Haig Zsolt – Kovács László

Fenyegetések a cybertérből

A 2007. áprilisi és májusi Észtországot ért információs támadásra reagálva a NATO bukaresti csúcstalálkozóján a szövetség úgy döntött, hogy Tallinban létrehozza a NATO cybervédelmi központját, amely a tagállamokat érő számítógépes támadások megelőzésével, illetve ezek kivédésével foglalkozik majd. Az alábbi cikk szerzői azokat a veszélyeket és fenyegetéseket, illetve azokat az információs műveleteket mutatják be, amelyek az új központ létrehozását indokolják.

A fenyegetések új színterei

Az információs termelési korszak és az információs társadalom kibontakozásával kialakuló gazdaságot globális információs környezet veszi körül. Ennek a környezetnek a műszaki alapját az az információs infrastruktúra képezi, amely az információcserét biztosító vezetékes és vezeték nélküli távközlési rendszerek, valamint számítógép-hálózatok és egyéb információszerző, -feldolgozó és -szétosztó rendszerek összessége.

E hálózatok digitális jeltovábbító közegei az optikai kábelek és rádiócsatornák, melyek a föld felszínén, a föld alatt, a tenger felszíne alatt vagy az űrben továbbítják az információkat. Ebben a globális információs hálózatban egyre nagyobb szerepet tölt be az internet, ami a rohamos ütemben bővülő globális elektronikus kereskedelem és elektronikus pénzpiac egyre nagyobb mértékben vesz igénybe. Az információs környezetben a világ minden érintett nemzetközi és nemzeti szerve, intézménye részt vesz.

A pénzügyi és gazdasági globalizációt lehetővé tevő információs környezet és az abban foglalt információs infrastruktúrák megjelenése alapvető változást idézett elő a hadszíntér tartalmi megítélését illetően is. Az eljövendő háborúk már nem jellemezhetők azokkal a kategóriákkal, melyek az első öbölháború (1991) előtt megszokottak voltak. Az első öbölháború gyökeresen megváltoztatta a hadviselő feleknek a harc, a hadművelet megvívásáról alkotott nézeteit.

A háború korábbi működési területei és dimenziói tovább bővültek. Az információs korszak, információs környezet, információs társadalom megjelenése következtében a katonai műveletek számára egy újabb működési terület alakult ki. A hadszíntér fizikai dimenziói kiegészülnek egyéb, úgynevezett virtuális dimenziókkal. Ezek a háború, illetve a katonai tevékenységek újabb működési területei, újabb színterei. Ezeket a működési tereket összefoglalva globális információs térnek nevezik, amelyben összehangolt információs műveletek *(information operations)* zajlanak.

A harctéren a különböző hálózatba kapcsolt elektronikai rendszerek az információs színtérnek azt a részét használják, amelyben a különféle elektronikus információs folyamatok (elektronikai úton végrehajtott adatszerzés, adatfeldolgozás, kommunikáció stb.) realizálódnak, illetve az elektronikai rendszerek elleni tevékenység és a védelem megvalósul. Az informá-

ciós színtér e tartományát gyakran cybertérnek is nevezzük.

Civil terminológia szerint a cybertér az elektronikus kommunikációs eszközök és rendszerek (számítógép-hálózatok, internet, telefonvonalak, műholdas rendszerek stb.) és a rajtuk található szolgáltatások, információk alkotta virtuális tér vagy világ összefoglaló neve, amit igen gyakran alkalmaznak a virtuális valóság világára is. A cybertér katonai értelmezése azonban kiterjeszti ezt a dimenziót, és nem csak a számítógép-hálózatok működési környezetét érti rajta. Napjainkban a harctéren elektronikai eszközökből (rádiók, radarok, navigációs eszközök, harctéri azonosító berendezések stb.) és számítógépekből olyan hálózatokat hoznak létre, ahol igen nehéz különválasztani egymástól a rendszert alkotó komponenseket. Amennyiben az ezek elleni tevékenységről és a saját oldalon ezek védelméről beszélünk, akkor mindenképpen komplex rendszerként kell azokat értelmezni, amelyeknek közös működési környezetük van. A harctéren ezek a hálózatos rendszerek (többnyire mobil rendszerekként) az elektromágneses energiát használják fel az adatok, információk megszerzésére, tárolására, továbbítására. Amennyiben ezek a rendszerek a teljes frekvenciaspektrumot használják, akkor azon keresztül lehet hozzájuk férni, vagyis felderíteni és támadni őket.

