerült, amelyek során nagymennyiségű adat kerül felvételre egyedi válaszadó, statisztikai egység (személy, szervezet, stb.) szinten. A felmérések eredményei általában aggregáltan kerülnek nyilvánosságra, ami azonban értelemszerűen információvesztéssel jár.

Az egyedi adatok (mikroadatok) számos további információt, összefüggést hordoznak, amelyek csak ezek felhasználásával, feldolgozásával nyerhetők ki, ez azonban magában hordozza a személyhez, statisztikai egységhez kapcsolódó adatok megismerésének,

¹ Az érintettnek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát.

felfedésének veszélyét. Emiatt a mikroadatok felhasználása megkerülhetetlen, de csak indokolt (pld. közigazgatási, kutatási, oktatási) célból és meghatározott eljárási korlátozásokkal lehetséges. Ennek részét képezi az azonosításra alkalmas adatok, nevek és a részletesebb behatárolást biztosító földrajzi adatok törlése, ami azonban többnyire nem elegendő. Általában különböző adatok módosításával kell biztosítani, hogy még ún. kvázi-azonosítók (egyes személyek néhány jellemző tulajdonsága) segítségével se lehessen valakit azonosítani.

Adatbázisok összekapcsolásának logikai, technikai korlátai, problémái

Adatbázisok összekapcsolása technikai értelemben azt jelenti, hogy különböző adatbázisok adataiból – fizikailag, vagy virtuálisan – egy új adatbázist hozunk létre. Relációs adatbázisok esetében ez különböző adattáblák sorainak összekapcsolását jelenti, amely megfelelő oszlopokban szereplő adatértékek egyezésére épül. Az adatbáziskezelés fogalomrendszerében ez ún. elsődleges kulcsok és idegen kulcsok² segítségével történhet.

Az adatbázisok – vizsgálatunk tárgyát képező – összekapcsolása technikai szempontból abban az esetben a legegyszerűbb, ha az egyes adatbázisok (táblák) tartalmazznak közös elsődleges, vagy idegen kulcsokat. Az előzőekben bemutatottak alapján, személyes adatokat tartalmazó adatbázisok esetében azonban ennek általában jogi korlátai vannak. A következőkben röviden áttekintjük az ilyen esetekben felmerülő technikai problémákat és megoldási lehetőségeket. Ennek keretében összegezzük az adattartalom és az adatminőség szinten felmerülő problémákat.

Az *adatbázisok összekapcsolásának adattartalom szintű problémái* akkor állnak fent, amikor az összekapcsoláshoz felhasználandó mezők részben, vagy egészben eltérő tartalmú, vagy belső struktúrájú adatokat tartalmazznak. Ezek az azonosításra kínáló adatok esetében a gyakorlatban sokszor előfordulnak: a különböző adatbázisok a személyneveket egy, vagy több – jellemzően karakteres – mezőben tartalmazzák. Egy mezőben történő ábrázolás esetén a név részét képezhetik különböző előtagok (dr., özv., id., stb.), esetleg utótagok (pld. rendfokozat, oktatói munkakör, stb.). Ugyanez igaz a szervezet megnevezésekre és hasonló mondható el a lakcímet, telephely címet tartalmazó mezők esetében is. Az összekapcsolás megvalósítása ilyen esetekben vagy valamilyen metrika szerinti "hasonlóság" alapján, vagy a strukturálatlan névadatok összetevőkre bontására³, majd a különböző forrásokból származó összetevők egyeztetésére építve lehetséges.

Az *adatbázisok összekapcsolásának adatminőség szintű problémái* abban rejlenek, hogy – elsősorban az adatfelvétel, adatszolgáltatás, adatrögzítés sajátosságaiból következően – azonos adatmező tartalom és formátum elgondolás esetén is gyakran találkozhatunk ugyanazon név, vagy cím eltérő megjelenítésével. Pld. személyek neve esetében valamennyi utónév, vagy csak a használt szerepeltetése, címek esetében pedig a címösszetevők – sok esetben az adatmező hossz korlátai miatt – eltérő megjelenítése (pld. Bajcsy Zsilinszky utca 23.; Bajcsy Zs. E. u. 23. I. em. 2; Bajcsy Zs. u. 23.; stb.). További, nem a pontatlanságból származó problémát okoznak a név-változások és a közterület megnevezés változások, valamint a házszám változások, ami eltérő időpontban felvett adatok esetében szintén akadályozza az összekapcsolást. [9]

A címek esetében megoldást jelenthet egy országos közhiteles címadatbázis és annak következetes alkalmazása, átvétele. Jelenleg a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala rendelkezik Magyarország házszám mélységű címadatbázisával, valamint Magyarország közterületeinek változásjegyzékével. Az előbbi

² Elsődleges kulcs: egy adattábla rekordjai egyértelmű azonosítását biztosító adatmező(együttes), melynek értéke az adott táblában egyedi. Idegen kulcs: egy adattáblában szereplő olyan adatmező(együttes), amely megegyezik egy másik tábla elsődleges kulcsával.

³ Ez automatikusan tökéletesen, minden lehetséges adatra kiterjedően (ma még) nem oldható meg.

azonban csak lakott címeket és közterületeket tartalmaz, a nem lakott címek (iparterületek, üdülőterületek, zártkertek, stb.) hiányoznak belőle. A KSH népszámlálásokhoz használt címadatbázisa tartalmaz lakott és nem lakott, külterületi és belterületi címeket is, azonban naprakészsége a tízéves népszámlálási ciklus miatt bizonytalanabb. Ennek a helyzetnek a feloldására született meg az Államreform Operatív Program keretében a "Közhiteles címregiszter kialakítása" kiemelt projekt felhívása.

A MAGYARORSZÁGI TÖRVÉNYI SZABÁLYOZÁS

Az adatbázisok összekapcsolásához, illetve a személyes adatok ennek alapját képező védelméhez kapcsolódó törvényi szabályozások kiinduló pontját az Alkotmánybíróság egyik 1991-es határozata képezte. Ennek következményeként született meg a személyazonosító kódokról szóló 1996. évi XX. törvény. 2007-ben jelent meg a CI. törvény, amely a döntéshozatalhoz szükséges adatbázis összekapcsolások feltételeit és rendjét szabályozta. Végül 2011-ben jelent meg az 1992-es adatvédelmi törvény helyébe lépő, az információs önrendelkezési jogról szóló CXII. törvény. A következőkben röviden áttekintjük ezen jogszabályok témánk szempontjából fontos összetevőit.

A 15/1991. Alkotmánybírósági határozat [10] az állami népesség-nyilvántartásról szóló törvényerejű rendeletet és ennek végrehajtási rendeleteit nyilvánította alkotmányellenesnek és semmisítette meg. A határozat az Alkotmányban szereplő személyes adatok védelméhez fűződő jogot már információs önrendelkezési jogként értelmezi. Megállapítja, hogy e jog gyakorlásának feltétele és legfontosabb garanciája a célhoz kötöttség, további garanciája az adattovábbítás és az adatok nyilvánosságra hozásának korlátozása. Rögzíti, hogy "személyes adatot harmadik személy számára hozzáférhetővé tenni – s eszerint adatfeldolgozási rendszereket egymással összekapcsolni – csak akkor szabad, ha minden egyes adat vonatkozásában az adattovábbítást megengedő összes feltétel teljesült."

A határozat számos egyéb rendelkezés mellett magát a korlátozás nélkül használható, általános és egységes személyi számot, mint univerzális azonosítót minősítette alkotmányellenesnek. Elismerve e megoldás technikai előnyeit és ennek következtében az adatfeldolgozás, igazgatás, szolgáltatások magasabb hatékonyságára gyakorolt hatását, kiemeli a személyiségi jogokra, köztük az információs önrendelkezési jogra gyakorolt súlyos kockázatát. Megállapítja, hogy ha a személyi számot az adatvédelem elvei következetes betartásával használják, értelmét veszti, mert előnyeit nem lehet kihasználni. Ellenkező esetben súlyosan veszélyezteti az önrendelkezés szabadságát és az emberi méltóságot.

Az 1996. évi XX. törvény az azonosító kódokról [11] – a hivatkozott Alkotmánybírósági határozatra válaszként – szabályozza a korábbi személyazonosító kód (személyi szám) helyébe lépő három azonosító kód (adóazonosító jel, társadalombiztosítási azonosító jel, személyi azonosító) képzésének, kezelésének és használatának szabályait. Tételesen felsorolja azon szerveket, amelyek az egyes azonosító kódokat törvényben meghatározott feladatkörükben eljárva jogosultak megismerni, vagy kezelni. Más adatkezelők az azonosító kódok használatára csak az érintett előzetes, írásbeli hozzájárulása alapján jogosultak. Annak az adatkezelőnek, amely több azonosító kód használatára jogosult, a különböző azonosító kódokat tartalmazó nyilvántartásait elkülönülten kell vezetnie. A törvény emellett rögzíti, hogy a természetes személyazonosító adatok közé a személy családi és utóneve, születési családi és utóneve, születési helye és ideje, valamint anyja születési családi és utóneve tartoznak.

A törvényben megjelenik a kapcsolati kód fogalma, mint a különböző célú adatkezelések közötti törvényes kapcsolat elősegítésére, megvalósítására képzett ideiglenes számsor. A kapcsolati kód rendeltetése, hogy az adatkezelők közötti kapcsolat – az érintett személy természetes személyazonosító adatokkal történt azonosítása után – egymás azonosító

kódjának megismerése, illetve a természetes személyazonosító adatok rendszeres átadása nélkül megvalósítható legyen. A kapcsolati kódot az adatot átadó adatkezelő képezi és azt rajta és az igénylőn kívül más nem ismerheti meg. A kapcsolati kódnak ugyanazon személyre vonatkozóan adatkéronként eltérőnek kell lennie.

A 2007. évi CI. törvény a döntéshozatalhoz szükséges adatokról [3] a természetes személyekre, vagy gazdasági szervezetekre vonatkozó mikroszintű adatok felhasználásának jogi feltételeit teremti meg.⁴ Célja a statisztikai célból gyűjtött adatok és a közigazgatás adminisztratív célokat szolgáló adatvagyonának másodlagos felhasználása kormányzati döntések hatásainak előzetes vizsgálatára, illetve eredményük utólagos értékelése.

A törvény előírja, hogy a közérdekű adatot annak kezelőjének át kell adnia az azt igénylő központi államigazgatási szervnek. Meghatározza azt is, hogy az adatkezelőnek az átadott adatokat visszafordíthatatlan módon módosítania kell, hogy az érintettel ne legyenek kapcsolatba hozhatóak (anonimizálás).⁵ A nevek törlése mellett a törvény előírja, hogy a személy lakcímére vonatkozó módosított adat kistérségnél nem lehet pontosabb.

A törvény részletesen szabályozza a különböző adatkezelők által kezelt adatok összekapcsolásának rendjét. Ennek alapját az ún. anonim kapcsolati kód biztosítja, amely adott személyre vonatkozó személyazonosító adatokból véletlenszerű elemet is tartalmazó módszerrel képzett karaktersor, amellyel ugyanazokból az adatokból mindig ugyanaz a karaktersor jön létre, de a létrejött karaktersorból a személyazonosító adatok nem állíthatók helyre. Az eljárás részletesebb bemutatására a későbbiekben kerül sor.

A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [5] az 1992-es adatvédelmi törvényt⁶ váltotta fel. Az egyébként számos bővítést, módosítást tartalmazó törvény témánk szempontjából a korábbi szabályozáshoz képest jelentős újdonságokat nem tartalmaz. Önállóan előírja viszont, hogy "a különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásban tárolt adatok – kivéve, ha azt törvény teszi lehetővé – közvetlenül ne legyenek összekapcsolhatóak és az érintetthez rendelkezhetőek". [5, 7. § (4)]

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Publikációnkban a közigazgatási adatbázisok összekapcsolásának kérdéseit vizsgáltuk. Feltártuk a közigazgatási adatbázisok összekapcsolásának szükségességét és célját; elemeztük az összekapcsolás jogi és technikai korlátait, problémáit és bemutattuk a témánkat érintő magyarországi törvényi szabályozást.

A közigazgatás elektronikus nyilvántartásai az elsődleges adminisztratív célok mellett adat alapú döntéshozás, statisztikai számítások, társadalomkutatási feladatok számára is felhasználhatók. Az államigazgatási nyilvántartások másodlagos felhasználását több nemzetközi szervezet - például az Európai Bizottság, az OECD, a Világbank és az ENSZ - is szorgalmazza, mint a kormányzati hatékonyság, illetve a kutatások ösztönzésének egy lehetséges eszközét. A közigazgatási adatvagyon felhasználását célozza meg segíteni az Európai Parlament és a Tanács 2003/98/EK számú irányelve. Az irányelv minimum szabályokat állapít meg a tagállamok közigazgatási szervei birtokában lévő dokumentumok (ideértve az adatokat is) további felhasználására [13].

⁴ A törvény kidolgozásának egyik alapját az Európai Parlamentnek és Tanácsnak a közszféra információinak további felhasználásáról szóló 2003/98/EK irányelve képezte. [12]

⁵ Ez a megoldás korábban már megjelent az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséhez kapcsolódóan is.

⁶ 1992. évi LXIII. törvény a személyi adatok védelméről és a közérdekű adatok nyilvánosságáról.

Magyarországon a fenti irányelv céljainak elérését a döntés előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló 2007. évi CI. törvény teszi lehetővé. A törvény kimondja, hogy az államnak és az államigazgatási szerveknek kötelessége, hogy a gazdaságra és a társadalmi folyamatokra kiható döntéseiket előzetesen mérlegeljék, eredményüket utólagosan vizsgálják, és ehhez adminisztratív céllal gyűjtött adatokat is felhasználjanak. Ez a törvény és a hozzá kapcsolódó kormányrendelet szabályozza a közigazgatási adatok összekapcsolásának lehetőségeit is. A szabályozásra az európai uniós irányelv mellett jelentősen hatottak a hazai adatvédelmi előírások, melyek európai szinten kifejezetten szigorúnak számítanak.

Az államigazgatási adatbázisok hatékony felhasználását, ezen belül az adatok összekapcsolását jelentősen segítené a közigazgatásban tárolt adatok koherens, azonos formátumú kezelése, a többszörösen duplikált tárolás kiküszöbölése és a nyilvántartott adatok metaadatait tároló adatbázis bevezetése.

A publikációnkban megfogalmazott gondolatok alapul szolgálhatnak egy következő kutatás témájához, mely az adatbázis összekapcsolás technikai megvalósításának kérdéskörét tekinthetné át.

Felhasznált irodalom

- [1] 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről
- [2] 38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról
- [3] 2007. évi CI. törvény a döntéselőkészítéshez szükséges adatok hozzáférhetőségének biztosításáról
- [4] 335/2007. (XII. 13.) Korm. Rendelete a döntéselőkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló 2007. évi CI. törvény végrehajtásáról
- [5] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- [6] Dr. Kulcsár Zoltán adatvédelmi szakértő blogja
<http://www.adatvedelmiszakerto.hu/2010/06/adatfeldolgozas-adatfeldolgozoi-szerzodes/>
(2012.11.26.)
- [7] Felsőoktatási kibocsátás 2009. Államigazgatási adatok integrációja. Kutatási jelentés. Educatio Társadalmi Szolgáltató Nonprofit Kft. Felsőoktatási Osztály, 2011.
- [8] Jóri András: Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése. PhD értekezés. – Pécsi Tudományegyetem, Állam és Jogtudományi Kar, 2010.
- [9] Jónás István-Novák Zoltán: A statisztikai adatbázisok összekapcsolásának tapasztalatai és lehetőségei. – Statisztikai Szemle, 2005 (83.)/5, 413-428. o.
- [10] 15/1991. (IV. 13.) AB határozat.
- [11] 1996. évi XX. törvény a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról.
- [12] Az Európai Parlament és a Tanács 2003/98/EK irányelve (2003. november 17.) a közszféra információinak további felhasználásáról.
- [13] Cseres-Gergely Zsombor - Scharle Ágota: Az államigazgatásban keletkező adatok nyilvánosságáról. <http://adatbank.mtaki.hu/files/dokum/2.pdf> (2012.11.26.)

Kassai Károly

kassai.karoly@hm.gov.hu

KIBERVESZÉLY ÉS A MAGYAR HONVÉDSÉG

Absztrakt

A korszerű élet és társadalom erősen függ a különböző információs rendszerektől és szolgáltatásoktól. Az összekapcsolt magánhálózatoknak, telekommunikációs szolgáltatásoknak, kormányzati hálózatoknak és az internetnek kölcsönös függőségei vannak, illetve a kibertérben lévő hálózatokat és szolgáltatásokat és adatokat érhetik belső vagy külső forrásból eredő negatív hatások.

A Magyar Honvédség katonai szervezeteinek rendszer és szervezet specifikus információs rendszerei, kritikus infrastruktúrái (benne kritikus információs infrastruktúrák) találhatóak a nemzeti és globális kibertérnek, így a kiberfenyegetések, sérülékenység és a kiberbiztonsággal kapcsolatos kérdések vizsgálata fontos és aktuális feladat a jobb és biztonságosabb katonai elektronikus adatkezelő szolgáltatások érdekében.

Modern life and society highly depends upon different information systems and information capabilities. The interconnected private networks, telecommunication services, governmental networks and the Internet have some interdependency and the services, networks and information may have some negative impacts in the cyberspace from internal and external sources.

The military organisations of Hungarian Defence Forces have system and organisation specified information services and critical infrastructures, including critical information infrastructures in the national and global cyberspace, so the study of cyber threats, vulnerabilities and cyber security related issues is real important and actual task for the better and secure military information services.

Kulcsszavak: *információvédelem, kiberbiztonság, kiberfenyegetés, kritikus információs infrastruktúra ~ information security, cyber security, cyber threat, critical information infrastructure.*

A „KIBER” ÉS FENYEGETÉSEI

Napjaink egyre népszerűbb témája a „kiberhadviselés” (cyberwar), a „kibertámadás” (cyber attack; a továbbiakban a „cyber” előtag napjaink gyakorlata szerint „kiber”-ként szerepel), illetve az ehhez kapcsolódó kérdések. Hazánkban e területen egységes álláspont, központi szabályozás nem azonosítható, a magyar szakkifejezések sem alakultak ki, így a Magyar Honvédségnél is indokolt kiberveszéllyel kapcsolatos általános kérdések vizsgálata.

Az elektronikus adatkezelés területén a *veszélyek megállapítása a fenyegetések és a sebezhetőség felmérésének, a bekövetkezés gyakoriságának és súlyosságának elemzésének rendjéből áll*, minden esetben adott elektronikus adatkezelési szolgáltatásra, infrastruktúrára, vagy annak elemére vonatkoztatva, így célszerű ezt a sorrendet követni a kiberveszély általános értelmezése esetében is.

A „kibertér”-en (cyberspace) lényegi megfogalmazás szerint az összekapcsolt hálózatok világát célszerű érteni, mely megfogalmazás legfontosabb eleme az *összekapcsolás*. A német Kiber Stratégia pontosan megfogalmazza, hogy a külső kapcsolatokkal nem rendelkező elektronikus adatkezelés nem része a kibertérnek. [1.] Az összekapcsolás történhet azonos vagy különböző szintű védelmi rendszabályokkal rendelkező hálózatok között, tartalmazhat teljes vagy részleges szolgáltatás elérést, illetve önmagában az internet csatlakoztatása is összekapcsolás (nyilvános hálózattal történő összekapcsolás). Láncszerűen összekapcsolt hálózatok esetében elképzelhető, hogy egy hálózat felé nem a közvetlenül csatlakozó hálózathoz érkezik a fenyegetés, hanem azon keresztül egy további hálózathoz. A kibertér értelmezésénél a szolgáltatás hardver és szoftver összetevőin kívül *magát az adatot is elemként kell figyelembe venni*.

A „kiberművelet” (cyber operation) a kibertérben végzett elektronikus adatkezelés és az adatkezelő képességek működésével kapcsolatos tevékenységek, illetve tágran értelmezve az ezek védelmére, befolyásolására vagy támadására (pl. kibertámadás; cyber attack) irányuló tevékenységek, folyamatok.

A „kiberbiztonság” (cyber security) a kibertérben lévő szolgáltatás vagy adat meghatározott (kiber)fenyegetések (cyber threats) ellen, előre meghatározott védelmi szintű állapotát jelenti.

A „kibertér” vagy a „kiberinfrastruktúra” (cyber infrastructure) fogalom tartalma esetenként térben, vagy fizikai jellemzőkkel nehezen meghatározható, a képességek alakulása szerint dinamikusan változó tartalommal bír, beleértve az adatok és hozzáférési lehetőségek sokféleségét, valamint az adat, vagy infrastruktúra hozzáférési lehetőséggel rendelkező személyek körét is.

A kiberfenyegetéseknél *célszerű a fenyegetések eredetét tisztázni, ami támpontot adhat a kihívások kezeléséhez szükséges szervezetek azonosításához is*. Egy Európa Parlament számára készített tanulmány szerint alapvetően a hacker tevékenység, a szervezett bűnözés, az ideológiai vagy politikai szélsőségesség és az állami szereplők által támogatott kiber területű agresszió képezi a fenyegetések forrását.

A Nemzetközi Távközlési Szövetség (International Telecommunication Union; ITU) számára készített szakterületi tanulmány is ehhez hasonlóan fogalmaz (az „állami szereplők” megfogalmazás helyett „hírszerző szervezetek”-et alkalmazva), az előbbieket mellett külön kategóriában említve az oknyomozó riportereket és az elégedetlen alkalmazottakat (ez utóbbi kategóriát a korábbi forrás egyszerűen a hacker kategóriába sorolta). [2.]

A fenyegetések eredetét egy nemzetközi információbiztonsági szabvány [3.] a következőként azonosítja: hacker, cracker; szervezett bűnözők; terroristák; ipari kémek és belső szereplő.

A kiberfenyegetés a Világ Gazdasági Fórum tavalyi évre vonatkozó tanulmánya szerint lehet:

- *Kiberlopás*, ami egyre erősödő iparaggá válik, különösen ahol a gazdasági fejlődés a globális kommunikációs technológia hozzáféréseivel párosul.
- *Kiberkémkedés*, a magán és közszférában egyaránt értelmezve, benne a hírszerzés új formáival, amely fenyegetés nem csak az ellenséges, hanem a szövetséges államokból is származik.
- *Kiberháború*, figyelembe véve a háború értelmezése körüli téves civil értelmezéseket. Háború a kibertérben is lehetséges, illetve a hagyományos és kiberháború kölcsönhatásának egyre nagyobb kockázata van a társadalmakra; az online agresszió nem csak támogatása, hanem hagyományos támadások lehetséges provokálása is lehet.
- *Kiberterrorizmus*, ami az internet nyitottsága, a biztonság és a magánjellegű adatok szempontjából kevésbé ismert. A terrorista szervezetek az elmúlt években egyre szélesebb körben használják az internetet elméleti megalapozásra, toborzásra, műveleti kommunikációra, valamint kiberlopásra.

A fenti szándékos vagy rosszindulatú fenyegetésekből adódó kockázatok hatásának fokozását jelenti az internethez csatlakoztatott „okos” rendszerek hiányosságainak széles skálájából adódó kockázat. [4.]

A kiberfenyegetés célja más ITU források szerint lehet:

- adatok vagy erőforrások megsemmisítése;
- adatok illetéktelen módosítása vagy megismerése;
- adatok vagy erőforrások eltulajdonítása, eltávolítása vagy elvesztése;
- adatok illetéktelen felfedése;
- szolgáltatások megszakítása vagy korlátozása; [5.]
- megsemmisítés, feljogosított személy adataival történő visszaélés. [6.]

Egyéb ITU forrás szerint a fenyegetések lehetnek *véletlenek* (hardver vagy szoftver hiba, kiszolgáló elemek meghibásodásai) vagy *szándékosak* (vírusok és egyéb rosszindulatú programok), *aktívak* (adat és erőforrás megváltoztatása) vagy *passzívak* (erőforrást nem változtató lehallgatás, forgalomelemzés), illetve el kell különíteni a (hálózat szempontjából) *külső és a belső eredetű* (valamilyen feljogosítással, helyi ismeretekkel rendelkező személy) támadásokat. [7.]

Az ISACA (Information Systems Audit and Control Association; Információrendszer Ellenőrök Egyesülete) Európára vonatkozó 2012-es biztonsági felmérés alapján a szervezeti szempontból legmagasabb kockázatú felhasználói tevékenységek: felhasználói jelszavak tárolása fájlban, magántulajdonú eszközön (80%), on-line fájlmegosztási szolgáltatások igénybevétele szervezeti adatok kezelésére (71%) szervezeti tulajdonú számítógép vagy okostelefon elvesztése (65%), személyes fájlok, zene, alkalmazások letöltése szervezeti tulajdonú számítógépre vagy okostelefonra (53%), felhasználói jelszavak tárolása fájlban, szervezeti tulajdonú eszközön (48%), szervezeti tulajdonú számítógép vagy okostelefon használata hivatalos levelezésre, adatkezelésre (43%). [8.]

Az Európai Unió államaiból jelentett incidensek alapján az Európai Hálózatbiztonsági Központ (European Network and Information Agency; ENISA) 2011-es évre vonatkozóan az állandó telefon, állandó internet szolgáltatások, mobil telefon (benne szöveges üzenet szolgáltatás) és mobil internet szolgáltatások bontásban értékelte a veszélyeket. Az incidensek okai: hardver és szoftverhiba (41%), áramellátás (20%), kábelhiba (14%), változáskezelési probléma (10%), vihar (6%), karbantartási hiányosság (6%), hóvihár (4%), humán hiba (4%),

áramingadozás (4%), kábellopás (2%), árvíz (2%), kibertámadás (2%), szolgáltatás túlszordulás (2%), fizikai támadás (2%). Az éves elemzés alapján a tanúságok a következők:

- A mobil hálózatok veszélyeztetése a legmagasabb (az incidens bejelentések 60%-a erre a területre vonatkozott).
- Az üzemkiesések a mobil szolgáltatások felhasználóit érinti a legnagyobb számban (összhangban a behatolások legnagyobb arányával).
- A hardver, szoftverhiba valamint a harmadik fél miatt (pl. áramszünet, szoftver javítócsomag hiány, külső üzemeltető hiányosságai) bekövetkezett hibák okozzák a kiesések túlnyomó részét. A hardver, szoftverhiba kiemelten veszélyezteti a mobil szolgáltatásokat (a komplexitás és a redundancia hiánya miatt).
- A természeti katasztrófák (kiemelten: vihar, árvíz, hóvihár) okozták a leghosszabb kieséseket (átlag: 45 óra).
- Az elektromos hálózattól való függés egyaránt kimutatható az állandó és a mobil rendszereknél. [9.]

Stratégiai szintű összefoglalásnak tekinthető az EU Biztonsági Stratégia megfogalmazása, mely szerint a kereskedelem, a befektetések, a technikai fejlődés erősítik Európa függőségét – így sebezhetőségét – az összekapcsolt szállítási, energetikai, információs és egyéb infrastruktúrákon keresztül. [10.] Ehhez hasonlítható a NATO megközelítés is, mert a NATO Stratégiai Koncepció szerint *a kibertámadások egyre gyakoribbá, szervezettebbé válnak és egyre nagyobb károkat okoznak* a közigazgatásban, az üzleti életben és a gazdaságban, veszélyeztethetik a szállítást, az energetikai rendszereket és egyéb kritikus infrastruktúrát is. A támadások elérték azt a küszöböt, amikor már a nemzeti és Euro-Atlanti jólétet, biztonságot és stabilitást fenyegetik. A támadások eredhetnek külföldi fegyveres erőktől és hírszerző szolgálatoktól, a szervezett bűnözés köreiből, terrorista és egyéb extrém csoportoktól. [11.]

A magyar felső szintű megfogalmazás a nemzetközi megfogalmazásokkal összhangban van. A Nemzeti Biztonsági Stratégia megállapítja, hogy az állam és a társadalom működése mind meghatározóbb módon a számítástechnikára épül. Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szinte mindenki számára elérhetővé vált eredményeit egyes államok, vagy nem-állami – akár terrorista – csoportok arra használhatják, hogy megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatok rendeltetészerű működését. Emiatt a kibertérben növekvő mértékben jelentkező nemzetbiztonsági, honvédelmi, bűnüldözési és katasztrófavédelmi vonatkozású kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelem feladatainak ellátására és a nemzeti kritikus infrastruktúra működésének biztosítására Magyarországnak is készen kell állnia. A nemzeti szintű védelem a Magyar Honvédség számára is iránymutatóan kettős feladatot jelent:

- *a tényleges vagy potenciális fenyegetések és kockázatok rendszeres felmérése és prioritizálása, a kormányzati koordináció erősítése, a társadalmi tudatosság fokozása, valamint a nemzetközi együttműködési lehetőségek kiaknázása;*
- *a nemzeti kritikus információs infrastruktúra védelmének erősítése mellett a szövetségesekkel és EU-partnerekkel együtt az információs rendszerek biztonságának erősítése, a megfelelő szintű kibervédelem kialakításában való részvétel.* [12.]

Az ISACA magyarországi tagozat által végzett, a 2011-es évet elemző tanulmánya szerint – az auditálások tapasztalata alapján – a leggyakrabban előforduló információbiztonsági problémák: túlzott jogosultságok (52%), nem megfelelő naplózás (42%), nem kielégítő változáskezelés (36%), összeférhetetlen szerepkörök (24%), az üzletmenet folytonosság nem megfelelő biztosítása (23%), és a fizikai biztonság hiányossága (17%). (A felmérés 114 magyar cég és intézmény bevonásával történt; 1/3 - 2/3 arányban költségvetési és magánszférából.) [13.]

A Puskás Tivadar Közalapítvány (Nemzeti Hálózatbiztonsági Központ, PTA CERT HUN) 2012. évi harmadik negyedéves jelentése szerint a magyar vállalati szférában tavaly az észlelt biztonsági incidensek megoszlása: eszközlopás (26%), bizalmas adatok kompromittálása (16%), belső behatolási kísérlet (8%), külső behatolási kísérlet (5%), csalás (4.5%). Egy másik hivatkozott felmérés szerint a magyar vállalati rendszeradminisztrátorok szerinti legfontosabb fenyegetések: a vírusfertőzés vagy hálózati támadás miatti leállás (31%), célzott külső támadás miatti adatvesztés (30%), hardverhiba vagy szándékos/véletlen törlés miatti adatvesztés (26%), felhő szolgáltatások biztonsága (24%), illetéktelen fizikai hozzáférés a belső hálózathoz (22%), tabletek és okostelefonok vállalati használata (20%). [14.]

A bemutatott fenyegetések illetve veszélyek az utóbbi időszak valamilyen gyakorlata alapján összeállítottak (statisztikák, interjúk), de a fenyegetések felméréséhez nemzetközi szabvány is nyújthat általános segítséget. [15.] Az általános fenyegetéslista a következő fő csoportokat tartalmazza:

- fizikai károk;
- természeti csapás;
- kritikus szolgáltatások kimaradása;
- sugárzás okozta károk;
- kompromittálódás;
- technikai meghibásodás;
- engedély nélküli műveletek;
- funkciók veszélyeztetése.

A fentiek alapján megállapítható, hogy *a kiberfenyegetés eltérő veszélyű, széles skálán értelmezhető fogalom*. Hazánkban – más államokhoz hasonlóan – a közigazgatásban egy szervezet nem azonosítható, mint e fenyegetésekkel szemben a védelemért felelős szervezet. Feladata van a bűnüldözésnek és megelőzésnek, a nemzetbiztonsági tevékenységeknek és a terrorelhárításnak, az adóhatóságnak, a katonai felderítésnek. A védelem és helyreállítás területén eltérő feladata van a különböző szakmai feladatokkal megbízott szervezeteknek, mint a CERT-nek (Computer Emergency Response Team, Nemzeti Hálózatbiztonsági Központ), a minősített adatkezelés biztonsági felügyeletéért felelős Nemzeti Biztonsági Felügyeletnek, a közigazgatási rendszerek üzemeltetőinek és az önálló hálózatokat üzemeltető tárcáknak, a katasztrófavédelmi feladatokat végző szervezeteknek. Széles körben értelmezve említeni kell még a hardver és szoftverfejlesztésben, gyártásban érintett cégeket, tanácsadó cégeket, oktatási intézményeket, de szerepe van az igazságügyi szereplőknek, egyéb hatóságoknak és a jogszabályalkotóknak is.

A gyakorlati statisztikák láthatóan illeszthetők a szabvány alapú fenyegetések témaköreihez, illetve az is megállapítható, hogy *az általános fenyegetések a Magyar Honvédség elektronikus adatkezelő rendszerei nagy részénél értelmezhetők*, így az üzemeltetési sajátosságok figyelembe vételével ezek az eredmények hasznosíthatók.

SEBEZHETŐSÉG ÉS KOCKÁZATMENEDZSMENT

Az eddig említett általános fenyegetések után következik a sebezhetőség, az adatkezelő képességek értelmezésének és ismeretének, illetve a kockázatok menedzselésének kérdése.

A sebezhetőség vizsgálat adott elektronikus adatkezelő szolgáltatáshoz, infrastruktúrához köthető *szisztematikus, visszatérő jellegű felmérés és értékelés*. A vizsgálat összetett szervezeti, technikai, adminisztratív és szabályozási kérdésekre irányuló feladat, ami az szolgáltatás összetettsége, kiterjedése, fontossága szerint *felosztható, strukturálható*. A sebezhetőség vizsgálatát célszerű két lépcsőre bontani. Az első lépcső feladata valamilyen

általános módszertan, bevált gyakorlat alapján az általános sebezhetőségek azonosítása és csoportosítása, amit második lépcsőben követhet az adott helyszíneknek és rendszereknek megfelelő specifikus adatokkal történő kiegészítés (ami már nagy valószínűséggel az üzemeltető szervezet által bizalmasan kezelt adatok kategóriájába fog esni).

A sebezhetőség vizsgálat területén hazánkban jogszabály pontos követelményt nem azonosít, csak az valószínűsíthető, hogy a készülő elektronikus információbiztonsági törvény végrehajtási rendeletei valamilyen szinten az MSZ ISO 27000 szabványcsaláddhoz fognak igazodni. Az általános sebezhetőségi szempontrendszert ezek alapján az ISO/IEC 27005:2011 szabvány ajánlása szerint célszerű kialakítani [16.], melynek fontosabb területei a következők:

- *Hardver terület:* karbantartási hiányosságok, telepítési problémák, konfiguráció felügyelet hiánya, páratartalomra, porra vagy egyéb szennyeződésre való érzékenység, elektromágneses sugárzásra való érzékenység, hatékony konfiguráció felügyelet hiánya, áramellátás ingadozásra vagy kiesésre való érzékenység, hőmérsékletváltozásra való érzékenység, engedély nélküli módosítás, tárolási hiányosságok.
- *Szoftver terület:* szoftver tesztelési hiányosság, ismert szoftver hiba, kijelentkezés nélküli távozás lehetősége, megfelelő szintű törlés nélküli adathordozó használatra történő átadása vagy újrafelhasználása, szoftver kiadás hiányosságai, a hozzáférési jogosultságok nem megfelelő alkalmazása, naplózási hiányosság, nem megfelelő alkalmazások használata, túl bonyolult felhasználói felületek, üzemeltetési vagy felhasználói dokumentumok hiánya, az adatkezelő rendszer nem megfelelő beállításai, azonosítási és hitelesítési hiányosságok, jelszóbiztonsági menedzsment hiányosságai, felesleges szolgáltatások biztosítása, fejlesztés alatt álló vagy új szoftver alkalmazása, változáskezelés hiánya, kontroll nélküli szoftver letöltések, illetve illegális szoftverek alkalmazása, biztonsági mentések hiánya.
- *Hálózati terület:* nem megfelelően védett kommunikációs csatorna alkalmazása, érzékeny adatok védelem nélküli továbbítása, hibás kábelcsatlakozások, tartalék nélküli elem meghibásodása, az üzenet küldőjének vagy fogadójának nem megfelelő azonosítása és hitelesítése, nem biztonságosan kialakított hálózati architektúra, a jelszavak nyílt formában történő továbbítása, nem kielégítően működő hálózati menedzsment, nem megfelelően védett nyilvános hálózathoz való csatlakozás hiányosságai.
- *Személyi sebezhetőség:* személy távolléte, nem megfelelően kialakított eljárások, nem elégséges biztonsági képzés, hardver vagy szoftver nem megfelelő használata, hiányos biztonságtudatosság, külső fél vagy karbantartó, takarító személyzet felügyelet nélküli tevékenysége, eszköz vagy szolgáltatás használatának hiányos szabályozása.
- *Helyszín:* épületekbe vagy helyiségekbe történő belépés szabályozatlansága, áradásra érzékeny vagy talajvíz által fenyegetett helyen történő kialakítás, nem stabil áramellátás, épületek, ajtók vagy ablakok hiányos fizikai védelme.
- *Szervezet:* felhasználói jogosultságot szabályozó eljárások hiányosságai, szerződő felekkel, harmadik partnerrel kapcsolatos intézkedések hiányosságai, szabályozott audit vagy felügyeleti tevékenység hiánya, a kockázatok azonosítására és felmérésére vonatkozó eljárások hiánya, a bejelentett hibák rögzítésének hiánya, változáskezelési eljárások hiánya, üzemeltetési vagy biztonsági dokumentumok menedzselési hiányosságai, felelősségek meghatározásának hiányosságai, az adatkezelés szabályozási hiányosságai, a biztonsági incidensek esetén alkalmazandó fegyelmező intézkedések hiánya, a mobil adatkezelő eszközök használatának szabályozatlansága, helyiségen kívüli alkalmazás felügyeletének hiánya, a szerzői jogok védelmére vonatkozó eljárások hiánya.

A sebezhetőség vizsgálat és értékelés történhet *az üzemeltető szervezet által* (belső ellenőrzés), *jogszabályban meghatározott felügyeleti szerv által*, illetve ezt kiegészítően (és nem a komplex szempontú ellenőrzés helyett), történhet *belső vagy külső szervezet által* végzett technikai jellegű, specializált mérnöki szintű vizsgálat. Ezeket a vizsgálatokat egyes esetekben kiválthatja egy *független szervezet által végzett biztonsági audit*, melynek szabvány alapon történő megvalósítása az említett szabványcsaládon belül – erőforrások függvényében – hazánkban is megvalósítható.

A sebezhetőség kérdésénél gyakran félreértelmezett feladat a szolgáltatást biztosító elemek, pontosabban *az információs vagyontárgyak (assets) azonosítása*. A pontos konfiguráció ismerete, az azonnal alkalmazható tartalék eszközök és a raktárban lévő eszközök nyilvántartása nélkül javítási vagy helyreállítási lépések nem képzelhetők el. A kérdés további értelmezése elvezet a *kritikus infrastruktúra védelem*, ezen belül a *kritikus információs infrastruktúra védelem* témaköréhez. Hosszabb kifejtés nélkül is belátható a kritikus szolgáltatások azonosításának – és azok védelmére szervezett feladatok meghatározásának – fontossága. Az üzemeltető állománynak pontosan tudnia kell, hogy meghibásodások esetén milyen sorrendben kell helyreállítani a szolgáltatásokat – kiemelt figyelemmel a kritikus fontosságú felhasználók munkájának támogatására –, ami a pontos hardver és szoftver helyzet ismerete mellett már a vészhelyzeti és helyreállítási tervezési és képzési, gyakorlási feladatokra is rámutat. A már hivatkozott nemzetközi szabvány információs vagyontárgyakra vonatkozóan elsődleges és másodlagos vagyontárgyakat különít el. Elsődlegesek az szervezeti folyamatok és tevékenységek másodlagosak a hardver, szoftver, hálózat, személyek, helyszínek és szervezeti struktúra. [17.]

Az adott infrastruktúrához, elemekhez köthető fenyegetések és sebezhetőség az előfordulás gyakorisága, súlyossága figyelembevételével valamilyen kockázatelemzési módszertannal határozható meg, de célszerű a feladatot tovább gondolni. Az adott szolgáltatásra kimutatott veszély önmagában még nem teljes értékű adat, *a katonai képességek szempontjából kulcsfontosságúnak inkább a működési hatáselemzés* (Business Impact Analysis; BIA) *eredménye tekinthető*. A hatáselemzés azt mutatja meg, hogy az adott híradó és informatikai rendszer szolgáltatásainak kiesése vagy a szolgáltatási szint csökkenése mely műveleti képességekre milyen negatív hatást fejt ki. A felgyorsult élet veszélyeit jól szemlélteti, hogy egy német információbiztonsági kormányzati ajánlás a működési hatáselemzés dokumentumaira egyedileg azonosított változáskezelési eljárást javasol, illetve önmagát a hatáselemzést féléves gyakorisággal tartja szükségesnek. [18.]

A kibervédelmi helyzet tanulmányozása, a teendők azonosítása hazánkban is megkezdődött, egyik oldalról jól azonosíthatóan kritikus infrastruktúra védelem és kritikus információs infrastruktúra védelem irányultsággal. Egy magyar kritikus infrastruktúra védelmet elemző tanulmány az információs hadviselés tárgyalásánál a támadások célterületeiként a *tudati, fizikai és információs* dimenziót azonosítja. A tudati dimenziónál felsorolt tényezők elgondolkodtató, társadalmi szintű jelenségekre mutatnak rá, mint a *tudatlanság, az információs technológia vívmányaihoz való hozzáférés hiánya, az innoválható tudás hiánya, a rejtett tudás kihasználatlansága, az információs túlterheltség hatásai, az információs technológiákkal szembeni idegenkedés, bizalmatlanság, iszony*.

A tanulmány a fenyegetéseket a korábban ismertetett módon külső és belső fenyegetésekre bontja, ezen belül *magasan és alacsonyan szervezett fenyegetettségeket* különböztet meg.

A kritikus infrastruktúra védelem kialakítása a szerzők javaslata szerint a következő témakörökre tagolható (a témakörök önmagukban is összetett feladatokat tartalmaznak):

- a védelmi célok meghatározása;
- a kritikus infrastruktúrák meghatározása és azonosítása;
- a feltárt kritikus infrastruktúrák kritikus információs infrastruktúráinak meghatározása és azonosítása;

- a kritikus infrastruktúrák prioritizálása;
- a veszélyek és sérülékenységek feltárása;
- az ideális védelmi megoldások és akciótervek kidolgozása;
- az ideális védelmi megoldások és az aktuálisan alkalmazott védelmi megoldások összehasonlítása, és az esetleges hiányok vagy meg nem felelés pótlása vagy megszüntetése.

E feladatok támogatásához kiemelendő *az azonos szempontrendszer szükségessége meghatározáshoz, besoroláshoz, valamint a sérülékenység illetve a kockázatelemzés területén egységes módszertan, elvek alkalmazása, ami kormányzati szintű kutatási és fejlesztési támogatást igényel.* [19.]

Egy másik magyar tanulmányban Haig Zsolt és Kovács László – akár összegzésnek is értelmezhető megállapítása – szerint az említett három dimenzióban „a komplex információs támadások egymás után vagy egymással párhuzamosan, egyszerre több szinten, dimenzióban realizálódhatnak”. [20.]

E miatt az összetettség miatt – mint Nagyné Takács Veronika cikkében megállapította – kiemelt fontosságú, hogy *a védelem tervezése minél több szempont figyelembe vételével történjen, a védelmi rendszer többszintű és több elemből álló legyen, illetve a helyi és központi feladatok, felelősségi körök legyenek összehangolva.* [21.]

A kiberveszély általános összefoglalása, illetve az ehhez szükséges lépések átfogó ismertetése mellett megemlítendő, hogy *az időszakosan végzett, vagy egyedi változáshoz rendelt kockázatelemzés napjainkban már nem elégséges* a kellően rugalmas védelem kialakításához, illetve az incidenskezeléshez. A hálózatokba integrált szenzorok, adatfeldolgozó eljárások, automatikus értékelő megoldások és döntéstámogató alkalmazások *már lehetővé teszik a dinamikus kockázatelemzést,* az incidens során történő valós idejű beavatkozást, ami lényegesen eredményesebb lehet, mint a hálózati katasztrófa vagy információs károkozás utókezelése. A közel valós idejű információbiztonsági helyzetismeret (situation awareness) feltárja a negatív eseményeket, megmutatja a lehetséges kimeneteket, és segít annak a döntésnek meghozatalában, melynek eredménye lehet a szolgáltatás azonnali változtatása, szüneteltetése, az adatok hozzáférése azonnali letiltása vagy korlátozása, illetve a bizonyíték szolgáltatás érdekében már az ellenséges műveletekkel párhuzamosan is megtörténhet naplózás, együttműködő partner riasztása, hatósági bejelentés.

KATONAI SAJÁTOSSÁGOK

A Magyar Honvédség szervezeteinek irányításához, vezetéséhez és működéséhez szükséges elektronikus adatkezelő szolgáltatások biztonsága (vagy kiberbiztonsága) publikus formában részletesen nem tárgyalható, de az általános helyzetmegítéléshez szükséges áttekintéshez erre nincs is szükség. A honvédelmi feladatok ellátásához a következő típusú információs infrastruktúra elemeket kell megkülönböztetni:

- EU vagy NATO tulajdonú EU, vagy NATO adatot kezelő rendszer;
- nemzeti tulajdonú EU, vagy NATO adatot kezelő rendszer;
- kormányzati rendszer;
- honvédelmi ágazati állandó (stacioner) rendszer (MH Kormányzati Célú Elkülönült Hírközlő Hálózat és hozzá csatlakozó, vagy önállóan üzemelő helyi hálózat), vagy honvédelmi ágazati tábori rendszer;
- honvédelmi szervezettel együttműködő szervezet rendszere;
- nyilvános hálózat.

A felsorolás átfogalmazható úgy is, hogy az MH Kormányzati Célú Elkülönült Hírközlő Hálózat (annak célrendszerei, a központi szolgáltatásokat kiegészítő helyi szolgáltatások és tábori rendszerek), illetve az ezekhez csatlakozó más szervezetek hálózatainak és nyilvános hálózatok összekapcsolásainak összességéből kialakított kibertér alkotja a magyar katonai kiberteret, amely fogalom *a vizsgálati szempont szélesítésével magyar védelmi ágazati kiberterré bővíthető.*

Az MH Kormányzati Célú Elkülönült Hírközlő Hálózat jogszabályban meghatározott feltételek szerint [22.] üzemeltetett *kormányzati célú elkülönült hírközlő hálózat*, melynek hálózatgazdája a honvédelmi ágazatért felelős miniszter. Ez az elkülönülés üzemeltetési és biztonsági szempontból lényeges szempont, illetve megvilágítja azt a tényt is, hogy a *katonai képességeket biztosító szervezetek térben és időben dinamikusan más-más szolgáltatásokat vesznek igénybe*, más a függőségi viszonyuk a különböző célrendszerektől, vagy éppen az internettől. Emiatt nagyon nehezen értelmezhető a „Magyar Honvédség kibervédelme” és ehhez hasonló általános megfogalmazás, ami tízes nagyságrendű stratégiai, hadművelleti és harcászati szintű honvédelmi szervezet, háttérintézmény és tevékenységüket kiszolgáló hálózatok egységes értelmezését jelenti.

Megállapítható az is, hogy a katonai képességek működtetése a közsférában megszokotthoz képest *lényegesen nagyobb arányban tartalmaz minősített adatkezelést* (az ezzel járó kiegészítő védelmi rendszabályokkal együtt), haderőnemenként specializált tábori mobil eszközöket, egyéb katonai szolgáltatásokat, melyeket összefoglalóan nem lehet értelmezni, tárgyalásuk csak specifikusan lehetséges. Ebbe a körbe tartozik például a radaradat, a föld-levegő azonosításhoz szükséges speciális kommunikáció, a fegyverirányítási rendszerek vagy a harcászati rendszerek egyedileg kialakított jelkészlete, ahol a hagyományosan értelmezett „minősítő” és a minősítési folyamat követelményei közvetlenül nem alkalmazhatók.

További – nem csak a Honvédséget érintő – sajátosság, hogy hazánkban jelenleg *a minősített és a nem minősített elektronikus adatkezelésre nincs egységes szabályozási követelményrendszer meghatározva.* A nem minősített adatkezelésre jelenleg nincs jogszabályban megfogalmazott egyértelmű, végrehajtható követelmény. Minősített elektronikus adatkezelésre vonatkozóan átfogó megfogalmazású követelmény áll rendelkezésre, mely szerint „biztonsági követelményeket” kell meghatározni – és jóváhagyni, és ennek alapján „üzemeltetés biztonsági szabályzat”-ot kell készíteni és jóváhagyni. [23.]

A fentiek mellett szükség van a katonai sajátosságok értelmezésére. A stratégiai szintű adatkezelés a közigazgatásban még könnyen azonosítható elvek alapján működik, bár itt már megjelenik a szövetségi tagsággal kapcsolatos adatkezelés bonyolultsága. A Magyar Honvédségnél egyes esetekben tisztán azonosíthatók a NATO, EU (vagy egyéb két, vagy többoldalú nemzetközi kötelezettségvállalás alapján védendő) adatok halmaza, más esetben ezen adatok dinamikus változása, egymásba történő átalakulása könnyen megkeseríti a felhasználók életét. A katonai sajátosságoknál további *fontos tényező a mobilitás szükségességének és fontosságának megértése, támogatása.* Stratégiai vagy hadművelleti szinten is szükség van a felhasználók mobil kommunikációjának biztosítása, de ez lényegesen különbözik a harcászati jellegű mobil, kézi, vagy hordozható képességektől, ahol az adatkezelés jellege eltolódik az alacsonyabb minőségű, rövid elévülési idejű adatok felé, jellemzően a harcászati rádiókommunikációra támaszkodva.

Napjainkban katonai területen nem ritkaság *a NATO, EU vagy egyéb nemzetközi együttműködés, amit elektronikus minősített adatkezelő képességekkel is támogatni kell* (itt jelennek meg egyszerű esetben a „milyen nyilvántartásba kell venni”, vagy a „milyen akkreditált rendszeren tudom megoldani a feladatot” kérdések). Az adat identitás kezelése mellett a másik jellegzetes kihívás *a rövid elévülési idejű adatok kérdése.* A nemzeti légtérhelyzet pillanatnyi állapota érzékeny adat, ami átadás után már egy EU vagy NATO

egységes léghelyzet információ szerves részét képezi. Az ilyen jellegű minősített adat kezelése, vagy harcászati környezetben egy parancs, intézkedés kiadása nem egyenértékű a hagyományos irodai alkalmazású adatkezeléssel, így nyilvánvaló, hogy szükség van ezen esetek pontos meghatározására és *az adatkezelés sajátosságainak megfelelő specializált védelmi rendszabályok kialakítására.*

A Honvédség alkalmazása nem csak békeidőszakban, a közigazgatási rend szerinti körülmények között történhet. Az Alaptörvény különleges jogrendre vonatkozó fejezetében megfogalmazott esetekben kijelölt személy, vagy testület rendeletet alkothat, amellyel egyes törvények alkalmazását felfüggesztheti, törvényi rendelkezésektől eltérhet, valamint egyéb rendkívüli intézkedéseket hozhat. Ennek megfelelően a kibervédelem területén is meg kell tenni azokat az előkészítő lépéseket, melyek az adott biztonsági helyzetnek megfelelően a legjobban támogatják a katonai szervezetek híradó és informatikai rendszereinek védelmét speciális helyzetekben is.

A Honvédség esetében jogszabály fogalmazza meg a lehetőséget, hogy különleges jogrend időszakában az általános katonai híradó és informatikai szolgáltatások kiegészíthetők tömegkommunikációs létesítmények, berendezések igénybevételével, használatba történő átvételével. Elrendelhető elektronikus hírközlési szolgáltatás szüneteltetése, korlátozása vagy ellenőrzésének módosítása, illetve megtörténhet ezek használatra történő átvétele is. [24.] A jogszabályban megfogalmazott változtatások eredményeként módosult híradó és informatikai szolgáltatások *megkövetelik az üzemfelügyeleti és biztonságfelügyeleti rend átalakítását, kiegészítését, illetve szükségessé válhat új szervezési, műszaki megoldások kialakítása is.*

Az adatkezelésre vonatkozó jogszabályok változásai érinthetik az elektronikus adatkezelésre vonatkozó *biztonsági követelményeket, a hatósági eljárásokat, az üzemeltetésre vagy felügyeletre vonatkozó szabályokat.*

Az országvédelemhez szükséges egyedi helyzetek kezelése az elektronikus adatkezelő szolgáltatások, védelmi igények és megoldások naprakész ismeretét igényli, illetve *megköveteli azt a tudást is, ami lehetővé teszi a katonai szervezetek működéséhez szükséges jogszabályi változtatási javaslatok megtételét, új megoldások gyors és kreatív kialakítását.* Rendkívüli helyzetek szövetségi kötelezettségvállalás teljesítése közben is előfordulhatnak, ahol - akár egy másik földrészen, hiányos infrastrukturális feltételek között – szükség van szövetségi, vagy más nemzeti szolgáltatásokkal történő gyors együttműködés megszervezésére, szolgáltatások kölcsönös igénybevételére, ami – különösen minősített elektronikus adatok esetén – nem mindig tekinthető egyszerű esetnek.

AKTUÁLIS KIBERVÉDELMI FELADATOK

A Magyar Honvédségnél az információbiztonsági átfogó követelmények, irányelvek és feladatok miniszteri utasításban megfogalmazott információ biztonságpolitikában rögzítettek. [25.] *A kibervédelem feladatainak értelmezése az eddigi elektronikus információbiztonsági követelmények és eljárásrend erőforrások szerinti továbbfejlesztését jelenti, az eddig megtett szakmai lépések, feladatok átszervezésére vagy visszavonására nincs szükség. A továbblépéshez szükséges feladatok lényege a következő:*

A szükséges szabályozási környezet kialakítása. A meglévő szabályozási renden belül az üzemeltető, felügyelő és biztonságért felelős szervek és szervezetek hatáskörének, kibervédelmi feladatainak – benne a külső-belső együttműködési feladatainak – kidolgozása, a kritikus információs infrastruktúra védelem ágazati feladatrendjének kidolgozása, a különleges jogrendben alkalmazható eljárások irányelveinek meghatározása.

Az elektronikus adatkezelő hálózatok biztonsági szintjének emelése. A hálózatok biztonságának növelése érdekében szabvány és bevált gyakorlat alapú módszereket kell alkalmazni a biztonsági követelmények megfogalmazása és a védelmi rendszabályok

kialakítása, alkalmazása, felülvizsgálata és továbbfejlesztése során. Specializált módszertant kell kialakítani a védelmi rendszabályok ellenőrzéséhez. Kiegészítő védelmi rendszabályokat kell meghatározni, alkalmazni a magas kockázatú szolgáltatások biztonsága érdekében. Az infrastruktúra meghatározott elemeinél meghatározott szintű tanúsított terméket lehet alkalmazni, illetve az architektúra menedzselése során a központi szolgáltatásokat kell előtérbe helyezni és központi biztonsági mechanizmusokat kell alkalmazni helyi megoldások helyett. A hálózati szintű csatlakozásoknál fel kell használni a Nemzeti Távközlési Gerinchálózat adta lehetőségeket (tartalék útvonalak, illetve elsődleges védelmi vonal). Fel kell tární a szolgáltatások életciklusa során az üzemeltetéssel és fejlesztéssel kapcsolatos biztonsági réseket, azonosítani kell az ellátási láncban rejlő kockázatokat (supply chain risks), és ellensúlyozni kell azokat. Specializáltan erősíteni kell a biztonságtudatosságot (security awareness) a felhasználóknál, az üzemeltetőknel (beleértve a tervezést és az üzemeltetés irányítást), a biztonságért felelős állománynál, a kibervédelem kialakításában és fejlesztésében érintett vezetői és döntéshozó állománynál. A rendelkezésre álló kommunikációs lehetőségek kihasználásával ezeket a mozzanatokat figyelemfelhívó programokkal, időszakos tájékoztatásokkal kell erősíteni.