Az internet sebezhetősége nagyon sokak számára ismert. Az információs társadalom működése alapvetően függ attól, hogy igen sok információs rendszer (köztük számos kritikus információs infrastruktúra) használja az internetet. Ezért az internetnek — mint önmagában is kritikus infrastruktúrának — a biztonsága nemzetbiztonsági szempontból rendkívül fontos kérdés, melyet a kritikus információs infrastruktúrák védelmének megszervezése során figyelembe kell venni.

Ugyanakkor egy országban számos olyan hálózatba szervezett rendszer is működik, amely nem csatlakozik az internethez. A katonai vezetési rendszerek döntő többsége elszigetelt, zárt hálózatként működik, közvetlenül nem kapcsolódik a világhálóhoz. Ha csökkenteni akarjuk az ellenség vezetési és fegyverirányítási képességeit, akkor ezeket a hálózatokat a cybertérben elektronikai úton a teljes frekvenciatartományban kell támadni.

Az információs műveletek koncepciója

Az információnak a tudásalapú információs társadalomban kitüntetett és meghatározó szerepe van. Az információs társadalom működése az információk és információs rendszerek támadásán keresztül jelentősen befolyásolható, károsítható, hatékonysága csökkenthető. Az információs társadalom és annak védelmi rendszere olyan számítógép-hálózatokkal átszőtt hálózatos rendszerek komplexuma, amelyben minden mindennel összefügg. Ennek következtében a rendszer bármelyik súlyponti elemének információs támadása vagy védelme nemzetbiztonsági kérdés, amely védelmi síkon kihat az egész társadalomra, s ebből következően közös ügyünk. Nemzetbiztonsági szempontból nélkülözhetetlen annak ismerete, hogy az ellenfél információs rendszerei, információs műveleti képességei és módszerei milyen fejlettek.

Az információs műveletek elmélete szerint egy társadalomban első- és másodfokú társadalmi-technikai civilizációs fejlettségi rend működhet. A fejlett társadalmi rendszerek jogi és erkölcsi törvényekkel, szabályzókkal, szabványokkal irányítottan léteznek és működnek. Ezek a társadal-

mak – a magas fokú szervezettség révén – erősen szabályozott társadalmi rendhez tartoznak, amelyet az információs műveletek szempontjából második fokozatú fejlettségi szintnek nevezünk. Amennyiben ez a magas fokú szervezettségi rend valamilyen külső vagy belső negatív társadalmi vagy természeti oknál fogva megszűnik, vagyis a fejlett törvények és szabályzók már nem képesek működni és hatni, akkor az érintett szervezeteknél és technikai rendszereknél bekövetkezik a dereguláció, a társadalmi-technikai visszaesés az első fokozatú civilizációs szervezettségi szintre, ahol a természet törvényei objektív módon – a „káosz törvénye" szerint – hatnak. Az információs műveletek során a társadalom alapvető érdeke saját oldalon a második fokozatú civilizációs rend fenntartása, az ellenfélén pedig az első fokozatú civilizációs rend ideiglenes kialakítása, vagyis irányíthatatlan helyzet, sajátos káosz-rend előidézése. Az információs műveletek ezt a célt számos társadalmi és technikai részterületen érik el.

Az információs műveletek céljai között szerepel a szemben álló fél rendszereinek, hálózatainak, szervezeteinek megfosztása attól a lehetőségtől és képességtől, hogy külső anyagi utánpótlást, energiát vagy vezetési információt kapjanak, illetve cseréljenek. Ez történhet a különböző anyagi, energia- és információs folyamatok teljes megszakításával, működésük tartós korlátozásával vagy ideiglenes kikapcsolásával, zavarásával. A fenti célok elérését biztosító, támadó jellegű információs műveleteket közvetlenül – egyes kijelölt célpontokra koncentráló direkt támadási módszerrel – vagy közvetett módon – a kritikus célpontok, hálózatok, rendszerek elleni indirekt támadással – lehet végrehajtani. Nem ritka a közvetlen és közvetett támadási eljárás, módszer kombinálása. Az információs műveletek a célpontok szövevényes összefüggése, többszintű rétegződése és mátrix jellegű hálózatos kapcsolódása következtében gyakran nem egyes célpontok ellen irányulnak. Ehelyett inkább az egész rendszert érintő és káros hatást kifejtő, a teljesítményt csökkentő, úgynevezett degradáló, deregulációs hatás elérését célzó eredményre törekszenek a hatásalapú műveletek keretében.

Az információs műveletek célkitűzéseinek másik oldala a saját vezetési és információs rendszerek, központok, összeköttetések, távközlési és logisztikai vonalak, kritikus infrastruktúrák védelme. Más megközelítéssel az információs műveletek célja az, hogy a második fokozatú civilizációs rendet minél tovább és minél teljesebb mértékben tartsuk fenn és akadályozzuk meg a szemben álló felet abban, hogy társadalmunkat az alacsonyabb fejlettségű, első fokozatú, káosz felé tartó civilizációs rendre visszavesse.