A kibertámadások elleni képességek kialakítása és fejlesztése. Időszakosan és változáshoz kötötten elemezni és értékelni kell a kiberbiztonsággal kapcsolatos kockázatokat. Naprakészen kell tartani a kiberbiztonság aktuális állapotának megítéléséhez szükséges adatok körét és folyamatosan fejleszteni kell a szervezeten belüli és a szervezetek közötti együttműködés rendjét és feladatait. A védelmi rendszabályokon belül a detektálásra és jelzésre épülő mechanizmusok mellett folyamatosan fejleszteni kell a valós idejű döntéstámogatást és előkészítést, a reagálást, illetve a bizonyítékszolgáltatást és helyreállítást is támogató eljárásokat. Az üzemeltető, a biztonsági felügyeleti feladatokat ellátó, illetve a kibervédelmi eljárásokat irányító állomány számára specializált képzési és továbbképzési rendszert kell fenntartani. A reagáló képesség értékelésének érdekében komplex – a váratlan ellenőrzéseket is tartalmazó – ellenőrzési módszertant kell kialakítani és fenntartani. Ki kell használni az önkéntes szervezetekkel, oktatási és kutatási intézményekkel kapcsolatos nemzeti és nemzetközi együttműködési lehetőségeket (tanácsadás és konzultáció).

A szaktudás növelése. Az általános katonai képzésekbe a lehető legjobban integrálni kell az információbiztonsági ismereteket. A szükséges képességek kialakítása és fenntartása érdekében a biztonsági és üzemeltető állomány számára specializált, valóság-hű gyakorlati lehetőségeket kell biztosítani. A biztonsági incidensek, üzemeltetési tapasztalatok, gyakorlatok alapján szerzett tudást fel kell használni és be kell építeni a híradó és informatikai rendszerek védelmébe.

Kutatás és fejlesztés. Ki kell használni a központi kutatási programokban való részvétel, valamint a nemzeti és nemzetközi programokban, projektekben, K+F folyamatokban és feladatokban, illetve az ezeket megvalósító szervezetekben való részvétel lehetőségét. Figyelemmel kell kísérni az adatkezelési igényeket, folyamatosan elemezni kell a rendelkezésre álló megoldásokat, és elemezni kell alkalmazhatóságukat. A kibervédelmi feladatok tervezését az újonnan felbukkanó technológiák és azok hatásainak vizsgálatával, a technológiai trendek előrejelzésével kell támogatni.

Együttműködés. Az illetékes tárcaikkal, nemzeti hatóságokkal és kibervédelmi feladatokat ellátó szervezetekkel szoros, specializált együttműködést kell kialakítani, valamint ki kell használni az oktatási és tudományos intézményekkel, szervezetekkel való együttműködésből adódó lehetséges szinergikus hatásokat. Kapcsolatokat kell tartani a kiberbiztonság szempontjából jelentős gyártókkal, forgalmazókkal, auditor és tanácsadó szervezetekkel. Hatékonyan működő kapcsolatokat kell fenntartani a honvédelmi érdekből összekapcsolt nemzeti és nemzetközi hálózatok üzemeltető, illetve menedzsment állományával.

Az azonosított kiberveszélyek kezeléséhez szükséges feladatok megtervezése, megfogalmazása a Magyar Honvédségnél felső szinten *háromfokozatú rendben képzelhető el*. Első lépésként a honvédelmi tárca információbiztonsági politikájának felülvizsgálatára és szükség szerinti módosítására van szükség, figyelembe véve a kiberbiztonsági, illetve a már jogszabályban megfogalmazott kritikus infrastruktúra védelmi szempontokat.

A szükséges mértékű hatásokat garantáló képességek megtervezése érdekében – figyelembe véve a kibertér és a kibervédelem összetettségét – második lépésként az MH szintű kibervédelmi feladatokat megalapozó koncepciót kell kialakítani és jóváhagyni.

Harmadik lépésként a jóváhagyott koncepció alapján a megvalósításhoz szükséges feladatokat megfogalmazó, szakmai és erőforrási tervezési lépéseket, programokat tartalmazó stratégia kialakítására van szükség. A Magyar Honvédség eddigi szabályozási rendjének megfelelően – amíg jogszabály ettől eltérő követelményt nem határoz meg – a stratégiai feladatok megfogalmazására alkalmas eszköz az MH Informatikai Stratégia, illetve ennek alapján a fejlesztési és üzemeltetési feladatok tízéves, rövid távú (négyéves), és éves beszerzési tervekben történő megjelenítése. A stratégiában rögzítetteket (képességeket) a haderőfejlesztési eljárások rendje szerint kell tervezni, kialakítani és használatba venni, kiegészítve a szükséges szabályozási és képzési feladatokkal.

A kifejezetten kibertámadás elleni védelem megfogalmazása során szintén lehetőség van a szabvány alapú megközelítésre. A logikai vonalat az *esemény bekövetkezése – a detektálás és jelentés – az elemzés és döntés* (incidensé nyilvánítás) – a *válasz – a szabályozó rendszer felülvizsgálata* – és a *szolgáltatás javítás* blokkokban megfogalmazható lépések határozzák meg. [26.]

A kiberbiztonság nem csak katonai területen értelmezhető, így nyilvánvaló, hogy egy nemzeti álláspont kialakítása és fenntartása kiemelt feladat az Alaptörvényben megfogalmazott „nemzeti vagyon” (e fogalmon belül a nemzeti adatvagyon) védelme és az adatkezelő képességek rendelkezésre állás érdekében. A strukturált megközelítéshez a *nemzeti koncepció – nemzeti stratégia – megvalósítást célzó jogszabály(ok)* vonal követése látszik célszerűnek. A megoldásba beleértendő a fogalmi kérdések tisztázása, az elektronikus információ biztonság és a kiberbiztonság tartalmának, viszonyának tisztázása, mert *pontosan kidolgozott fogalmi rendszer nélkül a jogszabályalkotást nem szabad elkezdeni*. Az említett vizsgálati rendszerből hazánkban eddig egy keretjellegű elektronikus információbiztonsági törvénytervezet megfogalmazása történt meg. Ez a katonai képességek megfogalmazása területén egyrészt a nemzeti szabályozási folyamatok követésének és szükség szerinti támogatásának fontosságát jelzi, másrészt meghatározza azt a szakmai követelményt is, hogy a katonai képességek megfogalmazása a szabványok, bevált gyakorlat alkalmazásának vonalán haladjon (remélve, hogy a folyamatban lévő nemzeti szabályozás is ebben az irányban fog haladni).

ÖSSZEGZÉS

A kibertérben lévő szolgáltatások, események és incidensek összetett szempontok szerint meghatározható kiberbiztonságot eredményeznek. A szervezeti feladatok sokszínűsége, a szolgáltatások változásai nem teszik lehetővé, hogy a fenyegetések, sebezhetőségek hosszabb távra érvényes biztonsági szinten legyenek kezelhetők.

A változó kibervilágot fenyegetések területén egyre komplexebb és súlyosabb kihívások érik, miközben a védelemre fordított erőforrások csökkennek. Emiatt a kibervédelem területén *kiemelt jelentősége van a szolgáltatások, hálózati erőforrások, hozzáférésre feljogosítottak minimalizálására és szervezeti működéshez igazítására, a kritikus infrastruktúra és kritikus információs infrastruktúra pontos kijelölésére*.

A szolgáltatások, információs vagyontárgyak azonosítása mellett *létfontosságú a fenyegetések és sebezhetőségek azonosítása* (nem lehet minden ellen védekezni), az eseményekből a biztonsági incidensek helyes kiválasztása (nem minden eset kibertámadás), és a célkitűzéseknek megfelelő eljárások kialakítása, bevezetése és folyamatos felülvizsgálata.

A Magyar Honvédség szervezeteinek működéséhez szükséges kiberbiztonság megteremtése az erőforrásokhoz kötött, *folyamatban elképzelhető feladatrendszer*. A vázolt katonai elektronikus adatkezelő környezet meglehetősen összetett és változó, esetenként még a hálózat szempontjából „kívül” és „belül” megközelítések is értelmezést igényelnek, ami a terminológiai kérdések mellett kiemeli a *szolgáltatások szervezésének, biztosításának fontosságát*, illetve aláhúzza a *magas szintű felhasználói tudatosság szükségességét*.

A bemutatott fenyegetések és sebezhetőségek jó része a katonai elektronikus adatkezelő képességek esetében is értelmezhető, így igazolható, hogy a katonai képességek kialakításához létfontosságú a *nemzetközi trendek, folyamatok ismerete, a szabványok és bevált gyakorlat alapú tudás alkalmazása* és specializálása a hadművelleti és alkalmazói követelmények kiszolgálása érdekében.

A vázolt megoldás szerint csoportosított biztonsági célkitűzések mutatják, hogy a színesnek mondható sebezhetőségi területek miatt *a védelem kialakítása és fenntartása erőforrásokat igénylő, bonyolult, katonai műveletektől erősen függő cél és feladatrendszer*.

Felhasznált irodalom

- [1.] Cyber Security Strategy for Germany, 2011, p. 9;
http://www.cio.bund.de/SharedDocs/Publikationen/DE/StrategischeThemen/css_engl_download.pdf?__blob=publicationFile
- [2.] ITU National Cybersecurity Strategy Guide, 2011, 2. 4. 1. p;
<http://www.itu.int/ITUD/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf>
- [3.] ISO/IEC 27005: 2011, Information technology — Security techniques — Information security risk management, C melléklet p. 43- 44. feny.
- [4.] Global Risks 2011, World Economic Forum, 2012, Cyber security, p. 36.
<http://reports.weforum.org/global-risks-2011/>
- [5.] ITU X 1205. (2008) Overview of Cybersecurity 7. 3. p.
- [6.] ITU Security in Telecommunications and Information Technology, 2009, p. 9;
<http://www.itu.int/pub/T-HDB-SEC.04-2009>
- [7.] ITU National Cybersecurity Strategy Guide, 2011, 2. 4. 3. p.
- [8.] ISACA: 2012 IT Risk/Reward Barometer: Europe, p. 1-2;
www.isaca.org/risk-reward-barometer
- [9.] Annual Incident Reports 2011, ENISA, 2012 p. p. 8, 12, 15;
<http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011>
- [10.] A Secure Europe in a Better World, European Security Strategy, 2003, „The global challenges” fejezet; <http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>
- [11.] Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation, 2010, 12. p; http://www.nato.int/cps/en/natolive/official_texts_68580.htm
- [12.] 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról, 31. p.)

- [13.] Információbiztonsági helyzetkép 2011, ISACA Budapest Chapter, p. 12,
<http://www.kpmg.com/HU/hu/IssuesAndInsights/ArticlesPublications/Documents/Informaciobiztonsagi-helyzetkep-2011.pdf>
- [14.] PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ 2012. III. negyedéves jelentés, p. 9;
http://www.cert-hungary.hu/sites/default/files/news/cert_2012_quart_3.pdf
- [15.] ISO/IEC 27005: 2011, Information technology — Security techniques — Information security risk management, C melléklet p. 42- 43.
- [16.] ISO/IEC 27005: 2011, Information technology — Security techniques — Information security risk management, D melléklet p. 45- 48.
- [17.] ISO/IEC 27005: 2011, Information technology — Security techniques — Information security risk management, B melléklet p. 33.
- [18.] BSI Standard 100-4, Business Continuity Management, v 1.0, 2009, p. 18;
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile
- [19.] Haig Zsolt - Hajnal Béla - Kovács László - Muha Lajos - Sík Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana; ENO Advisory Kft. 2009; (p. 74, 76, 151-152 és 182-183; http://www.cert-hungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf
- [20.] Haig Zsolt – Kovács László: kritikus infrastruktúrák és kritikus információs infrastruktúrák (tanulmány), NKE, 2012; p. 100.
http://kovacsx.hu/download/doktorikepzes/KOVASZ_KII_Tanulmany_FINAL.pdf
- [21.] Nagyné Takács Veronika: A nemzeti kritikus infrastruktúrák védelmének szabályozási és szervezési kérdései, Hadmérnök, VII. Évfolyam 1. szám - 2012. március; p. 183.
http://hadmernok.hu/2012_1_takacs.pdf
- [22.] 346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról, 2. melléklet
- [23.] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 59. § (1)
- [24.] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről, 68.§. (4-5.)
- [25.] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról
- [26.] ISO/IEC 27 035: 2011 Information technology — Security techniques — Information security incident management, p. 23.

Krasznay Csaba

krasznay.csaba@uni-nke.hu

A POLGÁROK VÉDELME EGY KIBERKONFLIKTUSBAN

Absztrakt

A kiberhadviselés fogalmával, eszköztárával, célpontjaival mélyrehatóan foglalkozik a nemzetközi szakirodalom, de az ilyen konfliktusok állampolgárokra gyakorolt hatásának elemzésével egyelőre csak elvétve lehet találkozni. Jelen tanulmányban gondolat kísérlet szinten áttekintésre kerül egy tisztán informatikai eszközökkel végrehajtott komplex támadás állampolgárokat érintő hatásmechanizmusa, azok a kérdések, melyek bizonyosan felmerülnének egy ilyen szituációban, valamint az állami és ipari felelősségvállalás néhány javasolt iránya.

The definition, toolset and goals of cyber warfare is a widely examined question in the international literature, but it is hard to find any reference that deals with the effects to the citizens of such conflicts. This study is a thought experiment, which reviews the mechanism of a complex cyber-attack related to the citizens, emerging questions in this situation, and the proposed directions of public-private responsibilities.

Kulcsszavak: kibervédelem, kiberhadviselés, katasztrófavédelem, polgári védelem
~ cyber defense, cyber warfare, disaster management, civil protection

BEVEZETÉS

A világ számos országában fontos nemzetbiztonsági fenyegetésnek tartják a kritikus információs infrastruktúrákat érintő támadásokat. Nincs ez máshogy Magyarországon sem, ahol a Nemzeti Biztonsági Stratégia így fogalmaz: [1]

„Az állam és a társadalom működése – a gazdaság, a közigazgatás, vagy a védelmi szféra mellettszámos más területen is – mind meghatározóbb módon a számítástechnikára épül. Egyre sürgetőbb és összetettebbkihívásokkal kell számolnunk az informatikai- és telekommunikációs hálózatok, valamint a kapcsolódó kritikusinfrastruktúra fizikai és virtuális terében. Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szintemindenki számára elérhetővé vált eredményeit egyes államok, vagy nem-állami – akár terrorista – csoportok arhasználhatják, hogy megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatokrendeltetészerű működését. E támadások eredetét és motivációját gyakran nehéz felderíteni. A kibertérbenvilágsszerte növekvő mértékben jelentkező nemzetbiztonsági, honvédelmi, bűnüldözési és katasztrófavédelmivonatkozású kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelemfeladatainak ellátására és a nemzeti kritikus infrastruktúra működésének biztosítására Magyarországnak is készen kellállnia.”

A konkrét feladatok között azonban nem jelentkezik a katasztrófa- és polgári védelmi vetület, holott egy összetett kibertámadás hatásai elsősorban az állampolgárokat érintik. A nemzetközi szakirodalom áttanulmányozása sem segít abban, hogyan kell (ha kell egyáltalán) a lakosságot felkészíteni az informatikai támadások hatásaira. A civileket érintő kérdések általában három területre korlátozódnak. Egyrészt élénk vita folyik arról, hogy a piaci szakembereket milyen módon lehet bevonni egy ország kibervédelmébe. Másodsor fontosnak tartják kiemelni, hogy a lakosság számára információbiztonsági tudatosság-képzéseket kell tartani, ahol megismerhetik a biztonságos internetezés alapjait. Harmadrészt feladatként jelenik meg az, hogy a közép- és felsőoktatásban minél több védelmi szakembert képezzenek ki, akik később állami szolgálatba állva segítik a támadások elhárítását. A katasztrófa- és polgári védelmi feladatok tehát nem egyértelműek, mélységük és szükségességük vita tárgya lehet! Jelen tanulmányban éppen ezért lehetséges irányok kerülnek felvázolásra, melyek helyességét és életképességét a következő évek gyakorlata igazolhatja!

KOMPLEX KIBERTÁMADÁSOK

A kibertámadások hatásaival kapcsolatos első kérdés az, hogy vajon megtörténhetnek-e? Ugyanis annak ellenére, hogy sokat foglalkozik a lehetőséggel a szakma, tisztán informatikai eszközökkel elkövetett komplex, komolynak nevezhető támadást még nem tapasztaltunk meg. Ismerjük az elektronikus információs rendszereinktől való függésünket, van elképzelésünk arról, milyen hatással járna ezek támadása, de ezeket a hatásokat eddig csak elszigetelten és legtöbbször nem szándékos incidens kapcsán tapasztalhattuk meg. Szakmai körökben ismert a Digitális Mohács forгатókönyv, mely egy elképzelt kibertámadás lefolyását mutatja be Magyarország ellen. [2] Az ott leírtak jó kiindulópontot jelentenek, de 2009-es publikációja óta olyan események történtek, melyek segítenek az ebben leírt lépéseket pontosítani.

Napjainkban jól elkülöníthető a kiberfenyegetések négy fajtája. Ezek a kiberbűnözés, a hacktizmus és kiberterrorizmus, a kiberkémkedés és a kiberhadviselés. A kiberbűnözés célja az informatikai eszközökön keresztül hasznoszerzés, elsősorban a hagyományos szervezett bűnözői csoportokhoz köthető. A hacktizmus és a kiberterrorizmus ugyan fogalmilag különálló cselekmény, de közös bennük, hogy elsősorban kisebb, decentralizált csoportok hajtják végre azokat az informatikai bűncselekményeket, melyek célja az, hogy minél

szélesebb tömegek lássák a csoport által képviselt ideológiai véleményt. Hatásuk elenyésző, ugyanis azt a fajta szervezettséget nem tudják felmutatni, mely egy hatékony kibertámadáshoz szükséges lenne. A médiahatásuk azonban igen komoly. A kiberkémkedés az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzést jelenti. A kiberhadviselés az államok közötti konfliktusokban jelenik meg, melynek során a felek informatikai eszközöket vetnek be egymás elektronikus információs rendszereinek befolyásolásának céljából.

Ezek közül a kiberterrorizmusnak és a kiberhadviselésnek lehet olyan vetülete, mely szükségessé teszi az összehangolt lakossági védelem megszervezését. Egy kiberterrorista esemény bekövetkezése azonban felettébb valószínűtlen, hiszen azok a csoportosulások, melyeknek érdekében állhat egy ilyen cselekmény végrehajtása, eddig nem mutatták jelét annak, hogy a szükséges képességek birtokában lennének. A Stuxnet kártékony kód megismerése óta tudjuk, hogy a lehetőség adott egy informatikai eszközökkel végrehajtott támadáshoz, de ezek kivitelezése olyan szellemi, anyagi és titkosszolgálati kapacitást igényel, melyet még egy államilag támogatott terroristacsoport sem tud felmutatni. Itt elsősorban az emberi erőforrás hiányát kell kiemelni, hiszen még napjainkban is kevés olyan szakember van a világon, akiknek programozói tudása elégséges lenne olyan kódok megírására, mely alkalmas egy sikeres kibertámadás véghezvitelére.

A kiberhadviselés azonban komoly, egyre növekvő lehetőség, mellyel a hagyományos, fegyveres konfliktusok kísérőjeként már napjainkban is számolni kell. Az intelligens fegyverek kiterjedt használata szükségszerűen magával hozza az ezeket irányító informatikai rendszerek ellehetetlenítésének igényét. Ha ezt a képességet egy ország kifejleszti, automatikusan készen áll a polgári célpontok támadására is, hiszen a fegyverzeteket irányító szoftverrendszerek nem sokban vagy egyáltalán nem különböznek a polgári kritikus információs infrastruktúráktól. Ennek a fejlődésnek az egyik lehetséges végeredménye a „kölcsonös kiberelrettetés” kialakulása, mely hasonlóan a nukleáris fegyverek területéhez azt fogja eredményezni, hogy bár az országok képesek egymás elektronikus információs rendszereire pusztító hatású csapást mérni, de mivel ismerik saját sérülékenységüket és a potenciális ellenfelek képességeit, ezzel a fegyverrel inkább nem élnek. Ennek példája lehet a Kína és Japán között kitört konfliktus a Szenkaku-szigetek miatt. [6] Annak ellenére, hogy mindkét ország képes komoly informatikai csapást intézni a másik felé, eddig elszigetelt esetektől eltekintve ódzkodtak élni ezzel a fegyverrel.

A kölcsönös kiberelrettetés különlegessége az is, hogy gyakorlatilag az összes ország ki tudja fejleszteni a kibertámadási kapacitását, hiszen az közel sem igényel akkora befektetést, mint bármely más fegyverzeté, ráadásul a nemzetközi jogi státusza sem alakult még ki teljesen. Egy komplex, összetett kibertámadás lehetőségével éppen ezért komolyan kell számolni, hiszen nehezebben kontrollálható, mint bármely más fegyverzet, a támadó kiléte nehezen bizonyítható, hatásai pedig jóval kiterjedtebbek, mint egy fegyveres csapásé amellet, hogy a halálos áldozatokkal nem, vagy csak nagyon kismértékben, járulékos formában kell számolni.

A rendelkezésre álló tapasztalatok szerint egy kibertámadás akkor jelent igazán komoly tehertételt egy országnak, ha koordinált, hullámokban jövő, multiszektoriális, hírszerzési információkkal támogatott és elsődlegesen károkozási célú. Koordinált, azaz olyan katonai irányítás áll mögötte, mely rendelkezik valamilyen stratégiai céllal, és annak rendeli alá az egyes műveleti tevékenységeket. Hullámokban jövő, ami azt jelenti, hogy a védelemért felelős szervek számára a támadások elhárítása rendkívül nehezzé válik, mivel a támadások típusai és célpontjai változatosak, előre kiszámíthatatlanok és egymást követők. Ennek ráadásul komoly demoralizáló hatása is van. Multiszektoriális, tehát több iparágat érintő, ami szintén megnehezíti a védelmet, hiszen a védelmi koordináció általában csak kevés iparágat ölel fel, a legtöbb stratégiai területen nincsen kialakult információbiztonsági együttműködés.

Hírszerzési információkkal támogatott, azaz az informatikai támadásokhoz szükséges információk nem csak nyílt forrásból származnak, hanem titkosszolgálati adatgyűjtés és információelemzés is segíti azokat, valamint egyes informatikai támadások végrehajtásához emberi erőforrást is igénybe vesznek az ún. social engineering módszer keretében. Elsődlegesen károkozási célú, ami elválasztja a kiberkémkedéstől a kibertámadásokat, ugyanis ebben az esetben az a cél, hogy az állam és polgárai érezzék a támadást, azaz látványosnak kell lennie a beavatkozásoknak.

Jó példa minderre Irán esete. A már említett Stuxnet kártékony kód felhasználását egyértelműen a kiberhadviselés egyik eszközének tekinthetjük, de sajtóértesülések szerint Barack Obama elnök széles körben engedélyezte az informatikai eszközök használatát az iráni konfliktus megoldása érdekében. [7] Ezek közé tartozik az USA virtuális iráni nagykövetségének megnyitása, mely egy angol és perzsa nyelvű honlap, amin keresztül többek között az iráni állampolgárok amerikai szemszögű tájékoztatása is megvalósítható. De az ENSZ által elrendelt gazdasági szankciók kikényszerítése is kivitelezhetetlen lenne informatikai eszközök nélkül. [8] És ezek csak azok a legálisan használható elemek, melyekről jelenleg tudomásunk van. Az iráni hatóságok folyamatosan gyanúsítják az amerikai és izraeli kormányokat informatikai beavatkozásokkal, amikre válaszul az amerikai hatóságok Iránt gyanúsítják az országban található célpontok elleni támadásokkal. [9], [10] Irán tehát az első kiberháborús zóna, ahol jogilag megalapozott és nemzetközileg nem kellően szabályozott, de legalábbis nem bizonyítható forrásból érkező informatikai támadások vegyesen fordulnak elő.

Egy komplex, kiterjedt kibertámadás az iráni példa alapján szinte biztosan célba veszi az ország közigazgatási rendszereit, nagyvállalatait, médiáját és alapvető közműveit is. Ennek célja kettős. Egyrészt a célpont ország gazdasági működésének ellehetetlenítése, másrészt az uralkodó politikai osztállyal szembeni bizalmatlanság erősítése. A modern gazdaság elképzelhetetlen elektronikus információs rendszerek nélkül, így ezek támadása segíti az első cél elérését. Az alapvető ellátási láncok megbontása pedig az egész országban olyan elégedetlenséget válthat ki, ami a politikai vezetés ellen hat, hiszen nehezen magyarázható és még nehezebben bizonyítható a tömegeknek, hogy egy áramszünetet vagy az ivóvíz szennyezését külső informatikai támadó váltotta ki. Így a támadók részéről ez a megoldás lényegesen egyszerűbb, biztonságosabb és olcsóbb, mint egy hagyományos fegyveres beavatkozás.

TÁRSADALMI HATÁSOK

Egy kiberkonfliktus társadalmi hatása kiszámíthatatlan. Arra vannak hazai és nemzetközi példák is, hogyan reagál a közvélemény egy kritikus informatikai rendszer véletlen leállására, de arra vonatkozóan nincsen semmilyen tapasztaltunk, hogy egy komplex kibertámadás milyen reakciókat váltana ki. Ami bizonyos, hogy az internetes kommunikáció leállása közvetve és közvetlenül is káoszt okozna, ahogy azt a 2012-es new yorki Sandy hurrikán alatt is érezni lehetett. [11] Ekkor a távközlési szolgáltatások mellett a korunk alapvető információforrásaiként szolgáló hírportálok jó része is elérhetetlenné vált a válságterületen élő polgárok számára.

Ha nincsen internet és távközlés, akkor az elektronikus fizetési megoldások is ellehetetlenednek. Márpedig minél fejlettebb egy ország, annál kevesebb készpénzt használnak és a különböző elektronikus megoldások uralják a piacot. Ez érezhetően befolyásolja az emberek hétköznapijait, akadályozza a kereskedelmet, de ami még ennél is rosszabb, komoly hatással van a gazdaság egészére. Ráadásul az internet hiánya nem csak a banki műveleteket veti vissza, hanem más szektorokban is megmutatkozik a hatása. Jó példa erre Egyiptom esete, ahol az arab tavasz idején a kormányzat lekapcsolta az országból kimenő

internetes forgalmat. Ez az OECD becslése szerint legalább 90 millió dollár kárt okozott az országnak és komoly fennakadást jelentett az egész gazdaságnak. [12] Ha egy kiterjedt támadással kell szembenézni, az mérhető károkat okoz egy ország gazdasági teljesítményében.

Az iráni kiberháború komolyan felveti azt a lehetőséget is, hogy a támadó az ország alapvető közműveinek működését próbálja befolyásolni. A Stuxnet bebizonyította, hogy van lehetőség az ún. ipari termelésirányító rendszerek (SCADA –Supervisory Control and Data Acquisition) működésének befolyásolására. Az olyan közművek, mint a víz, gáz, áram szolgáltatások mind alapvetően függnak az ilyen rendszerektől. Eddig nem történt olyan informatikai incidens, mely széles körben érintette volna az állampolgárok közművekhez való hozzáférését, de ezzel a lehetőséggel mindenképpen számolnia kell a kibervédelem felelőseinek.

Ahogy azzal is, hogy bonyolult, informatikafüggő ellátási láncok alakultak ki, melyek nélkül az alapellátás más elemei sem működőképesek. Az élelmiszerellátás például függ a gyártói, logisztikai, közlekedési és kereskedelmi elektronikus információs rendszerektől, ha ezek bármelyike működésképtelen, akkor az alapvetően fontos árucikkek nem, vagy csak jelentős késéssel tudnak eljutni az állampolgárokhoz. Eddig ilyen támadás sem került napvilágra, de a támadás kivitelezése egyszerűbbnek tűnik, mint a közművek esetén, hiszen kevésbé védett, széles körben elterjedt információs rendszerekkel dolgoznak ezekben a szektorokban.

A kiterjedt informatikai támadások nem várt halálesetekhez is vezethetnek az összeomló informatikai rendszerek közvetett hatásaként. Itt elsősorban a mentésirányító rendszerekre kell gondolni, melyeket Magyarországon ezekben az években kívánnak modernizálni és teljesen számítógépes alapokra építeni. Amennyiben ezek nem megfelelően működnek, könnyen előfordulhat olyan káosz, mint 1992-ben a londoni irányítási rendszer esetében, ahol a nem megfelelően működő számítógépes rendszer egyes becslések szerint 20-30 megelőzhető halálesetet eredményezett, mivel a mentők nem értek időben a helyszínekre. [13]

Nem véletlen, hogy Magyarország, hasonlóan a fejlett ipari országokhoz, kiemelten kezeli a kiberfenyegetéseket. A politikai döntéshozók is felismerték kitettségünket és stratégiai kérdésként kezelik a területet. De hasonlóan a világ számos országához, a kibervédelem megfelelő szervezése hosszú folyamat, melynek csak az elején járunk. A komoly informatikai hagyományokkal rendelkező országok is elsősorban az elrettentés stratégiáját használják, hiszen a hatékony védelem sok éves fejlesztést igényel. A Magyarországhoz hasonló méretű országoknak viszont az elrettentés lehetősége nem áll rendelkezésre, így az országban található anyagi és emberi erőforrások hatékony kihasználásával kell a megfelelő eljárásokat kialakítaniuk és állampolgáraikat megvédeniük. Ahogy országunk Nemzeti Katonai Stratégiája fogalmaz, „a nem fegyverrel elkövetett, halálos áldozatot közvetlenül nem követelő, de hatalmas anyagi károkat és káoszt előidézni képes újfajta, aszimmetrikus kihívások miatt bővült a háború és a támadás fogalmainak jelentése. A károkozás mértékétől függően egy nem fegyveres támadás – megítélését tekintve – akár egy fegyveres támadással is egyenértékű lehet. Ilyen fenyegetést jelent elsősorban a kiberhadviselés, amely anyagi kár okozásában és a közrend megzavarásában potenciálját tekintve egyre kevésbé marad el a hagyományos fegyverektől.” [14]

KATASZTRÓFA- ÉS POLGÁRI VÉDELMI FELADATOK

A katasztrófavédelemről szóló törvény szerint a katasztrófa „a veszélyhelyzet kihirdetésére alkalmas, illetve e helyzet kihirdetését el nem érő mértékű olyan állapot vagy helyzet, amely emberek életét, egészségét, anyagi értékeit, a lakosság alapvető ellátását, a természeti környezetet, a természeti értékeket olyan módon vagy mértékben veszélyezteti, károsítja, hogy a kár megelőzése, elhárítása vagy a következmények felszámolása meghaladja az erre rendelt szervezetek előírt együttműködési rendben történő védekezési lehetőségeit, és különleges intézkedések bevezetését, valamint az önkormányzatok és az állami szervek folyamatos és szigorúan összehangolt együttműködését, illetve nemzetközi segítség igénybevételét igényli.” [15] Az előző fejezetekben vázolt komplex informatikai támadások eredményezhetik ezt az állapotot, bár le kell szögezni, hogy erre eddig nem volt példa világunkban. A következőkben tehát abból a feltételezésből kell kiindulni, hogy az informatikai katasztrófa helyzet reálisan bekövetkezhet, és hatása megfelel a törvényben foglalt definíciónak.

A törvény részletesen szól az állami és civil szereplők katasztrófa helyzetekben történő szerepvállalásáról. A kiberkatasztrófák esetében azonban több feladat és felelős nem egyértelműen meghatározott. Szükséges tehát ezeket a hiányosságokat pótolni! Először is tudatosítani kell, hogy a hagyományos katasztrófák könnyen lehetnek informatikai támadások következményei, azaz „egyenjogúsítani” kell a kiberkatasztrófákat más eseményekkel! Ezután gondoskodni kell arról, hogy az informatikai katasztrófák is kezelhetők legyenek a katasztrófavédelmi törvény keretében!

A Kormány feladatai többek között a következőket tartalmazzák:

- meghatározza a Kormány tagjainak és a védekezésben érintett állami szerveknek a katasztrófavédelemmel kapcsolatos feladatait,
- összehangolja a katasztrófavédelemmel összefüggő oktatási, képzési, tudományos kutatási és műszaki fejlesztési tevékenységet,
- létrehozza az országos katasztrófavédelmi információs rendszert.

Jelenleg a kibervédelem számos szerv feladata között megtalálható, nem lehet egységes, központi koordinációról beszélni. Fontos feladat az ország kibervédelmi stratégiájának elfogadása, ebben az érintett szervek feladatainak meghatározása és a szükséges erőforrások biztosítása. Amíg ez a stratégia nem készül el, az elektronikus információbiztonságról szóló törvény elfogadása is jelentős előrelépést jelentene, hiszen ez már tartalmazza a szervezett kibervédelem létrehozásához szükséges alapelveket. Szintén ez a törvény tenné lehetővé azt is, hogy az országos katasztrófavédelmi információs rendszer az informatikai incidensekről is naprakész információkat kapjon.

A kibervédelemben élen járó országok mintájára és a törvény szellemében meg kell teremteni az oktatási és kutatás-fejlesztési kapacitásokat erre a területre is! A Nemzeti Közszolgálati Egyetemen komoly hagyománya van mind a kibervédelmi, mind a katasztrófavédelmi oktatásnak, ez jó bázist biztosíthatna egy komoly, európai léptékben is jelentős oktatói-kutatói bázis létrehozására és fenntartására. Ennek keretében végrehajtható lenne a kritikus információs infrastruktúrák felmérésének feladata is, melyek védelme a katasztrófák elleni védekezésért felelős miniszter feladatai között szerepel.

A központi államigazgatási szerv vezetőjének feladatai között a következők szerepelnek:

- a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszterrel egyeztetve végrehajtja a katasztrófavédelmi célú távközlési, informatikai, valamint ágazati mérő- és ellenőrző rendszerek egységes irányítási rendszerbe illeszkedő kialakítását és működtetését,

- kijelöli az ágazat katasztrófavédelemben részt vevő szerveit és a katasztrófavédelemben bevonható gazdálkodó, valamint az önkéntesen jelentkező civil szervezetek közül az állandó együttműködésre alkalmas és a helyi részvételnél átfogóbb tevékenységre is képes szervezeteket, meghatározza a katasztrófavédelemmel kapcsolatos feladataikat, jogszabály alapján intézkedik felkészítésükre és a működési feltételeik megteremtésére.

Komplex kibertámadások esetén a korábbi fejezetben írtak szerint a távközlési és informatikai hálózatok is célpontok lehetnek. Mindenképpen érdemes tehát végiggondolni azt a helyzetet, hogy ezek a rendszerek nem megfelelően működnek! Különösen azért, mert a közelmúltban az Egységes Digitális Rádiótávközlő Rendszer (EDR) leállításáról számolt be a sajtó, így nem elképzelhetetlen, hogy a védelemért felelős szervezeteknek az EDR működésképtelensége mellett kell dolgoznia. [16]

A kibervédelem területén működnek olyan civil szervezetek, melyek katasztrófa-helyzetben bevethek lennének, de ezek pontos feladatai egy ilyen szituációban nem egyértelműek. Az Önkéntes Kibervédelmi Összefogás (KIBEV) céljai között például a következő tétel is szerepel: „a KIBEV felajánlja az állam számára tagjainak szaktudását és tettekkészségét abból a célból, hogy a haza kibertereének védelmét szolgálja”. Az ilyen civil szervezeteket hatékonyan lehet bevonni a katasztrófa- és polgári védelem különböző területeire.

A megyei, fővárosi és helyi védelmi bizottság „szervezi a lakosság és a védekezésben érintett szervezetek riasztásának és tájékoztatásának előkészítését és végrehajtását”, a megyei, fővárosi védelmi bizottság elnöke pedig „felelős a riasztás, tájékoztatás előkészítéséért és végrehajtásáért, gondoskodik a lakosság és a gazdálkodó szervezetek riasztásához, tájékoztatásához szükséges eszközök működtetéséről”. A digitális világban azonban ez nem egyszerű feladat. Egy összehangolt kibertámadás ugyanis a médiafelületeket is érintheti, így nem könnyű eljuttatni a hiteles tájékoztatást a lakosság felé. A lakosság számára napjainkban a hírek elsődleges forrása az internet és az elektronikus hírközlő médiumok. Élve a feltételezéssel, hogy a legolvasottabb internetes honlapok is támadás áldozatai lesznek, azaz nem érhetők el, vagy feltörésük után hamis információkat közölnek, ezek nem megfelelő források. Ide kell érteni a Magyar Távirati Irodát is, mely szintén e-mailek és a weboldala segítségével juttatja el a szükséges információt a médiumoknak. A tévék és rádiók alapvetően ezekből a forrásokból táplálkoznak, így ide sem könnyű eljuttatni a megfelelő híreket. Ráadásul szinte minden helyen tisztán informatikai eszközökkel készítik a műsorfolyamot, ami szintén egy kiváló lehetőség a külső beavatkozásra. A digitális átállás pedig előbb-utóbb magával hozza azt is, hogy a műsorszórás is elképzelhetetlen lesz informatikai eszközök nélkül.

Több ország a helyi hírközlők kiesése miatt a Facebook és Twitter oldalakat választotta vészhelyzeti közlésekre. Így tett a Budapesti Közlekedési Központ is, mely a 2013. január eleji havazás idején az elérhetetlen saját weboldala helyett a Facebookot választotta elsődleges közlési felületnek. Viszont ha nincsen megfelelő internet-elérés, akkor ezek a csatornák is elérhetetlenné válnak. Mindenképpen végig kell tehát gondolni, hogyan biztosítható napjainkban a tömeg-tájékoztatás feladata megfelelő internetes és informatikai eszközök nélkül!

A megyei, fővárosi védelmi bizottság elnöke „folyamatosan értékeli a kialakult helyzetet, a védekezés helyzetét, minderről jelentést tesz a ... miniszteri biztosnak és tájékoztatja a kormányzati koordinációs szervet”. Ez feltételezi, hogy az incidens mértékéről és jellegéről megfelelő információk állnak rendelkezésre helyi és országos szinten is, azaz a védekezésért felelős szervezetnél megvalósul a szituációs tudatosság (situational awareness). Ehhez viszont szükség van a támadások célpontjaitól, elsősorban a kritikus információs infrastruktúrák üzemeltetőitől származó információkra, még hozzá közel valós időben. Ez egyfajta központi

információs rendszert feltételez, melybe előre meghatározott rend szerint érkeznek az információk. Természetesen előzetesen definiálni kell azt, hogy milyen incidenseket kell jelenteni, milyen részletezettséggel, hogyan lehet az üzleti titkokat védeni és hogyan lehet az információk hitelességét biztosítani. Foglalkozni kell továbbá a lakossági bejelentések fogadásával is, hiszen nem elképzelhetetlen, hogy a káosz fokozása érdekében a támadó egy, a lakosságot széles körben érintő, kártékony kódokat felhasználó támadást is indít.

A polgármester „részt vesz a feladatainak ellátása érdekében, a hivatásos katasztrófavédelmi szervek által szervezett felkészítéseken”, valamint „kijelöli a katasztrófák elleni védekezéssel összefüggő feladataiban közreműködő közbiztonsági referenst”, aki a „polgármester katasztrófák elleni védekezésre való felkészülési, védekezési, helyreállítási szakmai feladataiban, továbbá rendvédelmi és honvédelmi feladataiban közreműködő, köztisztviselői jogviszonyban álló, e feladat ellátására a polgármester által kijelölt, e törvény végrehajtási rendeletében meghatározott végzettséggel rendelkező személy”. Az egyértelmű, hogy egy kiberkatasztrófa esetén a katasztrófális hatást nem az informatikai rendszer hiánya, hanem az abból következő események jelentik. Azonban nagyon fontos, hogy a törvény szerint a polgármester és az általa kinevezett közbiztonsági referens legalább a kiberbiztonság alapvető fogalmával tisztában legyen, hogy jobban megérthessék egy kiberkatasztrófa mibenlétét. A szervezett oktatásokon tehát, ha röviden is, de érdemes kitérni arra, hogy mit jelentenek napjainkban az informatikai rendszerek, és milyen hatással lehetnek ezek kimaradásai. Hasznos lehet olyan katasztrófavédelmi gyakorlatok szervezése, melynek során akár kiváltó okként, akár egy elemként megjelenik a kibertámadás. Az elektronikus információbiztonságról szóló törvény tervezete foglalkozik az oktatás kérdésével, ennek keretében a katasztrófavédelemért felelős személyek rövid képzése is megvalósítható lenne!

Mivel a tanulmányban felvázolt kibertámadási forgatókönyv elsősorban a kritikus információs infrastruktúrákat célozná, elsődleges felelőssége van az azokat működtető gazdasági társaságnak az elhárításban. A törvény többek között az alábbi feladatok rója az ilyen szervezetekre:

- hatósági határozatban megjelölt, polgári védelmi kötelezettségen alapuló települési és munkahelyi polgári védelmi szervezetet hoz létre, kijelöli a munkahelyi polgári védelmi szervezet tagjait, és beosztásuk esetén gondoskodik a felkészítésükről, valamint a szervezet működtetéséről,
- szervezi és irányítja az alkalmazottak katasztrófavédelmi felkészítését.

Informatikai támadások esetében az elsődleges elhárítás egyébként is a szervezetre hárul, ahol általában egy helyi IT biztonsági koordinátor felelős az informatikai védelemért. Feladata hármas: koordinálnia kell a belső védelmet, kapcsolatot kell tartania a külső felekkel és részt kell vennie az alkalmazottak felkészítésében is. A katasztrófavédelmi tudás azonban speciális ismereteket igényel, így hasonlóan a polgármester és a közbiztonsági referensek oktatásához, a kritikus információs infrastruktúrák vezetőit és biztonsági felelőseit is megfelelő képzésben kell részesíteni az elektronikus információbiztonsági törvény tervezetének elvei alapján.

Ki kell még emelni az alkalmazottak felkészítésének fontosságát. Amennyiben az alkalmazottak hiteles, pontos és szakszerű felkészítést kapnak, és rajtuk keresztül ez az információ családtagjaikhoz, ismerőseikhez is eljut, egy kiberkatasztrófa miatt bekövetkező társadalmi pánik nagysága csökkenthető, jobban kézben tartható. A nagyvállalatok többségében jellemzően tartanak olyan információbiztonsági tudatossági oktatásokat, melyeknek keretében a kiberkatasztrófákról is szót lehet ejteni, így előzetesen is fel lehet készíteni a lakosság egy részét arra a tényre, hogy az informatikai rendszerek sérülése és annak továbbgyűrűző hatása reális lehetőség.

Szóba kerültek már azok a civil szervezetek, önkéntesek, akik hatékonyan tudnak eljárni egy kiberkatasztrófa elhárításában. A törvény szerint „az önkéntesen segítséget nyújtó személyek az adott feladat végrehajtásáért felelős személy irányításával látják el a számukra meghatározott feladatot”. Az információbiztonság területén olyan szakmai szervezetek és kapcsolatrendszer áll rendelkezésre, melyen keresztül hatékonyan lehet mozgósítani 1000-2000 szakembert. Ezeket az együttműködéseket azonban ki kell dolgozni és meg kell találni hatékony alkalmazásuk lehetőségeit!

Ki kell még térni a polgári védelem lehetőségeire is! A polgári védelem „olyan állami feladat-, eszköz- és intézkedési rendszer, amelynek célja katasztrófa, illetve fegyveres összeütközés esetén a lakosság életének megóvása, az életben maradás feltételeinek biztosítása, valamint a lakosság felkészítése azok hatásainak leküzdése és a túlélés feltételeinek megteremtése érdekében”. Bár nehezen elképzelhető egy olyan összetett támadás, amely olyan szinten terjed ki, hogy polgári védelmi aktivitásra lenne szükség, de például egy olyan támadás, mely magyar állampolgárok informatikai eszközeit (számítógépeit, okostelefonjait) tömegesen támadja, és ezekről indulnak a kritikus információs infrastruktúrákat érintő támadások, indokoltá teheti azt, hogy élni lehessen a polgári védelmi kötelezettség élesítésével. A hagyományos katasztrófa-elhárítás mellett érdemes megemlíteni, hogy Magyarországon több tízezer informatikával hivatásszerűen foglalkozó állampolgár él, akik adott esetben részt tudnak venni a lakosságot érintő informatikai incidensek elhárításában, ezzel hozzá tudnak járulni a közvetett katasztrófaesemények kivédésében.

ÖSSZEFOGLALÁS

Ma még megjósolhatatlan, hogy valaha is szembesülni fogunk-e olyan kibertámadással, mely érezhető hatással lesz az állampolgárok tömegei számára, illetve közvetett hatásain keresztül életük kerülnek veszélybe. El kell azonban fogadni azt, hogy mindaz, amit a tanulmány megfogalmaz, a valóságban is bekövetkezhet, hiszen egyes elemei mind megtörténtek – szerencsére eddig nem pusztító szándékkal. A politikai vezetés a kockázatot felismerte, annak hatékony kezelése azonban egyelőre kezdeti stádiumban van.

A katasztrófavédelmi törvény egyes lépései analóg módon átültethetők a kiberkatasztrófákra is, így csekély anyagi ráfordítással hatékonyan lehet felkészülni a kibertámadások kezelésére is. Jelen gondolat kísérlet több javaslatot tartalmaz a törvény kibervédelmi felhasználására, de legfontosabb feladatként az elektronikus információbiztonságról szóló jogszabály elfogadását jelöli meg. Még nem késő elkezdni a felkészülést, a döntést viszont minél előbb meg kell hozni arról, hogy a legfejlettebb országokhoz hasonlóan létfontosságúnak tartjuk-e információs rendszereinket!

Felhasznált irodalom

- [1] Magyar Kormány: A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny, 19. (2012) 1383.
- [2] Kovács, L., Krasznay, Cs.: Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság III., 1. (2010) 44-56.
- [3] Krasznay, Cs.: A magyar elektronikus közigazgatási alkalmazások információbiztonsági megoldásai. Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskola, 2011.
- [4] Kovács, L., Sipos, M.: A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. Hadmérnök V., 4. (2010) 163-172.

- [5] Tang, L., Zhang X.: Can Cyber Deterrence Work? In: A. Nagorski (Eds.), *Global Cyber Deterrence – Views from China, the U.S., Russia, India, and Norway*. EastWest Institute, 2010.
- [6] Kyodo, J.: Japanese websites come under attack as Senkaku squabble continues. The Japan Times Online, (2012. szeptember 20.). Forrás: <http://www.japantimes.co.jp/text/nn20120920b7.html>, letöltve: 2013. január 15.
- [7] Sanger, D. E.: Obama Order Sped Up Wave of Cyberattacks Against Iran. The New York Times (2012. június 1.). Forrás: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>, letöltve: 2013. január 15.
- [8] Cordesman, A. H., Bosserman, B., Khazai, S., Gold, B.: U.S. and Iran Strategic Competition – Sanctions, Energy, Arms Control, and Regime Change. Center for Strategic and International Studies, 2012.
- [9] Gladstone, R.: Iran Suggests Attacks on Computer Systems Came From the U.S. and Israel. The New York Times (2012. december 25.). Forrás: <http://www.nytimes.com/2012/12/26/world/middleeast/iran-says-hackers-targeted-power-plant-and-culture-ministry.html>, letöltve: 2013. január 15.
- [10] Leyden, J.: US gov blames Iran for cyberattacks on American banks. The Register Online (2013. január 9.). Forrás: http://www.theregister.co.uk/2013/01/09/us_banks_ddos_blamed_on_iran/, letöltve: 2013. január 15.
- [11] Kolbert, A.: Az internet örök, nem az, ami fut rajta. Index, (2012. november 13.). Forrás: http://index.hu/tech/2012/11/13/az_internet_orok_csak_ami_van_rajta_az_nem/, letöltve: 2013. január 15.
- [12] Organisation for Economic Co-operation and Development (OECD): The economic impact of shutting down Internet and mobile phone services in Egypt. OECD (2011. február 4.). Forrás: <http://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm>, letöltve: 2013. január 15.
- [13] Adamu, M., Alkazmi, A., Alsufyani, A., Al Shaigy, B., Chapman, D., Chappell, J.: London Ambulance Service Software Failure. University of Kent, 2010.
- [14] Magyar Kormány: 1656/2012. (XII. 20.) Korm. határozat. Magyarország Nemzeti Katonai stratégiájának elfogadásáról. Magyar Közlöny, 175. (2012) 29710.
- [15] Magyar Kormány: 2011. évi CXXXVIII. törvénya katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról. Magyar Közlöny, 113. (2011) 28842-28891
- [16] Magyar Távirati Iroda: Rejtély, mi okozta mentő-rendőr-tűzoltó rádiós rendszer leállítását. HVG Online (2013. január 7.). Forrás: http://hvg.hu/itthon/20130107_Rejtely_mi_ozokta_mentorendortuzolto_ra, letöltve: 2013. január 15.
- [17] HVG.hu: Leállt a BKK honlapja, a Facebookot használják. HVG Online (2013. január 14.). Forrás: http://hvg.hu/itthon/20130114_Leallt_a_BKK_honlapja, letöltve: 2013. január 15.

VII. Évfolyam 4. szám - 2012. december

Nagyné Takács Veronika

takacs.veronika@nav.gov.hu

A KÖZIGAZGATÁSI INFORMATIKAI RENDSZEREK FEJLESZTÉSÉVEL KAPCSOLATOS FELHASZNÁLÓI ELVÁRÁSOK

Absztrakt

Az elektronikus közigazgatás térhódítása következtében különböző szinteken egyre újabb elvárások fogalmazódnak meg az informatikai fejlesztés és üzemeltetés irányában. A cél színvonalas, felhasználóbarát és biztonságos elektronikus szolgáltatások nyújtása a társadalom egésze számára. A követelmények megfogalmazása és teljesítése széles körű együttműködést igényel.

As a result of the spread of e-government, more and more expectations are appear referring to IT development and management. The main goal is to create high quality, user-friendly and secure electronic services to the whole society. The formulation and performance require wide-ranging collaboration.

Kulcsszavak: *e-közigazgatás, elektronikus közszolgáltatások, kihívások és követelmények ~ e-Government, electronic public services, challenges and requirements*

BEVEZETÉS

A közigazgatás informatikai meghatározottsága vitathatatlan tény. Ahogyan az is, hogy a korszerű infokommunikációs technológiák közigazgatáson belüli elterjesztésének kulcsszereplői egyrészt az informatikai stratégiá(ka)t kidolgozó, tervező informatikai szakemberek, másrészt a közigazgatási szervek informatikai szakterületeinek szakképzett munkatársai, akik a folyamatosan fejlődő információtechnológiai környezetben meghatározzák, kifejlesztik, vagy a piacon megjelenő megoldások közül kiválasztják és testreszabják, majd üzembe adják és működtetik (üzemeltetik, valamint folyamatosan korszerűsítik) azokat az infokommunikációs eszközöket, módszereket és eljárásokat, amelyek a közigazgatási szervek tevékenységének ellátásához szükségesek, sőt nélkülözhetetlenek.

A közigazgatási informatikai tevékenység rendeltetése a közigazgatás alapvető működési irányjaiban jelentkező folyamatok, azaz a *front office* tevékenység (ügyfélkapcsolatok) és a *back office* tevékenység, a belső hivatali működés, valamint a közigazgatási szervek közötti együttműködés korszerű információtechnológiai eszközökkel történő támogatása.

Fentiekből következően az informatikai szakterület szolgáltató: gondoskodik a felhasználók által megfogalmazott igények kielégítését biztosító technológiák - infrastruktúrák, alkalmazások - rendelkezésre bocsátásáról és folyamatos rendelkezésre állásáról.

Az informatikai tevékenység akkor lehet eredményes, ha a vele szemben támasztott felhasználói elvárások egyértelműek, konzisztensek és reálisak. Ez a kíváncsi viszont úgy teljesülhet, ha a tág értelemben vett felhasználói kör az igényeit tudatosan, tervezetten és lehetőség szerint szabályozott formában továbbítja a szolgáltató felé.

Az informatikai fejlesztési igények felhasználói szintű megfogalmazása csak akkor vezethet a kívánt eredményre, ha az informatikai szakterület irányában megfogalmazott „megrendelés” a társadalmi és a szervezeti (nem-informatikai) adottságok, képességek pontos ismeretén és elemzésén, továbbá a lehetőségek alapos és elfogulatlan mérlegelésén alapul; az informatikától pedig nem csodát, hanem tervezett, ütemezett (kiszámítható) támogató tevékenységet és működést vár.

Jelen tanulmány a társadalmi – stratégiai szinten megfogalmazódó – elvárások és célkitűzések vázlatos ismertetése után a szervezeti szinten jelentkező aktuális igényeket és az ezek teljesítésével kapcsolatos informatikai megfontolásokat tekinti át.

STRATÉGIAI ELVÁRÁSOK ÉS CÉLKITŰZÉSEK

A tág értelemben vett felhasználói igények legfelső rétege az információs társadalom fejlesztéséhez szükséges stratégiai elvárások, amelyek megjelenhetnek nemzeti és nemzetközi szinten is. Ahogyan az Európai Unió egyik dokumentuma fogalmaz, az infokommunikációs technológiák a „társadalmi integráció, a jobb közszolgáltatások és a javuló életminőség” eléréséhez nyújthatnak segítséget. [1]

A stratégiai célok leképezésének egyik kiemelt területe a közigazgatás működésével kapcsolatos elvárások definiálása. Ezek érkezhettek a közigazgatás, a vállalkozások és az állampolgárok részéről is, és vonatkozhatnak a már említett működési irányok bármelyikére.

A közigazgatás informatikai fejlesztéssel kapcsolatos igényei kormányzati (és önkormányzati) dimenzióban, illetve az egyes közigazgatási szervek szintjén is megjelennek, a nézőpontból fakadóan eltérő tartalommal. Míg az előbbire elsősorban a stratégiai tervezés jellemző, az utóbbi esetében már jelentős hangsúlyt kaphat a napi működéssel kapcsolatos – operatív, akár eszköz-, módszer- és eljárás-szintű – igény-megfogalmazás is.

Kormányzati elképzelések

A Nemzeti Fejlesztési Minisztérium 2010-ben kiadott Digitális Megújulás Cselekvési Terve a nemzetközi trendek, az Európai Unió célkitűzései és a hazai helyzet áttekintését követően négy célcsoportban tartalmazza a társadalom infokommunikációs fejlettségi szintjének növelése érdekében szükséges akciókat. A harmadik intézkedési főirány – Hatékonyan és biztonságosan működő, szolgáltató állam – a tág értelemben vett közigazgatási informatikai feltételrendszer konszolidálása, valamint a közigazgatási informatikai tevékenység központosítása és egységesítése irányában ható intézkedéseket határoz meg.