Az információs műveletek önmagukban nem elégségesek egy háborús konfliktus megnyerésére, viszont egyértelműen bebizonyosodott, hogy az információs korszakban az információs műveletek nélkül siker nem érhető el. Erre jó példát szolgáltatnak a történelem első információs műveleteinek (az 1991-es első öbölháború) és az első hálózatos vezetésű háborújának (a 2003-as második öbölháború) figyelemre méltó tapasztalatai és tanulságai. Az első öbölháborúban a szövetséges erők sikerének döntő eleme az információs és a vezetési fölény volt, amit multiszenzoros adatszerzéssel, adatfúziós feldolgozási technológiákkal, számítógép-hálózatokra alapozott harcvezetéssel, az ellenség felderítő, vezetési és fegyverirányítási rendszereinek bénításával és félrevezetésével értek el. Mindezen tevékenységeket tervszerűen, egységes vezetés

alatt végezték, ami az információs műveletek egyik alapvető elve.

Az információs műveletek azon koordinált tevékenységeket jelentik, amelyek a szemben álló fél információira, távközlési és információs rendszereire gyakorolt hatásokkal képesek támogatni a döntéshozókat politikai és katonai céljaik elérésében úgy, hogy emellett a saját hasonló rendszereiket hatékonyan kihasználják és megóvják.

Az információs műveletek célja az információs fölény, végső soron a vezetési fölény elérésével a hadműveleti előny megszerzése, ezáltal biztosítva az információs fölény birtokosa számára azt, hogy a vezetési rendszereit és azok képességeit kihasználva a hadműveletet úgy vezesse és irányítsa, hogy az ellenséget megfossza a képességeitől.

Az információs műveletek a különböző elkülönülten is létező, komplex információs tevékenységek — elektronikai hadviselés, számítógép-hálózati hadviselés, pszichológiai műveletek, műveleti biztonság, katonai megtévesztés és az információs objektumok fizikai pusztítása — közötti integrációt és koordinációt jelentik, amelyeknek a szükségességét és létjogosultságát az összehangolt információs tevékenységek nagyságrendekkel növelhető hatékonysága adja. Hatékony alkalmazásuk békeidőben elkerülhetővé teheti a pusztító katonai tevékenységet.

A hagyományos hadviselési elvek korábban is tartalmazták a szemben álló fél vezetési pontjainak pusztítását, a parancsnokságok és a harcoló csapatok közötti híradás és a fegyverirányítás zavarását. Mivel azonban e tevékenységeket többnyire önállóan – egymással nem összehangoltan – hajtották végre, csak kivételes esetekben voltak képesek döntő befolyást gyakorolni a katonai műveletek eredményességére. A gyakorlati tapasztalatok azt mutatják, hogy az esetek többségében a vezetési rendszerek támadása korábban csupán megkönnyítette a kitűzött célok elérését, de rendszerint nem vált a siker alapvető tényezőjévé. Az információs műveletek lényege éppen az, hogy elemeinek integrált, összehangolt alkalmazása döntő módon képes befolyásolni a fegyveres küzdelem kimenetelét, a katonai és politikai célok elérését.

Az információs műveletek mellett egy másik – első pillantásra és értelmezésre szinonim – információs tevékenységi fajtájával is találkozhatunk, amely az információs műveletekhez hasonlóan, egymással szemben álló felek közötti információ alapú folyamatok befolyásával foglalkozik. Ez nem más, mint az információs hadviselés *(Information Warfare – IW).*

A NATO-ban és a legtöbb tagállamában hivatalosan elfogadott információs hadviselési doktrína nem létezik, helyette a már előzőekben ismertetett információs műveletekről beszélnek.

Az USA védelmi minisztériumának információs műveletekkel foglalkozó irányelvei és összhaderőnemi információs műveleti doktrínája (JP 3–13) szerint az információs hadviselés azon információs műveleteket jelenti, melyeket válság vagy háborús konfliktus idején alkalmaznak az ellenfelekkel szembeni speciális célok elérése vagy elősegítése érdekében.

Ettől eltérő felfogások szerint az információs hadviselés ugyanazon tevékenységet jelenti, mint az információs műveletek, csak manapság e kifejezést elsősorban a civil terminológiában használják. Érdemes megjegyezni, hogy míg kezdetben a NATO információs műveletekkel foglalkozó irányelvei ugyanezt a meghatározást tartalmazták, addig a mostani, legújabb elvekben (MC 422; AJP–3.10) már az információs

hadviselés, mint információs tevékenység nem található meg. Ez is azt a törekvést és doktrínafejlődést mutatja, hogy a NATO doktrínáiban egységesen az információs műveletek jelenjenek meg, elkerülendő azokat a félreértéseket, melyek a két fogalom körül fellelhetők.