A teendők teljes körű ismertetése meghaladná jelen munka kereteit, figyelmet érdemel azonban az *Államigazgatási folyamatok korszerűsítése* alfejezet, amely az informatikai fejlesztés kiindulópontjaiként a jogszabályi környezet konszolidációját és a szakmai folyamatok korszerűsítését határozza meg, továbbá az informatikai rendszerterv elkészítése feltételének tekinti „a hazai és uniós jogszabályokra épülő igazgatási rendszerterv” megrendelő és szállító általi (azaz közös!) elkészítését. [2]

A Közigazgatási és Igazságügyi Minisztérium által 2011-ben közzétett, *Magyary Zoltán Közigazgatás-fejlesztési Program* szerint „[a program] fontos része az e-közigazgatási szolgáltatások körének bővítése és minőségének javítása, mind a közigazgatás ügyfelei és a tisztviselők munkájának megkönnyítése, mind az eljárások és szervezeti folyamatok egyszerűbbé és gyorsabbá, így hatékonyabbá tétele érdekében”. [3]

A dokumentum a fejlesztések sikerességét biztosító alapelvek között nevesíti a közigazgatási informatika közigazgatást kiszolgáló jellegét, az infrastruktúra, az alkalmazások és az emberi erőforrások fejlesztése együtt haladását, az informatikai fejlesztés során a lehető legnagyobb fokú központosítást, a közigazgatás saját (tisztviselőkből álló) informatikusi személyzetének biztosítását, valamint a kormányzati feladatellátás és az informatikai fejlesztés egymáshoz viszonyított arányosságát.

A *Magyary Program*ban ismertetett konkrét kormányzati döntések a kormányzati szintű konszolidációs és egységesítési törekvéseket képviselik (nagy kormányzati elszámoló rendszerek konszolidációja, kormányzati hálózatbiztonság és védelmi képesség helyreállítása, egységes kormányzati dokumentum- és iratkezelési rendszer alkalmazása stb.).

A közigazgatás ügyfeleinek elvárásai

A közigazgatás optimális esetben ügyfelei elvárásainak pontos ismeretében, ez utóbbiakra is tekintettel fogalmazza meg fejlesztési stratégiai céljait.

A vállalkozások és az állampolgárok legfontosabb elvárásai az *ügyfelek adatainak jogszerű és biztonságos kezelése*, a bürokratikus működést felváltó *ügyfélbarát megoldások* bevezetése: az *adminisztrációs terhek csökkentése*, a *közigazgatási szervekkel történő kapcsolattartás többszorosára tétele* és az *ügyfelek esélyegyenlőségének biztosítása az eljárásokban*.

A közigazgatási szervek ügyfeleik adatait jogszabályi felhatalmazás alapján és jogszabályi garanciák mellett, az érintettek tudtával, beleegyezésével, a közigazgatási feladatellátáshoz szükséges mértékben, módon és ideig kezelhetik.

Az adminisztrációs terheket könnyítheti az ügyféli adatszolgáltatás és az ügyfelek által kezdeményezendő engedélyezési (bejelentési) eljárások számának csökkentése és maguknak az eljárásoknak az egyszerűsítése. Klasszikus példa a párhuzamos adatszolgáltatási kötelezettségek megszüntetése (a közigazgatás a közigazgatásban már „valahol” meglevő adatot ismételtelen ne kérje be), aminek informatikai feltétele a közigazgatási szervek adatbázisai közötti folyamatos és zavartalan – adat- és információvédelmi követelményeket is teljesítő – kapcsolat kiépítése.

A közigazgatási szervekkel való kapcsolattartás egyszerűsítésének területei a sokcsatornás kapcsolattartási lehetőség megteremtése, a papíralapú ügyintézés helyett az elektronikus kapcsolattartási eszközök, módszerek elterjesztése és az esélyegyenlőség biztosítása. A

sokcsatornás kapcsolattartás során az ügyfél maga választhatja meg a kommunikáció módját (ami a személyes ügyintézésen túl jellemzően az internet és a mobiltelefon igénybevételezt jelenti). Az elektronikussá váló ügyintézés terjedésében az ügyfelek számára elérhető és kényelmesen, könnyen igénybe vehető (!) informatikai szolgáltatások (elektronikus nyomtatványok, hitelességet biztosító elektronikus azonosítás és aláírás, elektronikus fizetés stb.) játszanak meghatározó szerepet.

Az esélyegyenlőség biztosítása érdekében a közigazgatás nyújtana ügyintézésbeli támogatást a különböző okok miatt hátrányos helyzetű ügyfelei számára (az érintett körbe tartoznak a fogyatékkal élők, de ma már a digitális írástudással nem rendelkezők is).

A KÖZIGAZGATÁSI INFORMATIKA FEJLESZTÉSI TERÜLETEI ÉS FEJLETTSÉGI MUTATÓI

Az informatikai tervezés, fejlesztés akkor eredményes, ha a kívánt eredményre vezet, azaz valóban modernizálja, hatékonyabbá teszi a közigazgatás működését.

A tervezéshez és a fejlesztéshez a stratégiai irányok, fejlesztendő területek korrekt meghatározására, az elvégzett informatikai tevékenység értékeléséhez a közigazgatási hatékonyság növekedésének mérésére van szükség.

Az Európai Unió követelményrendszere

Az Európai Tanács 2000. márciusban fogadta el a Lisszaboni Stratégiát, amely Európát a legversenyképesebb és legdinamikusabb gazdasági térséggé kívánta fejleszteni 2010-ig. A stratégia alapján a Bizottság három alapvető célt és tíz cselekvési területet meghatározó akciótervet dolgozott ki, amely a közigazgatás fejlesztése területén az online közigazgatás megteremtését (a közszolgáltatások elektronikus elérhetőségének biztosítását) tűzte ki célul. [4]

Az első akciótervet további stratégiai tervek és az előrehaladást összefoglaló dokumentumok követték, és bár az évtized közepére az eredetileg nagyon ambíciózus célkitűzéseket mérsékelni kellett, az *eEurope*-dokumentumokban az infokommunikációs prioritásokat egyre pontosabb megfogalmazásban rögzítették, és kialakítottak (majd korszerűsítettek) egy indikátor-rendszert is a tagállamok eredményeinek mérése és összehasonlítása érdekében.

Az Európai Tanács 2001. márciusi, stockholmi értekezletére meghatározták azon közigazgatási szolgáltatásokat, amelyekben az *online elérést* biztosítani és fejleszteni kell (*Alapvető közszolgáltatások jegyzéke* - Common list of basic public services, CLBPS). [5] Ugyancsak rögzítették azokat a fejlettségi (szofisztikációs) szinteket, amelyek teljesítésével az előrehaladás mérhető.

Az *Alapvető közszolgáltatások jegyzéke* az állampolgárok viszonylatában 12 fejlesztendő szolgáltatást nevesít: jövedelemadó-bevallás, munkaügyi hivatalokon keresztül álláskereső, társadalombiztosítási kifizetések (munkanélküli járadék, gyermekek utáni juttatások, gyógyítási költségek, felsőoktatási ösztöndíjak), személyi okmányok (útlevél, vezetői engedély), gépjármű-nyilvántartás, építési engedély iránti kérelem, rendőrségi bejelentés (pl. lopás esetén), közkönyvtárak (katalógusok, keresőeszközök elérése), anyakönyvek (születési, házassági, igénylés és kézbesítés), felsőoktatási/egyetemi jelentkezés, lakcímváltozás bejelentése, egészségügyi szolgáltatások (interaktív tájékoztatás az egyes kórházakban elérhető szolgáltatásokról, bejelentkezés). A vállalkozások számára fejlesztendő 8 szolgáltatás a jegyzék szerint: munkavállalók után fizetett hozzájárulások, társaságiadó-bevallás, ÁFA-bevallás, cégbejegyzés, statisztikai hivatal részére adatszolgáltatás, vámnyilatkozat, környezetvédelemmel kapcsolatos engedélyek, közbeszerzés.

Az online közszolgáltatás öt fejlettségi szintet érhet el. Az eredetileg meghatározott négy szofisztikáltsági fokozat az online információszolgáltatás, az egyirányú interakció (letölthető nyomtatványok hozzáférhetővé tétele), a kétirányú interakció (elektronikusan kitölthető és továbbítható űrlapok biztosítása) és a tranzakció (teljes körű online ügyintézés, beleértve a kézbesítést és a fizetést is). 2007-ben egy tanulmányban jelent meg először az ötödik szint, a personalizáció (proaktív és automatizált szolgáltatások nyújtása a közigazgatás részéről). Ezen a szinten a közigazgatási szervek a szolgáltatás színvonalának növelése és az ügyfélbarát jelleg erősítése érdekében már proaktív módon hajtanak végre egyes műveleteket (pl. előre kitöltik a benyújtandó űrlapokon azon adatokat, amelyek a közigazgatási szervek adatbázisaiban már rendelkezésre állnak), vagy egyes (jellemzően szociális vagy gazdasági jogot érintő) szolgáltatást automatikusan nyújtanak, nincs szükség arra, hogy az állampolgár (és később a vállalkozás) azt külön igényelje. [6]

Az előrehaladás 2001 óta a tagállamok éves adatszolgáltatásai alapján követhető nyomon, azonban az adatok a közigazgatás nyújtotta lehetőségeket, nem pedig az elektronikus közszolgáltatások tényleges igénybevételi mértékét tükrözik. [7]

A tapasztalatok alapján a nyomon követéssel kapcsolatos eredeti elvárások módosultak; megjelent a tényleges használat [8] és az ügyfél-elégedettség kimutatásának igénye is. Hangsúlyossá vált az a meggyőződés, hogy a *front office* folyamatok megújítása nem lehet eredményes a *back office* folyamatok újraszervezése nélkül. [9]

További mérési módszertanok

A közigazgatási modernizáció (hatékonyság-növelés) mérésére többféle – nemzetközi kutatóintézetek, nemzetközi szervezetek által kidolgozott és alkalmazott – módszertan létezik.

A legkomplexebb az ENSZ E-közigazgatási Felmérő Programja, amely évente 191 tagállam e- közigazgatási készenléti indexét rangsorolja. [7]

Árnyaltabb képet biztosíthatnak azon mutatók, amelyek bemeneti és kimeneti adatok mellett vagy helyett értékelést is tartalmaznak (eredményindikátorok, hatásindikátorok stb.); [10] tartalmuk és jelentőségük értékelése meghaladná jelen tanulmány kereteit.

A KÖZIGAZGATÁSI SZERVEN BELÜLI FELHASZNÁLÓI IGÉNYEK

Az egyes közigazgatási szerveken belül fejlesztési igények – természetesen igazodva a korábban említett elvárásokhoz – már lényegesen gyakorlatiasabb szemléletűek, és a szervezet működése, valamint a szervezet alkalmazottainak személyes kompetenciái és elvárásai alapján is megközelíthetők.

Az informatikai támogatás területei

A felhasználók által elvárt informatikai támogatás részterületei – a tevékenység szolgáltató jellegéből következően – a szervezet munkafolyamatai szerint is meghatározhatók.

Ma már evidencia a közigazgatási szerv alkalmazottai számára a megfelelő *irodai alkalmazáscsomag* (szövegszerkesztő, táblázatkezelő, prezentációkészítő és elektronikus levelezés) és a biztonságos *internet-elérés biztosítása*.

A szervezet alaptevékenységét jelentő *szakmai folyamatok támogatása* egyrészt a feladatok végrehajtását segítő *tranzakciós* vagy *eljárási rendszerek*, *alkalmazások biztosítását* jelenti. A közigazgatási szerv nagysága, tevékenységének összetettsége határozza meg azt, hogy egy integrált (minden szakmai részfolyamatot kiszolgáló) vagy több együttműködő rendszer, alkalmazás fenntartása indokolt.

Az *eljárási rendszerek* gyűjtik, feldolgozzák a közigazgatási szerv feladatellátásához szükséges adatokat, a feldolgozott adatok alapján lehetővé teszik formalizált dokumentumok

(pl. határozatok) létrehozását, tárolását és visszakeresését (dokumentumsablonok, dokumentumtárak).

Az egyre nagyobb tömegben rendelkezésre álló *adatok* egyes szakterületek igényei szerinti, lehetőség szerint automatizált és ütemezett, *értékelő-elemző feldolgozása* (adatelemzés és adatbányászat), *riportok készítése* az informatikai támogató tevékenység kiemelten fejlődő területe.

Az említett belső folyamatok mellett a közigazgatási szervek jelentős hányadánál a szakmai tevékenység hangsúlyos területe az ügyfélkapcsolat-kezelés. Ezen a területen a *közigazgatási szerv és az ügyfelek közötti kommunikáció különböző csatornáinak működtetése* (call center- és honlap-üzemeltetés, speciális alkalmazások, pl. nyomtatványkitöltők biztosítása) bír nagy jelentőséggel.

Az alaptevékenység ellátásához, a szervezet működtetéséhez szükséges *funkcionális folyamatok támogatása* során alapvetően a *pénzügyi, eszközgazdálkodási, humánpolitikai, irat-, dokumentum- és tartalomkezelő rendszerek, alkalmazások beszerzése, fejlesztése és üzemeltetése* az informatikai szakterület feladata.

A *szervezet vezetési folyamatainak támogatása* elsősorban a *döntéshozatalhoz szükséges információk* erre a célra kifejlesztett szoftverek, webes szolgáltatások és minialkalmazások révén történő *szolgáltatását* jelenti. Elvárás a könnyen kezelhető „vezetői műszerfal” (dashboard), amely a szükséges adatokat, ismereteket naprakészen és gyorsan értelmezhető formában (szövegesen és grafikusan) is biztosítja.

Az előzőekben említett működési irányok szervezeten túlmutató dimenzióval is rendelkeznek, a *felettes, az alárendelt és a társszervekkel folytatott együttműködés informatikai támogatása* a partnerszervezetek informatikai szakterületeinek együttműködését is feltételezi.

A szervezeten belüli *közösségi tevékenység támogatása* jellemzően a közigazgatási szerv belső hálózatán, az *intraneten kialakított hirdetőtáblák, blogok, általános információs tartalmak elérésének biztosításával* kapcsolatos feladatok ellátása.

A *felhasználók informatikaeszköz-használatának támogatása* folyamatos *szervizszolgáltatás*, speciális alkalmazásokkal (hibabejelentő rendszer, távfelügyelet, távmenedzsment stb.), valamint a közigazgatási szerv belső működési rendjével összhangban levő *hozzáférés-menedzsment és jogosultságkezelés*.

Az *informatikai tevékenység támogatása* az informatikai infrastruktúra és alkalmazások üzemeltetésével összefüggő – felhasználók számára csak az eredmény szempontjából releváns – szolgáltatások összessége.

A felhasználói szokások változásai

A személyes használatú infokommunikációs eszközök térnyerésével és folyamatos megújulásával, a digitális írástudás terjedésével a felhasználói szokások, elvárások is átalakulnak.

Egyre nagyobb a *mobilitás* – a *mobil eszközök (okostelefonok, táblagépek) alkalmazásának igénye*. Ezek az eszközök lehetővé teszik (tehetik) a munkahelyen kívüli munkavégzést, és így felmerül a munkahelyen megszokott és használt adatok és alkalmazások távoli (helytől független) elérésének szükségessége is.

A felhasználók közvetlen informatikai munkakörnyezetüket saját, egyedi igényeik szerint kívánják kialakítani, megnő az „*önkiszolgáló*” *megoldások*, a *testreszabott és a saját elvárásoknak megfelelően választható alkalmazások és kisalkalmazások iránti kereslet*.

Az alkalmazások hasznossága mellett egyre nagyobb szerepet kap a *használatosság (a kényelmes használat) követelménye*. A felhasználóbarát felületek és interakciók könnyítik az új alkalmazások meghonosítását, elfogadását, és gyorsíthatják a munkavégzést is, míg a nehézkes, nem szabványos kezelőfelület csökkenti a hatékonyságot.

A felgyorsult élet- és munkatempó miatt elvárás az információk megszerzése és továbbítása folyamatának felgyorsítása is, a felhasználói szempontból időpazarlónak tűnő *adminisztratív és védelmi eljárások időtartamának lerövidítése*.

INFORMATIKAI FEJLESZTÉSI MEGFONTOLÁSOK

A társadalmi és gazdasági környezet az informatikai támogató tevékenységgel szemben a felhasználói szükségletek és igények folyamatos és gyors kielégítésének, a korszerű és költséghatékony működés biztosításának - sokszor önmagában is ellentmondó - követelményeit fogalmazza meg.

A 2008 végétől kibontakozó *pénzügyi-gazdasági válság a közigazgatásban is takarékosabb működést tett szükségessé*. Az erőforrásokat elsősorban az üzemeltetés biztosítására fordították, fejlesztési feladatokat kellett elhalasztani. Elmaradtak az amortizációs cserék, ma már a megnövelt életciklus mellett is esedékessé váló technológia- és eszközbeszerzésekről kell gondoskodni.

Az új informatikai technológiák bevezetése kapcsán – bármennyire hangsúlyosak is a felhasználói elvárások – mindig mérlegelni szükséges, hogy egy eszköz vagy alkalmazás bevezetése *milyen hozzáadott értéket teremt*, mennyiben segíti elő a közigazgatási szerv feladatellátását. Fontos, hogy a piacon megjelenő újdonságok közül a már *kiforrott megoldások kerüljenek alkalmazásra*, elkerülendő a túl korai vagy a már elkésett adaptációt. Tudni és a felhasználókban is tudatosítani kell, hogy *az újdonságok bevezetése az első időszakban többletterhet* (pluszköltséget, munkafolyamat-lassulást stb.) *is eredményezhet*.

Az új technológia bevezetésénél számos esetben felmerül a saját beszerzés/fejlesztés és üzemeltetés vagy szolgáltatótól történő vásárlás kérdése. A *szolgáltatás-kihelyezés* (outsourcing) dilemmája a belső erőforrások tehermentesítésével párhuzamosan a korszerű technológiák viszonylag egyszerű elérése és a külső szolgáltatótól való függőség kialakulása közötti választás, legyen szó akár teljes körű IT-kihelyezésről, akár részleges infrastruktúra- vagy alkalmazás-üzemeltetésről.

Sajátos területet jelent a *felhőalapú számítástechnika* (cloud computing) *terjedése*. Új, korszerű technológia, amely – szabályozottság híján – adatvédelmi és informatikai biztonsági problémákat vet fel (pl. adatfeldolgozó azonosíthatósága határokon átnyúló adatáramlás esetén).

A *nyílt forráskódú* (open source) *szoftverek közigazgatási alkalmazása* európai uniós elvárás is. [4] Ezen programok bevezetésekor tudatában kell lenni annak, hogy egy ingyenes vagy nagyon kedvező árú, a fejlesztést követően viszonylag rövid időn belül elérhetővé tett alkalmazás várhatóan nem fogja ugyanazt a szolgáltatást biztosítani, amit egy hosszú ideig fejlesztett, tesztelt, folyamatosan finomított, és ezt árában is tükröző, kereskedelmi forgalomban beszerezhető termék. A kérdés ez esetben az, hogy mennyire szofisztikált programra van szükség az adott feladat ellátásához.

A *mobileszközök alkalmazása* felgyorsítja és kényelmesebbé teheti a munkafolyamatokat, azonban a bevett módszerekkel szigorúan ellenőrzött, telepített informatikai munkakörnyezettel szemben nagyobb biztonsági kockázatot jelent. Az okostelefonokra, táblagépekre telepíthető kisalkalmazások köztudottan sérülékenyebbek, a jogosult felhasználó ellenőrzése alóli kikerülés veszélye is nagyobb.

A saját tulajdonú (mobil)eszközök munkában való felhasználása (*konzumerizáció*, „Hozd be a saját eszközödet!” irányzat térhódítása) esetén alapvető biztonsági követelmény az informatikai szakterület általi menedzselhetőség, valamint az elérhető adatok és alkalmazások körének egyértelmű meghatározása.

Amennyiben a mobileszközök használata – a szervezet vezetésének döntése alapján – túlterjed a három klasszikus funkcionális alkalmazás (levelezés, telefonkönyv és

határidőnapló) elérésének biztosításán, fejlesztési feladatot jelenthet a szervezet által használt alkalmazások mobilváltozatának elkészítése is.

Az előbbieken ismertetett, a felhasználók által egyértelműen érzékelhető modernizáción kívül az informatikai szakterület feladata az informatikai infrastruktúra teljességének folyamatos karbantartása, megújítása – ami a felhasználók szemében állandó és kielégíthetetlen erőforrás-igényként jelenik meg.

Az informatikai eszközrendszer konzisztenciájának, funkcionális és biztonsági megfelelőségének, rendelkezésre állásának biztosítása állandó elemző-értékelő illetve adaptációs tevékenységet igényel az informatikai szakterülettől. Elengedhetetlen a saját képességek naprakész ismerete és kihasználásuk folyamatos optimalizálása (eszköz- és technológia-nyilvántartás, erőforrás-gazdálkodás, állapotfelmérések, kockázatok elemzése és kezelése stb.), az alkalmazkodás a változó jogi (szabályozói) és szervezeti (szakmai és funkcionális) követelményekhez.

A korszerű, lehetőség szerint alacsony üzemeltetési költségű, szabványos és szabályozott informatikai környezet biztosítása nemcsak „zöldmezős” fejlesztéseket, hanem a meglévő eszközök, adatbázisok, alkalmazások stb. folyamatos konszolidálását is jelenti.

A fejlesztés, korszerűsítés során figyelembe veendő informatikai követelményeket a vonatkozó ajánlások, módszertanok, szabványok részletesen tartalmazzák, ezek ismertetése jelen tanulmánynak nem célja. A beruházások tervezése és megvalósítása során a rugalmas módosítás és a lehetőség szerint folyamatos és zavartalan munkavégzés biztosításának igénye elvi szinten az integráltság (integrálhatóság), paraméterezhetőség, modularitás, interoperabilitás, szabványosság [11] követelményeinek teljesítését követeli meg.

INFORMÁCIÓBIZTONSÁG

Az informatikai fejlesztések eredményeit a felhasználók akkor tudják használni (élvezni), ha a telepített eszközök, alkalmazások rendeltetésszerűen működnek, és akkor akarják használni (igénybe venni), ha tudják – meggyőződtek róla vagy garantálták számukra –, hogy azok használata számukra előnyt (pl. gyorsabb, egyszerűbb ügyintézés vagy munkavégzés) jelent, nem pedig hátrányt (pl. adataik illetéktelenek általi megismerését vagy felhasználását).

Ezeknek az elvárásoknak a teljesítéséhez az informatikai eszközöknek és megoldásoknak nemcsak funkcionális szempontból kell megfelelőnek lenniük (azaz teljesíteni a velük szemben támasztott szakmai követelményeket), hanem biztonsági szempontból is. Az informatikai szakterületnek garantálnia kell egyrészt az informatikai rendszerek, másrészt a bennük tárolt adatok bizalmasságát (illetéktelenek általi meg nem ismerhetőségét), sértetlenségét (védetségét az illetéktelen módosítástól, beavatkozástól) és rendelkezésre állását (jogosultak általi zavartalan elérését).

Az informatikai rendszereket és a bennük tárolt adatokat védeni kell fizikai behatás, informatikai esemény vagy személyes beavatkozás révén bekövetkező, véletlen kár vagy szándékos károkozás ellen.

Az informatikai rendszerek sérülékenységevel összefüggő, elméleti és gyakorlati problémák és a lehetséges védelmi megoldások száma folyamatosan nő, irodalma végtelen (sajtócikkek és tanulmányok, szabványok és ajánlások).

Technológiai oldalról elsősorban az internet- és mobilhasználat, a külső hálózati kapcsolatok, a nem kiforrott és emiatt védelmi képességekkel még nem megfelelően rendelkező technológiák és eszközök elterjedése, a heterogén, esetenként korszerűtlen infrastruktúra védelmének bonyolultsága jelent kihívásokat. Nem-technológiai oldalról a célzott támadások (sértett alkalmazottak, érdeklődő hackerek, kiberbűnözők) növekvő száma és a felhasználók biztonságtudatosságának hiánya az alapvető gond.

Az információbiztonság garantálása többszintű feladatrendszer meghatározását és teljesítését jelenti. Egyrészt maguknak a közigazgatási szerveknek kell saját informatikai infrastruktúrájuk és szolgáltatásai biztonsága érdekében a szükséges intézkedéseket meghatározni, végrehajtani és a végrehajtást ellenőrizni. Másrészt központi kormányzati feladat az információbiztonság szervezeti, szabályozási és technológiai követelmény- és feltételrendszerének kialakítása, amely alapján az egyes közigazgatási szervek saját és közös információbiztonsági tevékenységüket végezhetik. A legnehezebb feladat a két tervezési és végrehajtási szint összhangjának megteremtése – különös tekintettel arra, hogy az egyes szervek információbiztonsági tevékenysége több esetben már előrébb tart, mint az összkormányzati tervezés.

Az infokommunikációs technológiák védelme komoly erőforrásokat lekötő, soha véget nem érő, költséges tevékenység; az igazi gondot azonban a hiánya okozná.

ÖSSZEGZÉS

Az információtechnológiai eszközök elterjedése lehetőséget teremt társadalmi, szervezeti célok, közös és egyéni elvárások kielégítésére, és ezzel (vagy ezzel párhuzamosan) újabb és újabb igények forrásává válik.

A fejlődés eredményeként az infokommunikációs technológiák nemcsak kényelmet, jólétet biztosítanak, hanem komoly függőséget is eredményeznek, egyéni és közösségi szinten is.

Ebből következően mindannyiunk közös feladata és felelőssége a közigazgatási informatika ésszerű felhasználásának biztosítása, amihez mindenki helyzete, adottságai és képességei szerint járulhat hozzá: fejlődést biztosító, teljesíthető elvárások megfogalmazásával, a célok eléréséhez szükséges feltételek megteremtésével vagy éppen a rendelkezésre bocsátott eszközök korrekt, jogszerű alkalmazásával.

Felhasznált irodalom

- [1] A Bizottság közleménye a Tanácsnak, az európai Parlamentnek, az Európai gazdasági és Szociális Bizottságnak és a Régiók Bizottságának COM(2005) 229 végleges
- [2] Digitális Megújulás Cselekvési Terv 2010-2014., Nemzeti Fejlesztési Minisztérium, Budapest, 2010.
- [3] Magyar Zoltán Közigazgatás-fejlesztési Program (MP 11.0), Közigazgatási és Igazságügyi Minisztérium, Budapest, 2011. június 10.
- [4] eEurope 2002. An Information Society For All. Draft Action Plan prepared by the European Commission for the European Council in Feira. 19-20. June 2000. COM (2000) 330 final
- [5] eEurope 2002. Impact and Priorities. A communication to the Spring European Council in Stockholm, 23-24. March 2001. Communication from the Commission to the Council and the European Parliament. COM (2001) 140 final
- [6] The User Challenge, Benchmarking The Supply Of Online Public Services. 7th Measurement. September 2007. Capgemini.
http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf
- [7] Dr. habil. Tózsá István: Az elektronikus közigazgatás helyzete – Új Magyar Közigazgatás, 2012. május, 5. évfolyam 5. szám, 2-12. o.
- [8] eEurope 2005: Benchmarking indicators. Communication from the Commission to the Council and the European Parliament. COM (2003) 655 final

- [9] Information Society Benchmarking Report.
http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/051222%20Final%20Benchmarking%20Report.pdf. Letöltve: 2012. 07. 10.
- [10] Dr. Budai Balázs Benjámín PhD: A közigazgatás és az elektronikus közigazgatási fejlesztések hatékonyságának mérése napjainkban – Új Magyar Közigazgatás, 2012. május, 5. évfolyam 5. szám, 13-29. o.
- [11] Dr. Négyesi Imre: A információ szerepe a katonai – vezetői információs rendszerekben. Hadtudományi Szemle 2009. (II.) 1., 119-123. o.
<http://hadtudomanyiszemle.uni-nke.hu>. Letöltve: 2012. 07. 06.

Négyesi Imre

negyesi.imre@uni-nke.hu

DIE UNTERSTÜTZUNG DER SOLDATEN MIT ECHTZEITDATEN

Abstrakt

Eine der wichtigen Fragen unserer Sonnen, wie die Führer mit einem verschiedenen Niveau zu einer Entscheidung über eine Bestimmungsfrage wie schnell kommen können. Schnelle und gute Entscheidungsinformationen, die für die Bestimmung nur (Daten) eintreten, können wir mit seinem effizienten Gebrauch, um dafür zu bringen. Auf allen Gebieten des Lebens, aber dem Erwerb der Echtzeitinformationen und seiner Verarbeitung machen das Bilden der schnellen Entscheidungen möglich im Betriebsleben besonders. Diese Veröffentlichung untersuchte die Gelegenheiten dieser Echtzeitdatenverarbeitung, die Gelegenheit der militärischen Anwendung berücksichtigend.

Nowadays, it has a growing importance to make decision in good time at any level of leaders. Mainly in business word, but also in all fields of the life there could not be a fast and good decisions without aproprate information gathering and efficient realtime data processing. With consideration the chance of military usage this publication analyses the opportunities of this real time data processing.

Napjaink egyik fontos kérdése, hogy a különböző szintű vezetők milyen gyorsan tudnak döntést hozni egy-egy meghatározó kérdésben. Gyors és jó döntéseket csak a rendelkezésre álló információk (adatok) hatékony felhasználásával tudunk hozni. Az élet minden területén, de különösen az üzleti életben a gyors döntések meghozatalát a valós idejű információk megszerzése és feldolgozása teszi lehetővé. Ennek a valós idejű adatfeldolgozásnak a lehetőségeit vizsgálta ez a publikáció, figyelembe véve a katonai alkalmazás lehetőségét.

Schlüsselworte: Informatika, Információs társadalom, Információ, Adat ~ informatik, informationsgesellschaft, information, daten ~ informatics, information society, information, data

EINFÜHRUNG

Die korporativen Führer mit einem verschiedenen Niveau (hier die Kommandanten des militärischen Korps aufzählend), nur passende aktuelle Informationen (Daten) ihre Aufgaben können mit seiner Hilfe hingerichtet werden, um ihre Organisationen zu leiten. Bewiesene Tatsache, dass die Masse der Informationen dafür in der Größenordnung von den menschlichen Arbeitskräften und den Finanzmitteln erforderlich ist, das am effizientesten Zuweisen den Aufgaben gefunden zu werden. Die Gelegenheiten des Zu-Stande-Bringens der Leistungsfähigkeit, der Versicherung der ihm zugeteilten Daten sind in einem zunehmend breiteren Kreis verfügbar. Wir untersuchten die Verwirklichungsformen dieser Gelegenheiten in dieser Veröffentlichung mit der Präsentation von wirklichen, arbeitenden Systemen.

DIE ROLLE DER INFORMATIONEN IN DEN ARMEEN

Die amerikanische Armee das Zentrum der Forschung, Entwicklung und Technikkommunikationselektronik war der Gastgeber dieses Programms, für das es sein primäres Ziel in der Größenordnung von den Entwicklungspartnern war, um über die Pläne der Armee im Thema der Anwendung der rechenbetonten Wolke informiert zu werden. Es wurde auf diesem Programm definiert, dass es notwendig ist, die so genannte Funktionswolke für die amerikanische Armee zu schaffen.

Das wird die Wolke sein, die es, gemäß den Plänen das Armeedatensammeln und eine Intelligenz die Tätigkeiten des Agenten auf den Operationsgebieten unterstützen wird. Die fähigen Fachmänner der Armee baten darum als das im Interesse von ihm verschiedene Industriegesellschaften, die Universitäten und die anderen Regierungsorganisationen, wie in Anwendungen dem Thema zusammenhängend gereicht werden sollte. Die Offiziere der Armee brachten die Gelegenheit einer allgemeinen Infrastruktur herauf, die wird schafft, der die Lagerung der multinationalen Firmengeheimdienst-Daten und seine Behandlung bevorzugt, und es ein rechenbetontes Fachwerk für die Ausführung von Analysen zur Verfügung stellt.

Diese Einleitung vom Teil der amerikanischen Armee es beweist es eindeutig, dass die Offiziere die Gelegenheiten erkannten, die in der rechenbetonten Wolke wohnen. Die vorhandenen Mängel und ein ausdrücklicher, beträchtlicher werden zur gleichen Zeit gesehen Schritte möchten auf dem Gebiet der Anwendung der Wolkentechnologie gemacht werden, die in Armeen geschieht. [1]

EINE GELEGENHEIT AUF DIE REALISIERUNG

Es Unternehmen von SAP ein HANA¹ entwickelte Ziel-Ausrüstung, die auf einen Namen antwortet, der zwischen den Geschäftsnachrichtendienstanwendungen zusammen mit seinen Partnern beträchtlich sein kann. Das eine Datenanalytiker-Maschine, deren Prüfung es SAP es durchführte und seinen auf die Ergebnisse basierten Vertrieb anfang.

Auf HANA Sybase im Gedächtnis auf die Datenspeichertechnik, und einen Server-Hersteller wird auf der Hardware von Partnern gebaut. Es im Gedächtnis die Essenz eines Konzepts, dass die Daten nicht in einem klassischen Datenbankdressierer gefunden werden können, aber im Gedächtnis, wo es möglich ist, sie mit Größenordnungen schneller, aber dem Niveau der Parallelismus-Zunahmen zu erreichen. Es, im Gedächtnis so Technologie wie Schätzend, dass was die Verarbeitung der zahlreichen Menge von Echtzeitdaten macht, die im

¹ High-Performance Analytics Appliance

Gedächtnis des Servers möglich, damit von den Analysen und von Transaktionen geschehen, ein unmittelbares Ergebnis zur Verfügung stellt.

HANA Basis, organisierte eine Software, die sich an die Analysen anpasst, in gezogene Säulen gut Läden die Daten, meine ich, dass die Daten der Säulen eines Tisches einander folgen. Mathematische oder algorithmic Operationen mit leichteren homogenen Daten so, wie was das Summieren, die Mittelwertbildung, in eine Reihe-Richtung, Filtern zu machen. Die Softwaregeräte sind an einem Verdiener-Analytiker und Datenmodell eine Verfügung zum Kämmen der Daten. Die festen Betriebsleiter können unmittelbare Simulationen Quasi-basiert auf den HANA blitzschnellen rechenbetonten Motor neben den Abfragen durchführen, die auf den echten Daten und Analysen beruhen. [2]

Sybase präsentierte die neueste Version der Datenbank eines IQ der 15.3-t IQ, Mission dessen, die sogar mehr Tausend gleichzeitige Benutzer, die Skala üben, jeden den Zugang für die angesammelten Informationen für ihn zur Verfügung stellen lassen, die die besten Entscheidungen erlaubt werden lassen, immer in einer Organisation gemacht zu werden. Die Anwendung zielt auf die großen Firmendatenlager, aber als es auf Gebieten so bereits nützlich sein kann. Die wichtigste Neuheit der Datenbankvollendungslagerung mit einer Säulenbasis im PlexQ zukünftigen Bratrost, durch das Datenlager Sie Geschäftsintelligenz im Falle Aufgaben mehr Tausend parallele Benutzer und eine Abfrage sind, kann geübt werden erklettern das System.

Die Gesellschaften können die Gelegenheiten ausnutzen, die in der Geschäftsanalytik gemäß Sybase dann völlig wohnen, wenn alles, was das Arbeiten an den Echtzeitdaten bekommt und es ist möglich, die Analyse den Teil der Basisprozesse zu machen. Der Kreis von denjenigen, die Analyse-Abnahmen natürlich im Laufe der militärischen Anwendung durchführen können. Die Befehlen-Substanz mit einem verschiedenen Niveau kann es jedoch im Wesentlichen Gelegenheiten verwerten. Sybase entwickelte seine neue Datenbank, die auf solche Art und Weise das in die Rücksicht nimmt, dass er es möglich woran der Dienst von mehr parallelen Benutzern, das Laufen von vielen Abfragen machen sollte.

Der IQ 15.3 PlexQ auf man wird auf paralleler Architektur gebaut, weil er schaffte, die Skala-Bars damit gemäß Sybase stark zu überwinden. PlexQ fragen Plattform verteilt, aber auf einer überraschenden Weise nicht geteilt nichts, aber geteilt nähert sich alles, gemäß Sybase im Falle des Datenlagers und ein Geschäftsanalytik-Gebrauch der Vorteil davon, das das parallele Laufen der ohne es möglichen Abfragen macht, dass der Bratrost eines seiner Elemente oder der Server überbürden würde. Wenn Sybase IQ Optimizer, den Optimierung einer Abfrage schafft, in dieser Richtung im Laufe der Analyse zu bekommen, dass die Abfrage einen Verbindungspunkt überbürden würde, sie prüft, um parallel zu sein, und auf mehr Kommunikationsendpunkte einzeln, um sich zu befassen. Die Gesellschaften können eine Art Selbstbedienungsdatenstapelplätze für ihre verschiedenen Abteilungen aufbauen, damit hingebungsvollen Mitteln erlaubt werden sollte, von den organisatorischen Einheiten zur Verfügung zu stehen. [3]

MILITÄRISCHE ANWENDUNGEN

Aus der Zahl von den militärischen Anwendungen lassen uns ein untersuchen, welcher sich mit dem Schutz des Personals mit einem der wichtigsten Gebiete im Laufe der Ausführung der militärischen Aufgaben befasst. In der amerikanischen Armee za leitet USAMRMC² die Forschungen, die sich mit den Geräten befassen, die die Theater des Krieges fortgesetzt werden können. Die commandership Kollege-Gelehrten bildeten sich hoch, Programm-Betriebsleiter, die Experten aus, die das Herstellen eines Kontakts und Unterstützen des

² USAMRMC=United States Army Medical Research and Materiel Command

Personals bevorzugen. Seine Gesamtheit wurden ungefähr 6000 militärische, bürgerlich, und der Konstrukteur-Personal zur Organisation in der Größenordnung vom commandership bestellt, und ordnen Sie unter, um die Arbeit von Einheiten zu bevorzugen.

Mit dem USAMRMC Management Tempus Pro [4] entwickelte ein fortgeschrittenes Kompaktsystem, mit dessen Hilfe die Mannschaften, die auf dem Theater des Krieges kämpfen, erträglich sind. Die entwickelte Einheit stellt die Daten den Ärzten auf dem Schlachtfeld auf die Promotion der geschehenden verwundeten Versorgung zur Verfügung. Die TEMPUS-Pro drei vereinigen Gerät in einem einzelmem manuellem Modul, das die unmittelbare Kommunikation möglich mit anderen Einheiten, das einleitende Scheckkrankenhaus schlecht lebenswichtiger und der telemetric macht, macht man den Zugang möglich zu Daten, und macht es möglichen Instruktionsaufwand von den erfahrenen hygienischen Dienstleistern für die weniger erfahrenen kriegesischen Ärzte. Die Einheit eine Fähigkeit, die im Laufe der Versorgung außergewöhnlich nützlich sein kann, steht vom Echtzeitaudio und einem Video zur Verfügung. Wichtiger Gesichtspunkt, der es ist, dass der TEMPUS-Pro es geduldige Daten (aufrechterhalten kann, der die Lebensstatistik) fast durch den Gesundheitsfürsorge-Transport ist, der bis zu Punkten völlig bis zum Krankenhaus-Zimmer geschieht. Auf einer Weise solcher werden die hygienischen Daten des Patienten mit ihm verlassen, geht irgendwo - dass das sehr wichtig ist.

Der TEMPUS-Pro das Schlüsselement eines Systems die neue Technologie. Es wurde so geplant, dass leicht, beweglich und ihn haltbar sein lassen. Der TEMPUS-Pro sein Ziel, dass der taktische Kommunikationsradioman die Unterstützung von Netzen, die Internetprotokoll-Basisübertragung ausnutzt, die den qualifizierten und nicht die qualifizierten Systeme im Stande sein lassen, Zeichen digital seine Richtung zu senden. Dieser Gesichtspunkt die direkte Digitalübertragung, was seine Bestimmung des Vorteils der TEMPUS-Pro-nak seine Vorgänger ist. Mit dieser neuen Einheit können wir Personalangaben von einem des Apparats auf den anderen vom Land vortragen, die die kranken hygienischen Daten des Personals lassen, der ihn transportiert, treten für das Handeln zur Zeit des Hubschrauberkrankenhaus-Transports ein. Es ist möglich, die Lebensdokumente des Patienten auf den Systemen ohne das verschiedene Kabel auszutauschen, und es ist möglich, in eine unveränderliche medizinische Aufzeichnung schließlich zu legen. Das sichere Digitalsystem versichert es, dass die Daten damit nicht verloren werden dürfen und Fehler gehasst werden kann.

Kapitalziel, wie ich lieben würde, die Krankenhaus-Daten noch vor dem Patienten zu wissen, kommt hierher. Die Lagerung der geduldigen Daten wichtig, aber nicht absolut notwendig, dass die Ärzte die Daten auf ihren eigenen Computern die Daten versorgen. Darauf kann die Wolkentechnologie, mit der noch Bilder und lebende Videos der Verletzungen gesichert werden, die für Ärzte notwendig sind, eine Lösung sein. Der TEMPUS-Pro die Ärzte können die ernsten Verletzungen schnell mit seiner Hilfe, wie das die Echtzeitbilder, und die Chirurgen schätzen, die mit der lebenden Person und der Echtzeitgebrauch der telemetric Daten erfahren sind, kann ihren Kollegen mit dem Aufwand von entfernten Instruktionen helfen.

Der Schutz der menschlichen Arbeitskräfte kann ein anderes Gerät haben, wenn valós-idejű wir auf den Seiten der Militäreinsätze mit Informationen handeln. Der Dienst der ausgewerteten Feindnachrichten muss die Wolkentechnologie zwischen den ersten gemäß dem verwenden. High Performance Technologies Inc (HPTi) [5] Unternehmen, das dieser Weg konzentriert, die mit der Unterstützung der amerikanischen Bundesregierung planen und einen wie das die private Wolke begreifen, die die neuesten Nachrichtendienstinformationen zu amerikanischen Mannschaften vermittelt, die in einer Echtzeit in Afghanistan nahe aufstellen werden. Die Entwicklung des Programms begann, als die amerikanische Armee so entschied, dass eine private Wolke genug für die Voraussetzungen basiert machen kann, auf dem die Analysen in einem vollen Maß, Daten processings stb rechtskräftig sind.

Die Armee verwendet Anwendungen der offenen Quelle eher allgemein, die Elastizität und die Geschwindigkeit so versichernd, und, die die Abhängigkeit von den großen Herstellern vermieden werden lassen. HPTi erbot sich, eine einheitliche Lösung vorzubereiten, die die Straße für die Algorithmen behandelt, und alle Daten versichert. In der Anwendungsoffenen Quelle ist Hadoop Software, die eine Software wie das ist, verwendetes Bibliotheksfachwerk-System, was die verteilte Verarbeitung möglich im Falle der großen Dateien macht. Zur Realisierung MapReduce-t waren sie nützlich, dass ein so programmierendes Modell, das große Dateien für seine Verarbeitung verwenden. HPTi stellt es der Armee im Sinne des Vertrags auf sich-wolke selbst seine Unterstützung zur Verfügung.

ZUSAMMENFASSUNG, SCHLUSSFOLGERUNGEN

Bewiesene Tatsache, dass die korporativen Führer mit einem verschiedenen Niveau (hier die Kommandanten des militärischen Korps aufzählend), nur passende aktuelle Informationen (Daten) ihre Aufgaben mit seiner Hilfe hingerichtet werden können, um ihre Organisationen zu leiten. Wurde bewiesen es ist, dass die Masse der Informationen dafür erforderlich ist, dass die menschlichen Arbeitskräfte und die Finanzmittel das am effizientesten Zuweisen den Aufgaben gefunden werden lassen. Die Gelegenheiten des Zu-Stande-Bringens der Leistungsfähigkeit, der Versicherung der ihm zugeteilten Daten sind in einem zunehmend breiteren Kreis verfügbar. Die Überprüfung dieser Gelegenheiten breitete sich auf dem Gebiet der militärischen Aufgaben aus. Wir probten es mit der Beschreibung von wirklichen Systemen eine Hypotenuse zu weiter dem Formen eines Bildes. Ein völlig Hypotenuse schrieb es dem Schaffen eines Bildes hier natürlich die Reihe von Tatsachen wenig. Aber weil eine auf diese zwei Artikel bereits basierte Endschlussfolgerung gestärkt werden kann, dass die Zukunft die Wolkentechnologie, es BI und Große Daten in der Fahrrolle auf mehreren der Gebiete eines Lebens so in den Armeen sein wird.

Literatur

- [1] www.cerdec.army.mil, 2012.11.22.
- [2] <http://www.sap.com/solutions/technology/in-memory-computing-platform/hana/overview/index.epx>, 2012.11.22.
- [3] http://www.sybase.com/files/Technical_Documents/SybaseIQ15_Technical_Overview_v15_SCRIPTED.pdf, 2012.11.22.
- [4] <http://www.rdtltd.com/military-sector/>, 2012.11.22.
- [5] <http://www.drc.com/solutions/it/>, 2012.11.26.

Puskás Béla

THE RISKS OF NETWORKS' COMPLEXITY

Abstract

"We live in an accelerated world" sounds one of the most common truisms of our age. Comparing to the previous decades this feeling is mainly caused by the dynamic flow of information, fast traffic and transportation means and the globalization, which have been resulted by the booming technical development. Nowadays a journey from Hungary to the United States does not resemble the risky and long-run adventure as it was at the wake of the last century. We also can keep connection with our relatives living on another continent easily. Consequently the people have got closer to each other but at the same time they loosened their connections as well. We live in the virtual space and rarely contact our friends physically. This gap between the individuals and their physical reality is getting so wide, that they don't realize the devastation of environment or the natural disasters.

Az előző évtizedekhez képest a dinamikus információáramlás, a transzport eszközök fejlődése, a globalizáció eredményeként a műszaki fejlődés felgyorsult. Napjainkban már nem számít kockázatos és hosszú kalandnak átutazni az Egyesült Államokba, mint ahogy ez a múlt század elején volt. Mi is, mint humán szféra könnyen tarthatunk kapcsolatot rokonainkkal, ismerőseinkkel, akik akár egy másik kontinensen is élhetnek. Következésképpen az emberek az IT hálózatok segítségével közelebb kerültek egymáshoz, de ugyanakkor lazított is a kapcsolatuk. Virtuális térben élünk, amit az is bizonyít, hogy csak ritkán találkozunk személyesen ismerőseinkkel, barátainkkal. Ez a különbség az egyének és a fizikai valóság egyre növekvő eltávolodását hozhatja, miközben környezetünkben jelentős változások, természeti katasztrófák játszódhatnak le.

Keywords: *network attack, future IT warfare, structure of networks ~ hálózati támadások, a jövő informatikai hadviselése hálózatok szerkezete*

“We have built our future upon a capability that we have not learned how to protect! “1

HOW HAS THE REVOLUTIONARY ELECTRONIC DEVELOPMENT CHANGED OUR COMMON LIFE?

On the 4th of September in 1837 the inventor, Samuel Morze introduced his electromagnetic telegraph. In order to use it two things were essential. One of them was the Morze alphabet, while the other was the telegraph network itself. At that time the bit rate was “only” at around 5 bit/sec.

In 1876 Alexander Graham Bell had the telephone patented. He also had to establish and operate a network thus he founded the Bell Telephone Company in 1877. Presently it is the well-known American Telephone and Telegraph Co. (AT&T).

Between 1895 and 1901², based on James Clerk Maxwell’s theory regarding the radio waves, Nikola Tesla, Guglielmo Marconi and Alexander Popov “independently” from each other invented the radiotelegraph.

In 1957 the Soviet Union launched “Sputnik”, the first satellite of mankind. As a response, the President of the USA and the Department of Defense founded ARPA³ in 1958. In 1969 an experimental network was established and some others joined in later. Five years earlier Paul Baran had already pointed out: in order to create a minimum risk level communication channel, a partitioned network had to be established instead of the decentralized ones. According to his theory the separated packets used on the Internet had to be sent through individual nodes toward their destinations. Nevertheless his idea was rejected.

IN THE SEVENTIES THE INTERNET STARTED ITS OWN LIFE.

More and more institutions joined the network, but not on the way as Baran thought. Instead of the partitioned network a scale-free model was evolved. Due to its extension and rapid development the network couldn’t be controlled exclusively. The dominant original goal of an operational network, which is protected against attacks, was not taken into account any more. On the contrary THE INTERNET, which is highly resistant against random errors, was born. It is quite similar to the other networks of our life, such as social networks, networks of the human bodies (nerve system, connections between cells etc.) but it resembles the networks of spreading epidemics and many other else.

Do we really know what has come to life by the Internet?

The main problem is that not only the simple common user doesn’t understand it, but the IT professionals are not able to clear up the matter as well. We don’t have proper knowledge about the network structure and we can’t obtain it by our way of thinking. We have to apply the theory of networks. For example documents are being prepared faster on Internet than the search engines can locate and index them. Nowadays they don’t even try it and only the 30-40 % of the whole document is mapped even by the most effective search engines. In case of cell phones, especially the smart phones, the situation is quite the same. Their development is so fast that their effect to the hardwares, softwares and the other system can’t be measured. Recently 10 % of the Internet data flow is going through mobile networks.

Then how the USA, NATO or Hungary can prepare themselves for the future IT warfare and how can we protect our critical IT systems against the hackers and terrorists?

¹ George Tenet Former CIA director

² In 1901 Marconi introduced his invention for what the Nobel Prize in Physics was awarded to him in 1909-ben. Tesla had already introduced his patent in 1896, while Popov had done so in 1895.

³ Advanced Research Projects Agency

Today the real task is not to understand the occurrences going on the Internet or the Internet itself as an entity. Today when it became a part of our life we have to insert it into our complex world.

The terrorist organizations and other criminal groups sometimes hide secret messages in the chaos of the Internet. They can communicate on the network or exploiting its and the users' weaknesses in order to gain money.

Against whom do we have to protect our systems?

In most of the cases the attackers are completely unknown. They hide their sources and even their homeland can't be identified properly. Usually not the owners of the concept execute the attack, but they get "innocent" prying men to do the messy job. They provide only the method and pattern of the attack. The communication channels and the logistics background are also given by someone else. They rarely have particular political or economical interests, the attack is simply considered as a challenge or a funny joke.

I think that in the future it will be very important to get familiar with the nodes of networks and their connections. We have to realize that the network is not just one-dimensional. The connections and effects of seemingly different social and electronic networks have to be researched. Not only the threatened system has to be examined but all the other linked networks as well. Besides the structures of networks we have to know the structures and the very details of the points (e.g. cells). From this point of view the node cannot be described as a mathematical concept because if today something is considered to be indivisible, tomorrow that can be a set. According to Albert-László Barabási the XXI century is going to be the age of complexity.

What has to be studied?

The matter is not so simple. Moreover it becomes more complex if we consider another dimension as well: the movements of nodes. The nodes can change continuously and dynamically. If the nodes are the critical infrastructures we have to count on their permanent movements. What has not been a node before that can become so and vice versa. This fact regards the Internet nodes especially.

In order to determine the items of networks we have to deal with complexity as well. Traditional telecommunication, television, informatics etc. networks and their nodes can be mentioned only within the category of electronic networks. All the network items such as routers, switches, modems, hubs, repeaters, transfer medias, servers, data storages, firewalls, adapters and their features influencing the functions of the "system" have to be studied. We also can test the linking "devices", for example printers, monitor-keyboard switches, different input devices, adapter interfaces (smart phones, TV, PDA, GPS etc.), medical equipment, control systems of critical infrastructures such as traffic lamps or airplanes. The device-free surveys concerning the physical and logical network topology, softwares, hardware and software settings, regulators, physical protection, the human factor, environmental effects are also very interesting of course. The parameters of these factors are quite sophisticated as well but their mutual effects and the quality of their linkage create a complex and immense system.

The Internet has become a complex network. Since it is continuously expanding it can be called scale-free network as well. While studying the network, Barabási and his team noted two facts: the expansion and the popularity.

The scale-free systems are highly resistant to random errors but a targeted attack against the centres can disintegrate them easily. Many vertices, which have only a few edges, can be eliminated but it doesn't have significant effect on the whole network. The destruction of the 80% of Internet nodes leaves the remaining 20% operational nodes working as an intact network.

There can be another practical question in connection with the networks: Do the malfunctions of devices, eruptions of social conflicts, devastations of biological or chemical disasters happen accidentally?

The segments of the network can be paralysed by a series of chance events or a well-organized, targeted attack.

It is easy to see, that as the drawing of the lottery, the malfunction of a random device is also not able to interfere the operation of the whole scale-free network. What is the probability that I can select that particular node, which has many links or especially important for the connection? In case of the Internet and other similar networks the degree exponent is less than three. Because of this fact there is no threshold, which prevents the network disintegration, when the nodes are removed continuously.

However a targeted attack is different. If the nodes with many links are destroyed firstly and it is carried on with the other nodes with less and less links, the network falls apart at a certain threshold. Usually this threshold can be reached quite soon and the attacker doesn't have to destroy too many nodes with many links. Although our system resistant to errors, but the removal of the nodes with many links (e.g. central routers) impose an almost unbearable burden onto the other important nodes and transfer medias. The other items can work for a while, but later packets are going to be lost and congestions are going to emerge, which is very similar to a DoS attack.

I am of the opinion that the nodes providing important links can cause similar problems. Although redundant connections are always installed within the systems these connections have smaller capacity.

Perhaps if the Internet would have not started to live its own "life" and in 1964 Baran would have succeeded in fulfilling his basic theory concerning the primacy of distributed models, we should not fear of the targeted attacks as much. But there is no point dealing with "what if..." questions because these processes are irreversible. We could consider the particular "systems" of evolution having similar networks instead. We may owe our life to it.

Consequently the items of the system, their mutual effects and links and the map of the network have to be known properly. I haven't mentioned the types of graphs, which make the structure of networks more difficult. For instance whether a graph is directed or not does make difference and the network structure modification effect of the relocation of the edge between two vertices can not be neglected either. The complex system can not be protected without this knowledge.

Based on data bases, data storages, documents and images some modern softwares are able to graphically depict the complicated networks and map the complex structures. By the assistance of these softwares false information and connections can be identified, forecasts and algorithms can be prepared. The different aspects (timeline, too many or few but highlighted connections) could reveal hidden, important information.

One of the most important part of the cognition is the obtainment and sorting of information. The concerning data can be obtained from unclassified and classified sources, for instance from the data bases of telecommunication ventures, social sites, Internet providers, manufacturers and many other sources.

If we know our system and lead a safety-conscious life we can avoid such unpleasant events⁴, which occurred to the director of MI6, Sir John Sawer. It is obvious, that the problem of mapping the complexity is not only a matter of IT professionals. We have to realize that everything is linked with each other and the physical and logistical networks have mutual

⁴ In 2009 Sir John Sawers's wife uploaded some family images onto a social site. By these pictures hostile organizations or individuals could obtain sensitive information, which could endanger Sawers and indirectly the MI6.

effects on each other as well. We can't be sure that the erased digital information really vanishes.

References

- [1] Barabási, A.-L. (2003). *Behálózva*. Budapest: Magyar könyvklub.
- [2] University of Debrecen. (without date). *Az Internet története.*, source: http://www.inf.unideb.hu/~bodai/internet/internet_tortenete.html;
Download date: 30/09/2012
- [3] Defense Technical Information Center. (2002). *Information Technology Industry Study Final Paper.*,
source: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA425460>;
Download date: 30/09/2012
- [4] ELTE. (2006). *Az elektronikus sajtó története.*,
source: <http://mmi.elte.hu>;
http://mmi.elte.hu/szabadbolcseszeti/index.php?option=com_tanelem&id_tanelem=548&tip=0; Download date: 27/09/2012
- [5] National Geographic Magyarország. (without date). *Samuel Morse, a távíró feltalálója.*,
source: http://www.ng.hu/Civilizacio/2005/04/Samuel_Morse_a_taviro_feltalaloja;
Download date: 28/09/2012
- [6] Péter, B. (19/09/2012). A globális IT-rendszerek erdejében. *Computerworld*, page: 4.

VII. Évfolyam 4. szám - 2012. december

Szentgáli Gergely
gergely.szerntgali@gmail.com

AZ EURÓPAI UNIÓ KIBERBIZTONSÁGI TÖREKVÉSEI ÉS SZERVEZETEI I.

Absztrakt

Napjainkra a kiberbiztonság kérdése az első számú biztonságpolitikai kihívások között szerepel. Az információs társadalmak biztonságát meghatározó informatikai környezet és a hozzá kapcsolódó kihívások minden államot arra sarkallnak, hogy építsék ki a megfelelő védelmi szerveket és alkossák meg a szükséges jogszabályokat. Ezt a felelősséget az Európai Unió is felismerte és megkezdte a felkészülést ezen új típusú biztonsági kihívás kezelésére. Jelen cikkben az Unió kiberbiztonsággal kapcsolatos jogi lépéseit és az Európai Digitális Menetrendet fogom elemezni. Az írás második részében (amely a következő Hadmérnökben fog megjelenni) az EU kiberbiztonságáért felelős kiemelt szervezeteit fogom bemutatni.

In the recent years, the conception of cyber security developed into a critical security policy matter. Security challenges associated with the informatical environment, which are determining the security of informational societies, are reinforcing states to create their own enforcement agencies and to materialise the requisite legal measures. The European Union has acknowledged this sort of responsibility, and it began to prepare the management of new forms of security challenges. In my recent writing I will analyze the EU's legal steps toward cyber security, and the Digital Agenda for Europe. In the second part of the paper (which will be released in the next issue) I am presenting the EU's further bodies and actions.

Kulcsszavak: kiberbiztonság, Digitális Menetrend, kritikus információs infrastruktúrák, Európai Unió ~ cyber security, Digital Agenda of Europe, critical information infrastructure

BEVEZETÉS

Szinte már közhelynek számít, hogy az információs társadalmak függnek a modern kori információs eszközöktől és infrastruktúráktól. Az sem újdonság, hogy ezeknek a rendszereknek a védelme elengedhetetlen kormányzati feladat. Mindazonáltal a probléma még mindig aktuális, hiszen naponta jelennek meg új fenyegetések mind a fizikai, mind az információs dimenzióban, amelyek ezeket az infrastruktúrákat fenyegetik.

Számos állam elkezdte kidolgozni a saját stratégiáit a kiberbiztonság kérdésével kapcsolatban. Ez a folyamat az Európai Unió tagállamainál is elindult, jelenleg az alábbi államok rendelkeznek önálló stratégiával: Észtország (2008), Finnország (2008), Szlovákia (2008), Csehország (2011), Franciaország (2011), Németország (2011), Litvánia (2011), Luxembourg (2011), Hollandia (2011) és az Egyesült Királyság (2011).¹

A döntéshozók azt is felismerték, hogy ezeknek a rendszereknek a védelme nem feltétlen kezelhető kizárólagosan az államhatárokon belül, hiszen számos infrastruktúra határokon átnyúló hálózatot alkot. Pontosan ezért szükséges, hogy a különböző nemzetközi szervezetek, az őket alkotó tagállamok biztonságának erősítése érdekében megerősítsék a saját rendszereiket, és koordinációs segítséget nyújtva elősegítsék az állami képességek kialakítását is. Ahogyan a NATO-ban, az Európai Unióban is realizálódott ez a probléma, amelyeket számtalan válasz követett.

JOGSZABÁLYOK, PROGRAMOK ÉS LÉPÉSEK EGY BIZTONSÁGOSABB UNIÓÉRT

A kibervédelem kérdésének vizsgálatakor az első számú technikai kihívás a kritikus infrastruktúrák és a hozzájuk kapcsolódó kritikus információs infrastruktúrák védelme. Az Európai Unió hangsúlyos módon 2004 óta foglalkozik a kritikus infrastruktúrák védelmével.

2004. október 20-án fogadta el a Bizottság a „*Kritikus infrastruktúrák védelme a terrorizmus elleni küzdelemben*” című közleményt,² illetve még ez év decemberében a Tanács jóváhagyta a Kritikus Infrastruktúrák Figyelmeztető Információs Hálózat³ felállítását.⁴

2005. november 17-én fogadták el az uniós döntéshozók a „*Zöld Könyv a kritikus infrastruktúra védelem európai programjáról*”⁵ című dokumentumot. Ehhez a programhoz igazodik a magyarországi szabályozás, a 2080/2008. (VI. 30.) kormányhatározat, azaz a *Kritikus Infrastruktúra Védelem Nemzeti Programjáról*⁶ elnevezésű jogszabály. Azonban ez az uniós dokumentum azonban nem csak ezért fontos, hanem abból az okból is, hogy meghatározásra kerülnek benne a kritikus információs infrastruktúrák is, amelyek a magyar jogszabályokban még nem lelhetőek fel.

¹National Cyber Security Strategies.

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport 5-6 o. Letöltés ideje: 2012. október 1. Néhány európai állam részletesebb elemzését lásd KOVÁCS László: *Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I.* In: Hadmérnök. VII. évfolyam. 2012/2. 304-311. o.

²Critical Infrastructure Protection in the Fight Against Terrorism. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF> Letöltés ideje: 2012. október 10.

³Critical Infrastructure Warning Information Network – CIWIN

⁴RÁCZ László István: *Kritikus infrastruktúra védelem hazai és nemzetközi szabályozási rendszere.* In: Hadmérnök. VII. évfolyam. 2012/2. 168. o.

⁵*Zöld Könyv a kritikus infrastruktúra védelem európai programjáról.*

<http://www.ivb.org.hu/documents/INNOVACIOSklub/200812ho/ZoldKonyv.pdf>;

Letöltés ideje: 2012. október 10.

⁶2080/2008. (VI.30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. In: Határozatok Tára. 2008/31. 217-231. o.

A kritikus infrastruktúrák részét képezik a kritikus információs infrastruktúrák. Muha Lajos, a Nemzeti Közszerálati Egyetem tanára, doktori disszertációjában az alábbi definíciót fogalmazta a kritikus információs infrastruktúrákkal kapcsolatban:

„Azon az infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikus infrastruktúra elemek, továbbá a kritikus infrastruktúra elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása, vagy megsemmisülése a kritikus infrastruktúrák működésképtelenségét jelentősen csökkentené.”⁷

Ezeknek a létesítményeknek a megléte és védelme – tekintve, hogy a kritikus infrastruktúrák részét képezik – elengedhetetlen feladat a mindennapi élet feltételeinek biztosításához, kiesésük rendkívüli károkat okozna a gazdaságban.⁸ Ennek elkerülése érdekében készült el a 2009. március 30-án elfogadott *„Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása”* című dokumentum.⁹ A bizottsági közlemény alaposan végigveszi a kritikus informatikai infrastruktúrákkal kapcsolatos veszélyeket, illetve mindezekhez kapcsolódóan egy cselekvési tervet is felvázol.

A dokumentum kiválóan rámutat, hogy komoly elmaradások vannak ez ügyben a tagállami szinteken, érezhető eltérések vannak mind a felkészültség, mind a szaktudás tekintetében. Ahogyan említettem, a magyar országgyűlés csupán a kritikus infrastruktúrák védelmével kapcsolatos kormányhatározatot fogadott eddig el, azonban a kritikus információs infrastruktúrák védelmével kapcsolatosan semmilyen jogszabály nem rendelkezik. Ez is egy olyan hiányosság, amit hazánkban a jövőben minél hamarabb pótolnia kell.¹⁰

A közlemény szintén fontosfelismerése, hogy a kritikus információs infrastruktúrák döntő többségben a magánszféra tulajdonában vannak, így a kormányzat és a magánszféra közötti kommunikáció – csak úgy, mint a kiberbiztonság számos aspektusában – létfontosságú.

Az európai irányelvhez kapcsolódó cselekvési terv eredményeiről számol be a 2011. március 31-én elfogadott, *„Eredmények és következő lépések: a globális kiberbiztonság felé”* című bizottsági közlemény.¹¹ Az alapvetően pozitív eredményeket tartalmazó dokumentum további számos ajánlást tesz a jövőbeni lépésekkel kapcsolatosan, kiemelve a CERT hálózat további kiépítésének szükségességét, illetve egy kiberbiztonsági vészhelyzeti terv kidolgozását 2012-ig.

A kéretlen levelek, azaz a spamek, illetve a különböző kémprogramok és kártékony szoftverek elterjedésére is reagált már az európai közösség. A spamek problematikája már

⁷MUHA Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. PhD értekezés. ZMNE, Budapest, 2007. 40. o.

⁸A részletes felsorolásért lásd HAIG Zsolt: Az információs társadalom információbiztonsága. In: Bolyai Szemle. XVII. évfolyam. 2008/4. 175. o.

⁹Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása.

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:HU:PDF>

Letöltés ideje: 2012. október 6.

¹⁰Muha Lajos már megfogalmazott egy ezzel kapcsolatos javaslatot, lásd MUHA Lajos: Infokommunikációs Biztonsági Stratégia. In: Hadmérnök. IV. évfolyam. 2009/1. 214-224. o. Fontos azonban megjegyezni, hogy az Európai Digitális Menetrendben meghatározott lépéseket kivitelező Digitális Megújulás Cselekvési Terv 2010-2014 című kormánydokumentum már tartalmazza a keretek kialakítását elősegítő lépéseket. Mindezekről lásd a következő fejezetet.

¹¹Eredmények és következő lépések: a globális kiberbiztonság felé

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:HU:PDF>

Letöltés ideje: 2012. október 6.

2002-ben¹² és 2004-ben¹³ is előkerült, azonban más káros tevékenységekkel kapcsolatosan 2006. november 15-én adott ki közleményt a Bizottság.¹⁴ A közlemény nagy hangsúlyt fektet a tudatosságnövelő lépések, illetve a nemzetközi együttműködés fontosságára. Biztosítja a tagállamokat, hogy továbbra is támogatja azokat a kutatási és fejlesztési folyamatokat, amelyek segíthetnek a kártékony kibertéri jelenlét ellen. Mindezekhez kapcsolódóan megjegyzi, hogy az eddigi tapasztalatok azt mutatják, hogy szerény befektetéssel jelentős eredmény érhető el. Véleményem szerint ez a gondolat a teljes kibervédelmi törekvésekre kiterjeszthető, hiszen a kiberképességek kialakítása mind tagállami, mind nemzetközi szervezeti szinten viszonylag alacsony költségvetésű lépés, viszont a hatékonysága és a haszna mégis rendkívül nagy.

Az Európai Unió komolyan foglalkozik a fiatalok védelmével is. Ebbe a törekvésbe illeszkedik bele a *Biztonságos internet program 2009-2013* is.¹⁵ Az Európai Parlament és a Tanács 1351/2008/EK határozata¹⁶ alapján elindított program célja, hogy azonosítsa a gyermekekre leselkedő internetes veszélyeket, illetve harcoljon ellenük. Továbbá lehetőséget biztosít a jogellenes internetes tartalmak bejelentésére.¹⁷

Végül érdemes megemlíteni a formálódó európai kiberbiztonsági stratégiát. Az előzetes iránymutatást¹⁸ olvasva elmondhatjuk, hogy az Európai Internetes Biztonsági Stratégia nevet viselő projekt nem egy tipikus kiberbiztonsági stratégia lesz, azonban számos hasonlóságot felfedezhetünk a klasszikus stratégiákat vizsgálva. Mindenesetre fontos iránymutató lesz az Unió, mint nemzetközi szervezet számára, hogy miképpen kezelje a kibertéri fenyegetéseket.

Ezen törekvések közé illeszkedik a véleményem szerinti legfontosabb dokumentum is: az Európai Digitális Menetrend.

A DIGITÁLIS MENETREND ÉS A KIBERTÁMADÁSOK

A gazdasági válság nem csak az Unió gazdasági gyengeségeire, hanem más területekkel kapcsolatos problémákra is rávilágított. Ezekre a problémákra való reagálásként került elfogadásra 2010. március 3-án az *Európa 2020 – Az intelligens, fenntartható és inkluzív fejlődés stratégiája*¹⁹ című dokumentumot. A stratégia alapvető célja az új európai gazdasági modell kialakítása és az ehhez kapcsolódó területek fejlesztése. Ennek értelmében öt kiemelt célkitűzést határoztak meg a jogalkotók:

- *foglalkoztatás*: a 20–64 évesek foglalkoztatási rátájának 75%-ra növelése;

¹²2002. július 12-én fogadták el az Európai Parlament és a Tanács 2002/58/EK irányelvét, melynek 13. cikke tiltja a spamküldést. Lásd *Az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:hu:HTML> Letöltés ideje: 2012. október 6.

¹³Ekkor fogadták el a 2002-es irányelvvel kapcsolatos kiegészítő lépéseket. Lásd *Measures to counter unsolicited commercial communications or 'spam'*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0028:FIN:EN:PDF> Letöltés ideje: 2012. október 6.

¹⁴A kéretlen levelek, a kémprogramok és a rosszindulatú szoftverek elleni küzdelemről. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:HU:PDF> Letöltés ideje: 2012. október 6.

¹⁵A programnak már volt egy megelőző szakasza is (*Biztonságos internet plusz*), ami 2005-től 2008-ig tartott.

¹⁶*Az Internetet és egyéb kommunikációs technológiákat használó gyermekek védelmére irányuló többéves közösségi program létrehozásáról*.

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:348:0118:0127:HU:PDF> Letöltés ideje: 2012. október 6.

¹⁷Magyarországon is üzemel már ilyen weboldal, lásd *Biztonságos Internet*. <http://www.biztonsagosinternet.hu/> Letöltés ideje: 2012. október 6.

¹⁸*ROADMAP: Proposal on a European Strategy for Internet Security* http://ec.europa.eu/governance/impact/planned_ia/docs/2012_info_003_european_internet_security_strategy_en.pdf Letöltés ideje: 2012. október 6.

¹⁹*Európa 2020 – Az intelligens, fenntartható és inkluzív fejlődés stratégiája*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:HU:PDF> Letöltés ideje: 2012. október 2.

- *K+F*: a bruttó hazai termék (GDP) 3%-ának kutatásra és fejlesztésre való fordítása;
- *éghajlatváltozás/energia*: a szén-dioxid-kibocsátás 20%-kal (amennyiben lehetséges, 30%-kal) való csökkentése; a megújuló energiaforrások arányának és az energiahatékonyságnak 20–20%-kal való növelése;
- *oktatás*: az iskolából kimaradók arányának 10% alá csökkentése és a felsőoktatási oklevéllel rendelkezők arányának 40%-ra való növelése;
- *szegénység/társadalmi kirekesztés*: a szegénység által veszélyeztetett lakosok számának 20 millióval való csökkentése.²⁰

A stratégia hét kiemelt kezdeményezést is előreirányoz, amelynek egyik eleme a 2010. augusztus 26-án elfogadott *Európai digitális menetrend*.²¹ A menetrend fő célja egy egységes digitális piac létrehozása egy biztonságos és világos jogi keretekkel rendelkező környezetben. E cél elérése érdekében számos lépés megtételére van szükség mind uniós, mind tagállami szinten:

- 2013-ig a minimális szélessáv mindenki számára elérhető legyen;
- 2015-ig szűnjön meg a különbség a belföldi és a roaming tarifák között;
- 2015-ig a rendszeres internethasználat mutatója érje el a 75 %-ot (a jelenlegi 60 %-ról), a hátrányos helyzetűek esetében pedig a 60 %-ot;
- 2015-ig a felére kell csökkenteni azoknak a számát, akik még sosem használtak internetet.²²

Témánk szempontjából azonban a legfontosabb az internet biztonságával kapcsolatos felismerések és a hozzájuk tartozó reakciók. Ahogyan a vonatkozó részben is olvashatjuk: „Az európaiak nem fognak olyan technológiát felkarolni, amelyben nem bíznak – a digitális kor nem lehet egyenlősem a Nagy Testvérrel, sem az »internetes vadnyugattal«.”²³

A dokumentum vonatkozó része számos problémás pontra rámutat. A spam üzenetek növekvő mértéke, a banki szolgáltatások, illetve a személyes adatok egyre kifinomultabb módszerekkel való támadása ugyanúgy megjelenik, mint az államok ellen folytatott kiberhadviselés veszélye is.

A Menetrend kiválóan vázolja azokat a területeket, amelyek terén lépéseket kell tenni: gyermekpornográfia elleni harc; kritikus infrastruktúrák informatikai védelme; saját hálózatok védelme; tagállami operatív csoportok kialakításának támogatása. Magyarán a kibervédelem teljes spektrumát igyekeznek megvalósítani, ami azért is fontos, mert kezdetben az Európai Unió csupán a saját közös rendszereinek védelmét tartotta fontosnak, most azonban már egyértelművé vált, hogy a tagállamok felzárkóztatása ezen a téren elengedhetetlenül fontos a sikeres védelem kialakításához.

Minden tagállam kötelessége, hogy kidolgozza a saját cselekvési tervét, amely a Digitális Menetrendben megfogalmazottak elérését segíti. Magyarország tekintetében a 2010. december 20-án elfogadott *Digitális Megújulás Cselekvési Terv 2010-2014*²⁴ az iránymutató

²⁰Európa 2020: az Európai Unió növekedési stratégiája.

http://europa.eu/legislation_summaries/employment_and_social_policy/eu2020/em0028_hu.htm

Letöltés ideje: 2012. október 2.

²¹Az európai digitális menetrend.(a továbbiakban: MENETREND 2010.) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:HU:PDF> Letöltés ideje: 2012. október 2.

²²Miről szól a Digitális

Agenda?http://www.euvonal.hu/index.php?op=kerdesvalasz_reszletes&kerdes_valasz_id=1634

Letöltés ideje: 2012. október 2.

²³MENETREND 2010. 18. o.

²⁴Digitális Megújulás Cselekvési Terv 2010-2014.

http://www.kormany.hu/download/6/4f/00000/Digitalis_Megujulas_Cselekvesi_Terv.pdf

Letöltés ideje: 2012. október 1.

dokumentum. A program célja, hogy a magyarországi információs társadalmat mind technikai, mind gazdasági szempontból fejlessze.

Véleményem szerint a cselekvési tervnek két nagyon fontos pontja van. Az első a kritikus információs infrastruktúráknak védelmével kapcsolatosan meghatározott lépések, illetve a kapcsolódó akciók, amelyek a következők:

- A kritikus információs infrastruktúra védelem vezetésének és a védelmi stratégia kidolgozásának kormányzati kézbe vétele, a vonatkozó EU irányelvnek megfelelően;
- Az állam vezetésével, kidolgozott módszertan alapján a nemzeti kritikus infrastruktúra, valamint az európai kritikus infrastruktúra elemek kijelölése, illetve a kijelölések folyamatos felülvizsgálata;
- A kritikus információs infrastruktúra védelmi szabályok és feladatok állami kijelölése
- Összkormányzati szinten a kritikus információs infrastruktúrák védelme területén a tudatosság növelés és az oktatás, továbbképzés.²⁵

A második fontos pont a közigazgatási információs rendszerek biztonságának növelése. Mindehhez a dokumentum az alábbi akciókat kapcsolja:

- Adatszabványok, információbiztonsági követelmények kompatibilitásának megteremtése az egészségügyi informatikában;
- IT-biztonsági jogszabályok átdolgozása;
- Magas színvonalú informatikai biztonsági megoldások bevezetésének támogatása a kormányzat részére egységes szabályozás alapján.²⁶

Ami a Digitális Menetrend további értékét adja az az, hogy a problémák megfogalmazásán kívül – ahogyan azt olvashattuk – válaszokat is kínál. Konkrét lépésekkel és új szervek kialakításával reagál a felmerülő fenyegetésekre, továbbá világossá teszi, hogy mely feladatok tartoznak az Unió hatáskörébe és melyek a tagállamokéba, illetve melyek azok, amelyeket közösen kell kivitelezni. Mindezekről lásd az 1. ábrát.

	Uniós szintű feladat	Tagállami feladat
Hálózat- és információbiztonsági politika végrehajtása	✓	
Kiberbűnözés elleni központ létrehozása	✓	
Globális kockázatok kezelése	✓	
Kiberbűnözést figyelő országos platformok kialakítása		✓
Jogellenes internetes tartalmak bejelentésére alkalmas pontok kialakítása		✓
Hálózatvédelmi gyakorlatok kivitelezése	✓	✓
Kritikus információs infrastruktúrák védelme	✓	✓
Számítástechnikai Sürgősségi Reagáló Egység kialakítása	✓	✓

1. ábra. Az Európai Digitális Menetrend által meghatározott fő feladatok megoszlása
(Forrás: Menetrend 2010. 20-21. o.)

Ezek azok a körülmények, amiért a Digitális Menetrendet az egyik legfontosabb lépésnek tartom az EU kibervédelmének kialakításánál. Láthatóan jól átgondolt, egymásra épülő tervezet, amiből számos pontja megvalósult már. A végrehajtott lépések hatékonysága

²⁵i. m. 91. o.

²⁶i. m. 68. o.

természetesen csak rövid idővel később nyerhet igazolást, azonban tagadhatatlan tényré vált, hogy az Unió komolyan veszi ezen új típusú biztonsági kihívást.

ÖSSZEGZÉS

A fentiekben bemutatam az Európai Unió legfontosabb dokumentumait és jogi lépéseit a kiberbiztonság erősítése érdekében. Jól látható, hogy a jogi keretek kialakítása nagy erővel folyik, napjainkra már az unió szintjén a tárgyalta kérdés majdnem összes szegmense rendelkezik önálló iránymutatással. Magyarán az érzékeny területek azonosítása megtörtént. Innentől kezdve a tagállamok felelőssége, hogy a legalacsonyabb szintektől kezdve felkészüljenek a különböző incidensek kezelésére.

Érdekes trend figyelhető meg az uniós kommunikáció tekintetében, miszerint a kezdetben alapvetően ajánlás jellegűek voltak az informatikai és információbiztonság területéhez kapcsolódó intézkedések, később azonban számos lépés kötelező jellegűvé vált. Mindez természetesen üdvözlendő változás, hiszen a tagállamok közötti különbség – akár képességek, akár stratégiákat tekintetében – a közös biztonságot gyengítik.

A tanulmányom következő részében az uniós kibervédelmi szervezeteket és a lehetséges együttműködő partnereket fogom bemutatni.

Felhasznált irodalom

- [1] 2080/2008. (VI.30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. In: Határozatok Tára. 2008/31. 217-231. o. ISSN 2063-0395
- [2] A Bizottság megerősítene az informatikai támadásokkal szembeni védelmet Európában. <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1239&format=HTML&aged=1&language=HU&guiLanguage=en>; Letöltés ideje: 2012. október 4.
- [3] Az európai digitális menetrend. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:HU:PDF> Letöltés ideje: 2012. október 2.
- [4] Critical Infrastructure Protection in the Fight Against Terrorism. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF> Letöltés ideje: 2012. október 10.
- [5] Digitális Megújulás Cselekvési Terv 2010-2014. http://www.kormany.hu/download/6/4f/00000/Digitalis_Megujulas_Cselekvesi_Terv.pdf; Letöltés ideje: 2012. október 1.
- [6] Európa 2020 – Az intelligens, fenntartható és inkluzív fejlődés stratégiája. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:HU:PDF>; Letöltés ideje: 2012. október 2.
- [7] Európa 2020: az Európai Unió növekedési stratégiája. http://europa.eu/legislation_summaries/employment_and_social_policy/eu2020/em0028_hu.htm; Letöltés ideje: 2012. október 2.
- [8] HAIG Zsolt: Az információs társadalom információbiztonsága. In: Bolyai Szemle. XVII. évfolyam. 2008/4. 167-180. ISSN 1416-1443
- [9] KOVÁCS László: Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I. In: Hadmérnök. VII. évfolyam. 2012/2. 302-311. o. ISSN 1788-1919

- [10] *Miről szól a Digitális Agenda?*
http://www.euvonal.hu/index.php?op=kerdesvalasz_reszletes&kerdes_valasz_id=1634;
Letöltés ideje: 2012. október 2.
- [11] *National Cyber Security Strategies.*
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport;
Letöltés ideje: 2012. október 1.
- [12] *Zöld Könyv a kritikus infrastruktúra védelem európai programjáról.*
<http://www.ivb.org.hu/documents/INNOVACIOSklub/200812ho/ZoldKonyv.pdf>;
Letöltés ideje: 2012. október 10.

Hollós Tamás
hollostamas@gmail.com

AZ IDEÁLIS VEZETŐ KOMMUNIKÁCIÓJA (VAGY A VEZETŐ IDEÁLIS KOMMUNIKÁCIÓJA?)

Absztrakt

Az írás címe több kérdést is felvet és nyomban rávilágít arra a dilemmára, hogy lehet-e valaki jó (ideális) vezető jó (ideális) kommunikáció nélkül. A közlemény azt vizsgálja, hogy milyen kommunikációs ügyesség kell ahhoz, hogy egy rendészeti területen dolgozó vezető ideálisnak legyen mondható. A hazai rendészeti közeg több szempontból is igen speciális; a leglényegesebb talán az igen erős hierarchizáltság, amely még a legrátermettebb, legképzettebb vezetőt is meglehetősen nagy próbatételnek veti alá. Azonban ez a hierarchizáltság sem gátolhatja meg a vezetői hatékonyság kommunikációs eszközökkel történő növelését.

The title of the article raises several questions and immediately casts a light on the dilemma whether one can be a good (ideal) leader without good (ideal) communication. The paper examines the communication skills a leader working in the area of law enforcement needs so that he/ she can be considered ideal. The law enforcement environment in Hungary is very special from several aspects; the most important factor is probably the rigid hierarchy, which severely tries even the fittest leaders with the highest qualifications. However, even such a hierarchic system must not prevent us from increasing leadership efficiency with communication tools.

Kulcsszavak: kommunikáció, „felhatalmazás”, kulturális szignál, relevancia ~ communication, empowerment, cultural signal, relevance

BEVEZETÉS

Létezik-e ideális vezető, mondható-e bárkire az, hogy ő ideális? Elvégre véleményem szerint ideálisnak azt a személyt lehetne nevezni, akit mindenki elfogad, akit mindenki tisztel, aki soha nem hibázik stb. De ilyen személy – talán kijelenthető – nincs. Hiszen ha a vezetőt a felettesei tehetségesnek, rátermettnek tartják, akkor a beosztottai szerint túl szigorú, és ez természetesen fordítva is igaz lehet: előfordulhat, hogy a főnököt nagyon szeretik a beosztottai, mert kicsit engedékenyebb, de az nem biztos, hogy ezt „felül” is jó szemmel nézik.

És egyáltalán: létezik-e olyan, hogy ideális kommunikáció? Mit tekinthetünk annak? És ha van olyan, hogy ideális kommunikáció, azzal egy vezetőnek feltétlenül rendelkeznie kell? Vagy megfordítva a kérdést: lehet valaki jó (ideális) vezető jó (ideális) kommunikáció nélkül is? Vagy ha már valaki ideális vezető, akkor az rögtön magába foglalja azt is, hogy ideális kommunikációval is rendelkezik?

A JÓ VEZETŐ JELLEMZŐI

A kérdés tehát először is az, hogy milyen is egy jó vezető, egy „jó főnök”? Természetesen, mint szinte minden ehhez hasonló kérdés a világon, ez is relatív, így az én véleményem is csak egy a sok közül – és nem biztos, hogy az a helyes.

Ha az ideális vezető tulajdonságait keressük, rögtön felmerül a „helyszín”, ugyanis egyáltalán nem mindegy, hogy az ember milyen környezetben, milyen közösségben vezető. Én személy szerint pedagógiai főiskolát is végeztem, majd annak elvégzése után tanítottam is egy tanévet egy Szekszárd közeli kisebb településen, annak általános iskolájában, illetve jelenleg is oktatok a Nemzeti Közszerződési Egyetem Rendészettudományi Karán. Véleményem szerint a tanár, a tanító is egyfajta vezető, elvégre a tanórán, a tanteremben (vagy akár azon kívül) legalább 45 percen át ő a főnök. Ugyanakkor a fő feladatai – mint például oktatás, önálló ismeretszerzésre nevelés, személyiségfejlesztés stb. – teljesen eltérőek egy rendőri vezetőétől. Nem is beszélve arról, hogy egy pedagógus munkájának része a fegyelmezés (sokszor rengeteg energiát és időt felemészítve), míg egy rendőri vezetőnek – optimális esetben – ezzel nem kell foglalkoznia. Hogy miért? Véleményem szerint azért, mert egy felnőtt ember tudja, miért van az adott munkahelyen, tudja, mik a feladatai és megcsinálja, amit a főnöke mond neki - ez azonban a gyerekekre nem feltétlenül érvényes. Látható tehát, hogy egyes vezetői magatartások között is van különbség, az említett példánál maradva a pedagógusé szinte teljesen különbözik egy rendőri vezetőétől, így ebbe nem is szeretnék részletesebben belemenni.

A vezetés mára egyértelműen tudománnyá vált: tanulható és elvárható jellemzőkkel. Ma a vezetők nagy része nem a szerencse kegyéből, születésénél fogva, de nem is áldozatos, lemondásokkal teli küzdelem után válik vezetővé, mint a múlt és a közelmúlt vezetőinek nagyobb része. Mára a vezetés szakma, illetve önálló tudományos terület lett, saját oktatási intézményekkel, szakfolyóiratokkal. Ez egyben azt is jelenti, hogy mindenki, aki érez magában hajlandóságot erre, könnyen válhat vezetővé. Természetesen számít a tehetség és az elhivatottság, de a lényeg – mint minden szakmánál – a szükséges végzettségek megszerzése és a következetes munka. Ma már a vezetők többsége is egykor beosztott, alkalmazott volt, aki a megfelelő végzettség megszerzése után hivatásszerűen kerül(t) pozíciójába.

Ezzel a folyamattal párhuzamosan megváltoztak a vezetőkkel szemben támasztott elvárások is. A társadalmi élet átforgatólódásával a korábban természetesnek tekinthető vezetői tulajdonságok „elavulttá” váltak. A hagyományos vezetői szerep számos olyan elemet foglalt magában, amelyek ma már nem feltétlenül érvényesek: a nagy hatalmi távolsággal jellemezhető, egyértelmű hierarchiába rendezhető, számos irracionális elemmel terhelt

klasszikus vezető-vezetett szereposztás lényegében működésképtelenné vált. A ma dolgozója már alapvetően nem fizikai teljesítményével, hanem szellemi munkával és igen gyakran kreativitásával dolgozik. Ez a munka jellemzően sokkal hasznosabb – azonban csak akkor, ha a dolgozó meglehetősen nagy szabadságot élvez munkája során. Természetesen a rendőrség alapvetően hierarchikus szervezet, amelyben mindenképpen erősebben jelennek meg olyan elemek, amelyek a gazdasági életben visszaszorulóban vannak, ezzel együtt a szolgáltató közigazgatás és a hatékonyság igénye itt is parancsolóan teszi szükségessé egyes, a nyereségérdekelt szervezeteknél megszokott változások átvételét. Megállapítható, hogy a legsikeresebb szervezetek szakítani igyekeznek a hagyományos felépítéssel, igyekeznek lelapítani a szervezeti piramist, száműzni a bürokráciát, fokozni a kommunikációt, átjárhatóvá tenni a hierarchiát.

Ebben a koncepcióban a jó főnök egészen más tulajdonságokkal jellemezhető. Az „empowerment”¹ kiváló lehetőség a munkatelésítmény fokozására, azonban csak akkor működőképes, ha a főnök tiszteletben tudja tartani ezt a függetlenséget. Ennek megfelelően a főnök nem különül el, irodája mindig nyitva áll munkatársai előtt (de legalábbis nem zárja kulcsra), sokkal inkább mentorként dolgozik. Szakmai tudása nem feltétlenül magasabb kollégáinál – általában nem a konkrét, hanem saját szakterületén, azaz a vezetésben számít professzionistának. Ez azt is jelenti, hogy elsősorban a „főnöki” munkák terén dolgozik és keveset foglalkozik a konkrét munkafeladatokkal, nem igyekszik azokat munkatársai helyett megoldani. Ez a kép tehát egy pozitív, könnyen elérhető, elsősorban segítő, összehangoló feladatokat ellátó vezető képét vetíti elénk. Nem egy nagy vállalkozás, multinacionális cég közvetít ilyen képet saját vezetőiről és a rendőrségi reformokban is határozottan jelenik meg ennek a vezetői típusnak a képe. Ugyanakkor hiba lenne nem észrevenni, hogy ez csak az érem egyik oldala.

A rendőri vezetőnek ugyanis elkerülhetetlenül találkoznia kell olyan kérdésekkel is, amelyeket csak hatalmi szóval tud megoldani. A feladatok nőnek, a terhelés egyre nagyobb, a jogszabályi környezet bonyolultabb és fokozottabb a társadalmi ellenőrzés is. A főnököknek épp ezért szinte folyamatosan monitorozni kell a fennhatóságuk alá tartozó területet és mindent megtenni azért, hogy a hatékonyság ne csökkenjen, viszont el lehessen kerülni azokat a helyzeteket, amelyek során a dolgozói önkény, a nem szakszerű fellépés támadási felületet ad a testület ellen. Ez pedig azt is jelenti, hogy minden munkatársat maximális teljesítményre kell rávenniük és csak igen szűk lehetőségeik vannak az elnézés, a támogatás terén. Más szavakkal: a főnökök helyzete ma sokkal közelebb áll a beosztottakéhoz annyiban, hogy nem megfelelő hozzáállás esetén őket vonják felelősségre. Ennek megfelelően a vezetőknek saját érdekükben is feltétlen feladatuk a nem megfelelő munkát végző munkatársak kiszűrése és eltávolítása, így ezen a téren a hierarchia, a formális szabályok alkalmazása nélkülözhetetlen. Ezek alapján fel lehet vázolni az „ideális” főnök személyiségjegyeit: az ilyen vezető képes a fenti szituációkban tökéletesen működni. Könnyű belátni, hogy ez lehetetlen: számos tekintetben ellentmondásos követelményeknek kellene megfelelnie.

Véleményem szerint egy vezetőnek soha nem szabad arra törekednie, hogy a beosztottai szeressék őt, hiszen sokszor előfordulhat, hogy népszerűtlen döntést kell hoznia; a lényeg, hogy tegye, amit tennie kell, még akkor is, ha ez nem mindenkinek tetszik. Egy jó főnök legyen kezdeményező, céltudatos, korrekt, kreatív, vállalja a felelősséget a tetteiért, álljon ki a beosztottjai mellett, folyamatosan képezze magát, mutasson példát az élet minden területén... és a sor még hosszan folytatható lenne. Látható tehát, hogy egy vezetőnek nagyon sok dologra kell odafigyelnie, és egy dolgot ezek alapján teljes biztonsággal kijelenthetünk: nagyon nehéz

¹ felhatalmazás; az emberek (állampolgárok) tudással és képességekkel való felruházása azért, hogy érdekeiket hatékonyabban képviselhessék és önállóan tudjanak életkörülményeik jobbításáért akciókat indukálni. <http://szocialis-gondozo.lapunk.hu/?modul=oldal&tartalom=688641> Letöltve: 2012. 10. 20.

jó vezetőnek lenni. És tartom, hogy tökéletes vezető márpedig nincs. De a cél az, hogy törekedjen a tökéletességre. És soha ne gondolja magáról, hogy el is érte azt...

A KOMMUNIKÁCIÓ

Tovább boncolgatva a bevezetőben említett dilemmát, meg kell vizsgálni, hogy mi is az ideális kommunikáció? Egyáltalán mi az, hogy kommunikáció?

A kommunikáció kifejezés a latin *communis* szóból ered, ami azt jelenti, hogy „közös”. A legegyszerűbb meghatározás szerint kommunikáció minden, amelyben információ továbbítása történik. Az emberek vonatkozásában ezt ki kell terjeszteni, ugyanis amikor kommunikálunk, akkor közösséget akarunk létesíteni valakivel, azaz meg akarunk osztani egy vagy több személlyel egy információt, gondolatot, érzést vagy állásfoglalást. Úgy is ki lehetne fejezni, hogy a kommunikáció segítségével az emberek megfelelő szimbólumok, szimbólum-rendszerek használata mellett információk, érzések, gondolatok közös értelmezésére törekcszenek. A kommunikáció lényege tehát az, hogy egy bizonyos hírrel kapcsolatban egy hullámhosszra hangolja a leadót és a felvevőt. Forgács József meghatározása szerint: „A kommunikáció dinamikus, kölcsönös folyamat, amely a korábban szerzett ismeretekre és a partnerek közös történetére épít.” [1]

A kommunikációt a vezető oldaláról megközelítve megállapítható, hogy az kiemelkedő szerepet játszik a munkája során, ideje nagy részét ugyanis – mint minden ember – kommunikációval tölti, ezért különösen fontos a megfelelő fellépés a különböző csoportokkal szemben. A vezető a kommunikáción keresztül irányítja a beosztottak munkáját, meghatározza a célokat, közli a beosztottakkal, hogy pontosan mit is vár el tőlük és ehhez milyen eszközök állnak rendelkezésre. Fontos tudatában lenni annak, hogy az irányítása alatt álló csapat vagy csoport garantálja a vezető sikerét is. Ezért (is) nagyon fontos a hiteles vezetői kommunikáció, hogy az elképzelésekkel az egész csapat azonosulni tudjon, hiszen így már nem a vezető, hanem az egész csoport akarataról beszélhetünk. Ha ezt sikerül megvalósítani egy vezetőnek, az már fél siker az eredményes együttműködés felé.

A vezető kommunikációja azonban nem csak a tervek, elképzelések minél pontosabb közléséről szól. A verbális és a nem verbális kommunikáció együttes eszközrendszere meghatározó lehet a beosztottak motivációjában, a kialakult konfliktusok kezelésében, a vezető és a csoport önérvényesítésének folyamatában (és a sor még hosszan folytatható lenne)... A jó vezetői kommunikáció tehát nem csupán a beszéd egy bizonyos alkalmazását jelenti, hanem egy önálló vezetői magatartást, egyfajta kultúrát, melynek elsődleges megnyilvánulásai a kommunikáció eszközein keresztül találkoznak a külvilággal. Buda Béla meghatározása szerint:

„A verbális csatorna az ember legspecifikusabb kommunikációs módja, önmagában csaknem teljesen alkalmas arra, hogy mindenféle emberi kommunikációt hordozzon, mindenféle információ továbbításához fel lehessen használni. Valamennyi kommunikációs csatorna közül a legbonyolultabb kóddal rendelkezik. Írott formájában a legtipikusabb eszköze a közvetett kommunikációnak.”[2]

A verbális csatornán keresztül egyezményes jeleket továbbítunk, melyek akár önmagukban is alkalmasak bármilyen információ továbbadására. Különösen jó nyelvi kifejezőkészsége esetén olyan érzelmeket, indulatokat is közölhetünk, amelyek természetes közlési csatornáik nem szóbeliek.

Ha a vezető kommunikációját vesszük, megállapíthatjuk, hogy ő nem csak saját magát képviseli, amikor megnyilvánul, hanem azt a szerv(ezet)et is, amelyikhez ő tartozik, azaz a hallgatóság nem csak róla alkot képet. Ebből is látható, hogy ez nagy felelősséggel jár, ezért minden megszólalásnak jelentősége van/lehet. Egy vezetőnek tudnia kell nyilvánosan beszélni, amelyhez jó szónoki képességek – szókincs, fogalmazáskészség, rögtönzés stb. –

kellenek. Fontos, hogy hogyan tud hatni a közönségre, hogy milyen az előadásmódjának a hatóereje, és ahhoz, hogy ez megfelelő legyen, nem csak alapos felkészültségre, hanem kellő mélységű önismeretre is szükség van. Fontos ugyanis, hogy az ember tisztában legyen a hiányosságaival, ellenkező esetben könnyen előfordulhat, hogy egy egyszerű eset is zavart kelt. A jobb megértés érdekében mondanivalója megformálása során igazodnia kell a közönség nyelvhasználatához, így nem mindegy, hogy kikhez is fog beszélni. Éppen ezért az előadást mindig meg kell előznie a felkészülésnek, hogy tudja, mit várnak el tőle, hogy ő milyen hatásra törekszik, hogy milyen a hallgatóság összetétele és annak a hallgatóságnak milyen előzetes ismeretei vannak az adott témáról. Utóbbi azért kiemelkedően fontos, mert ezen múlik, hogy mennyire használhatja a szaknyelvet, a különböző szakkifejezéseket. Ennek előzetes elmulasztása esetén előfordulhat, hogy a vevőközönség nem érti meg a hallottakat, ami egyik félnek sem megfelelő. Ugyanakkor a megfelelő szóhasználat sem garantálja, hogy a hallgatóság meg is jegyzi az előadó által közölteket, ezért az emlékezetbe véséshez ismétlésre van szükség. Amennyiben az előadónak van elegendő ideje a beszédre, akkor háromszor nyílik megfelelő alkalom arra, hogy ugyanazt elismételje: először az elején, amikor vázaltszerűen elmondja, hogy miről is fog beszélni, másodszor, amikor kifejti az adott témát, és harmadszor, amikor a végén lehetősége nyílik arra, hogy összefoglalja mindazt, ami elhangzott. Ez nemcsak azért jó, mert jobban rögzül a hallgatóságnál, hanem kiváló figyelemfenntartó hatása is van. Ehhez persze tökéletesen tisztában kell lenni az elmondani kívánt szöveggel, hogy tudja, melyek mondandójának leglényegesebb elemei.

Ha egy vezető kommunikációjáról beszélünk, nemcsak arról van szó, hogy neki kell valamilyen módon megnyilvánulnia, hanem arról is, hogy neki kell meghallgatnia másokat. Ezért fontos, hogy rendelkezzen a beszédértés magas fokú képességével. Ez nem feltétlen azt jelenti, hogy minden egyes szót értsen, amit neki mondanak, hanem sokkal inkább azt, hogy megértse a hozzá intézett beszéd lényegét, a mondanivaló esetleges mögöttes tartalmát. De ugyanilyen fontos az is, hogy azt is megértse, miért mondják neki azt, amit épp mondanak, hogy mit szeretnének vele elérni. Ehhez két alapvető kommunikációs képességet mindenképpen el kell sajátítania, az egyik az aktív meghallgatás technikája, a másik pedig az empátia keltése. Németh Erzsébet szerint a sikeres kommunikáció egyik további feltétele, hogy az ember legyen képes asszertív, vagyis egyenlő partnerként, udvarias és elegáns, de egyértelmű magabiztossággal viselkedni:

„Az asszertivitás azt jelenti, hogy magunk döntjük el, reagálunk-e valamire vagy sem, elmondjuk-e a véleményünket vagy sem. Azt jelenti, hogy szorongás nélkül kiállunk saját jogainkért anélkül, hogy közben mások jogait megsértenénk, vagy másokban szorongást keltenénk.”[3]

Egy vezetővel szemben igen fontos – talán az egyik legfontosabb – követelmény a határozottság, a magabiztosság, hiszen elég belegondolni abba, hogy milyen képet is fest magáról az, aki bizonytalan, aki már az első keresztkérdésnél sem tudja, fiú-e vagy lány. Márpedig nem szabad elfelejteni, hogy egy vezető nem csak saját magát, hanem egy adott szervezetet is képvisel, így – mivel az ember gyakran hajlamos az általánosításra – sokszor az ő tulajdonságait az egész szervezettel azonosítják, ami igen nagy felelősséget rejt magában. Ezért (is) szükséges, hogy véleményét, elképzelését minden körülmények között elő tudja adni és meg is tudja védeni azt, hogy fellépése határozott legyen. Molnár Katalin szerint:

„Az a szakmai vezető, akinek megfelelő képzettsége és részben a képzés során, részben a gyakorlatban szerzett és megerősített tudása van, magabiztosabban közlekedik a munkája során előálló helyzetekben. S ha mindehhez még magas szellemi és érzelmi intelligencia, valamint vezetői képesség is társul, szinte nincs olyan ismeretlen, váratlan szituáció, amiben ne állná meg a helyét, amelyre ne találná meg a megoldást. A határozottságnak és magabiztosságnak szükséges alapja ugyanakkor a magasan fejlett önismeret és az ehhez nélkülözhetetlen önkritika is.”[4]

A stílusrétegeket vizsgálva megállapítható, hogy egy rendészeti vezető életében, mindennapi munkájában a hivatalos stílus van jelen a legerőteljesebben. Ennek a műfajnak a nyelvezete igen nehézkes, így nagyon fontos, hogy az azokat olvasó, illetve azokat feldolgozó személy jó szövegértési képességgel rendelkezzen, főleg azért, mert ezeket a szövegeket sokszor nem elég pusztán megérteni, hanem gyakran reagálni is kell rájuk. Ebből pedig egyenesen következik, hogy a vezetőnek jó fogalmazókészséggel is rendelkeznie kell. Egy rendészeti vezetőnek azonban nemcsak a hivatalos, hanem egyéb stílusrétegekben is járatosnak kell lennie, ugyanis munkája többször állhat elő olyan szituáció, amikor – akár írásban, akár szóban – más stílusban kell megnyilvánulnia. Jó példa erre, amikor – bármilyen oknál fogva – valamely médiumban kell megnyilvánulnia, ebben az esetben a publicisztikai stílust kell alkalmaznia, de ugyanígy előfordulhat, hogy a társalgási vagy a tudományos stílus elemeit kell felhasználnia a kommunikáció során. Látható tehát, hogy a vezető kommunikációja igen szerteágazó lehet, nem elég egy-egy stílusréteg ismereteiben való „jártasság”.

Egyes esetekben az is előfordulhat, hogy a nem verbális kommunikáció teljességgel a beszéd helyére lép (pl. a süketnémák jelnyelve), ezért akár valamennyi, beszéddel kifejezhető tartalom közlésére alkalmas lehet. A kommunikációs folyamat során az ember – akár tudatosan, akár tudattalanul – hatást gyakorol a másik ember gondolkodására, és e hatás közvetítéséhez különböző eszközöket használ fel. Ezek során jeleket, szimbólumokat alkalmaz, amelyek a gondolatokat mint tartalmakat hordozzák. A kommunikáció azonban korántsem mindig tudatosan zajlik, hiszen – akár akarjuk, akár nem – folyamatosan küldünk jeleket a többi (a kommunikációban részt vevő) személy felé. A verbális kommunikáció önmagában lehetne félreértések forrása is, hiszen egy-egy szó vagy kifejezés nem biztos, hogy mindenki számára ugyanolyan jelentéssel bír, ezért kell mindig kiemelt figyelmet fordítani a nem verbális jelekre, hiszen ezek a szóban elmondott információk kiegészítésére, ellenőrzésére vagy éppen hangsúlyozására szolgál(hat)nak. Arc kifejezéseink, gesztusaink, hangképzésünk, mozdulataink, tekintetünk, testtartásunk, térközsabályozásunk, azaz a nem verbális jelzéseink a szavakon túli, illetve azokkal párhuzamosan haladó egyéb kifejező megnyilvánulásokat közvetítik, és ezek bizony legalább annyit árulnak el rólunk, mint az, amit mondunk vagy az, ahogyan kinézünk.

Megállapítható tehát, hogy a nem verbális kommunikációt gyakran kevésbé tudatosan értelmezzük, mint magát a nyelvet. Ebből következik, hogy ezek a nem verbális jelzések gyakran többet árulnak el a beszélőről – feltárva elrejtteni kívánt érzéseit, érzelmeit –, mint amennyit ő maga ki szeretne nyilvánítani. Ez akár arról is tájékoztathat bennünket, hogy az adott személy mikor mond igazat és mikor hazudik. A nyelvi és a nem verbális üzenetek abban különböznek tehát egymástól, hogy utóbbiakat általában gyorsabban küldjük és fogadjuk, kevesebb tudatos kontroll irányul rájuk (kevésbé követjük őket figyelemmel), valamint hatásosabban kommunikálnak különböző érzelmeiket, mint a nyelv. A nyelvnek és a kommunikációs rendszereknek különböző jellegzetességeik vannak, ezek pedig meghatározzák a társas interakcióban való ideális szerepüket. A legtöbb érintkezésben a verbális és a nem verbális üzeneteket együtt használjuk.

A beszéd során egy jellegzetes, nem verbális kommunikációs csatorna, az úgynevezett vokális kommunikáció is szükségszerűen működik. Ez tehát egy olyan jelzés, amely kizárólag a szóbeli kommunikációval együtt fordul elő és egyben szorosan összefonódik a beszéd tartalmával. A kimondott szavakon kívül nagyon sok mindent kifejezhetünk a hangunkkal is. Megállapítható, hogy a hatékony kommunikáció alapja mondanivalónk tagolt, jól hallható és érthető bemutatása. A kiejtés legyen tiszta és pontos, kerülendő a túl gyors, kapkodó beszéd. A légzés legyen természetes, nem hallható, a hangerő pedig tegye lehetővé, hogy mondanivalónk – amennyiben több ember előtt beszélünk – mindenki számára pontosan érthető legyen. Természetesen mindezek – amennyiben így teljesülnek – mit sem érnek, ha

érdektelen, unalmas a téma, hiszen akkor hosszabb távon senki figyelmét sem lehet lekötni, de ez (is) egy a vezető sok szép feladata közül, hogy hogyan lehet egy esetlegesen unalmas, „száraz” anyagot is érdekessé tenni a hallgatóság számára.

Ahhoz, hogy valaki tökéletesen tudjon uralni bármely kommunikációs szituációt – márpedig egy rendészeti vezető tekintetében nem lehet más a cél –, ahhoz minden eszközt pontosan ismernie és tudatosan alkalmaznia kell, nem elfeledve természetesen, hogy a nem verbális jelzések alapvetően ösztönösen működnek, ezért – a verbális közléssel ellentétben – nehezen manipulálhatóak.

Megállapítható tehát, hogy a nem verbális jelzések inkább a közlő érzelmi állapotára, a kommunikációs partnerekhez fűződő viszonyára utalnak. Ahhoz, hogy a mondanivaló – és az azt kinyilvánító személy is – hiteles legyen, a verbális és nem verbális kommunikációs sajátosságok összhangjára van szükség.

A kommunikációról szóló szakirodalomban gyakran találkozni azzal, hogy az ember személyes környezetének jellegzetes tárgyait, külsőségeit is kommunikációnak veszik. Bár ennek például a *“Nem a ruha teszi az embert”* [5] szólás ellentmond, de egyrészt – bár kevésbé ismert – létezik olyan szólás is, hogy *„Ruha teszi az embert”* [6], másrészt szerény véleményem szerint is sok mindent elárul az emberről nem csak a ruhája, hanem a hajviselete, a megjelenése, illetve az a munkahelyi környezet is, amelyet a magáénak mondhat, amelynek kialakítása az ő nevéhez köthető. Buda Béla ezeket a jellemzőket *kulturális szignálnak* nevezi, melyekről így ír: „...különböző tárgyak és testi állapotok vagy díszítések kulturális jelentőséget kapnak, a kulturális konszenzus elfogadja, hogy ezeket ki lehet nyilvánítani, meg lehet mutatni, és valamilyen kifejező értékük van. Általában ezek azokat a főbb közösségeket reprezentálják a személyiségben és annak interakcióiban, amelyekben az illető személyiség él vagy amelyekben felnőtt. Ezek nagyobb része tudatosan vállalt, gondozott jelzés, csak kisebb része spontán öntudatlan.”[7]

Ha a megjelenés, a mindennapi viselet kerül szóba, mindig egy volt vezetőm jut eszembe, aki saját tapasztalatai alapján két dologra is megtanított, de talán helyesebb, ha azt írom, hogy felhívta a figyelmem. Az egyik, hogy ha azt szeretném elérni, hogy felnézzenek rám a beosztottaim, hogy mindig adjanak a szavamra vagy hogy csak nyugodt szívvel tudjam nekik jelezni, hogy ők is tartsák be az egyenruházati előírásokat, akkor soha nem szabad rendezetlen viselettel vagy ahogy ő mondta – és ezt muszáj idéznem –, „trógerul” megjelennem nemcsak a munkahelyen, hanem a mindennapi életben sem. És hogy ezt mire alapozza? Pár éve, egy meleg nyári napon lement a lakóházától mintegy 16 és fél méterre található (kis)boltba papucsban, egy rövidnadrágban és egy szakadt pólóban, és persze kívül mással találkozott volna ott, ha nem az egyik beosztottjával... Állítása szerint utána érezte, hogy már nem olyan a főnök-beosztott viszony, már nem úgy tekint rá a személy, mint azelőtt, és mivel ez szerinte ennek az esetnek volt köszönhető, így azóta akkor is „fényescipő-vasaltnadrág-vasalting”-szettet húz, ha csak leviszi a szemetet... Lehet, hogy igaza van, lehet, hogy nincs, mindenesetre elgondolkodtató a történet.

A másik eset, ami miatt egy életre szóló – és ebben az esetben feltétel nélkül megszívlelendő – tanáccsal látott el, a következő volt: délután 13.00 órára az ő főnökéhez volt hivatalos egy értekezletre, és ebéd után – mint mindig – szokása szerint megivott egy kávé. Viszont szokásával ellentétben ezúttal leitta az ingét, amit – már megint muszáj leírnom, hogy állítása szerint – se azelőtt, se azóta soha nem tett meg a munkahelyén. Persze mikor máskor történt volna, ha nem 20 perccel az értekezlet előtt? Így azóta mindig tart egy tartalék egyenruhát – nemcsak inget, hanem egy komplett szettet – a szekrényében, és ezt javasolja másnak is.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

A címben – illetve konkrétan a bevezetőben – felmerülő kérdésre véleményem szerint egyértelműen nem a válasz, azaz nem lehet senkiből sem jó (ideális) vezető jó (ideális) kommunikáció nélkül. Ahhoz, hogy valaki jó vezető legyen, több kompetenciával is rendelkeznie kell, és ezek közül csak az egyik a jó kommunikációs készség. Azonban ne felejtjük el, hogy egy vezető – mint mindenki más is – minden pillanatban kommunikál. Mivel ő az általa vezetett szervezet első számú megjelenítője, ezért nem teheti meg, hogy „elbújik a világ elől”, hogy nem megy emberek közé. Egy vezetőnek minden pillanatban készen kell állnia arra a kommunikációra, akár arról van szó, hogy egy beosztottja fordul hozzá egy problémával, akár arról, hogy a szervezeten kívül kell megnyilvánulnia. Ezért (is) különösen fontos, hogy tisztában legyen a kommunikációra vonatkozó ismeretekkel, sőt, ne csak tisztában legyen velük, hanem megfelelő szinten alkalmazza, használja is azokat a mindennapjai során.

Felhasznált irodalom

- [1] Forgács József: A társas érintkezés pszichológiája. – Kairosz Kiadó, Budapest, 2007, pp. 134. - ISBN: 978 963 913 771 4
- [2] Buda Béla: A közvetlen emberi kommunikáció szabályszerűségei. – Animula Kiadó, Budapest, 1994, pp. 71. - ISBN 963 333 043 2
- [3] Németh Erzsébet: Az önismeret és a kommunikációs készség fejlesztése. – Századvég Kiadó, Budapest, 2002, pp. 73. – ISBN: 963 921 131 1
- [4] Molnár Katalin: Rendészeti kommunikáció vezetőknek. – Rendőrtiszti Főiskola, Budapest, 2007, pp. 41.
- [5] [6] O. Nagy Gábor: Magyar szólások és közmondások. – Talentum, 1999., pp. 584. – ISBN 963 645 081 1
- [7] Buda Béla: A közvetlen emberi kommunikáció szabályszerűségei. – Animula Kiadó, Budapest, 1994, pp. 104. - ISBN 963 333 043 2