Az információs műveletek támadó és védelmi jellegűek lehetnek, amelyeket politikai, gazdasági és kulturális téren, valamint a katonai tevékenységek minden szintjén folytatnak.

A támadó információs műveletek arra irányulnak, hogy speciális célok érdekében vagy speciális fenyegetésekre válaszul hatást gyakoroljanak a másik fél információira, információalapú folyamataira, információs rendszereire békeidőben és válság vagy konfliktus idején egyaránt. Az információs műveletek támadó jellegű alkalmazása képes lelassítani és megzavarni a másik fél feladatai tervszerű végrehajtásának ütemét, akadályozni az erőkifejtés összpontosítását, valamint befolyásolni a kialakult helyzet értékelését. Az információs támadás közvetlen és közvetett formában valósulhat meg. A közvetlen információs támadás – más néven belső vagy behatoló jellegű támadás – során a támadó fél egyrészt a különböző információbiztonsági rendszabályokat kikerülve bejut a kommunikációs rendszerekbe és számítógép-hálózatokba, hozzáfér különböző adatbázisokhoz stb. és számára hasznosítható információkhoz jut. Másrészt zavaró jelekkel, megtévesztő információkkal, rosszindulatú szoftverek bejuttatásával tönkreteszi, módosítja, törli stb. a szemben álló fél számára fontos információkat. A közvetett információs támadás – más néven külső vagy szenzor alapú támadás – során a támadó fél hozzáférhetővé teszi a szemben álló fél számára a saját félrevezető információit, ezáltal megtéveszti annak felderítő rendszereit és így befolyásolja a helyzetértékelését.

A védelmi információs műveletek arra irányulnak, hogy egyrészt fenntartsák a hozzáférhetőséget az információkhoz, információalapú folyamatokhoz, és biztosítsák az információs rendszerek hatékony használatát békeidőben, illetve válság vagy konfliktus idején. Másrészt arra, hogy megvédjék a saját erők speciális céljai eléréséhez szükséges kritikus információkat. A vezetési információs rendszerek védelme azzal biztosítja saját vezetési képességeink fenntartását, hogy kihasználja a saját rendszerekben rejlő lehetőségeket, illetve lehetetlenné teszi, hogy a szemben álló fél beavatkozzon információs rendszereinkbe, minimálisra csökkenti saját vezetési és információs rendszereink sebezhetőségét és a közöttük fellépő zavarokat.

Tekintettel arra, hogy a fejlett információs társadalmak igen nagymértékben függnek az információs infrastruktúráktól és közöttük egyre inkább a távközlési rendszerektől, illetve a számítógép-hálózatoktól, nem meglepő, hogy egyes országok e rendszerek védelmét létfontosságúnak tartják. Ennek megfelelően a számítógép-hálózati hadviselés – kiegészülve az elektronikai hadviseléssel és az annak tevékenységét megalapozó elektronikai felderítéssel – cyberhadviselés néven egyre fontosabb szerepet kap az információs műveleteken belül.

A fejlett haderőkben rájöttek arra, hogy a cybertér egyre növekvő szerepet tölt be a modern hadviselésben. Felismerték, hogy amennyiben nem tesznek lépéseket a cyberhadviselési erők felállítására, akkor jelentős hátrányba kerülhetnek más országokkal szemben. Ennek megfelelően a világ több országában (USA, Kína, Oroszország) megindultak az ilyen képességek fejlesztésére irányuló törekvések. Az Amerikai Egyesült Államokban napjainkban

alakítják meg a légierő cyberparancsnokságát *(Air Force Cyber Command),* mely a tervek szerint 2008. október elején kezdi meg működését. A tervek szerint a parancsnokság feladata lesz, hogy a cybertérből nagy pontosságú önirányítású rakétákkal, elektronikai zavaró eszközökkel, lézer- és irányított energiájú fegyverekkel, továbbá számítógép-hálózati támadó eszközökkel és módszerekkel csapásokat mérjenek az ellenséges országok hálózat alapú katonai vezetési rendszereire, kritikus információs infrastruktúráira, ezen belül kiemelten az internethálózatra, a cellás rendszerű mobiltelefon-hálózatokra, az energiaellátás irányító rendszereire stb.

Támadások a cybertérből

Napjainkban egyre több cybertámadással találkozhatunk. Szinte naponta kapjuk a híreket, hogy különböző ismert és nagy forgalmú weboldalak túlterheléses támadás *(Distributed Denial of Service – DDoS)* áldozatává váltak. A legelső dokumentált cybertámadást 1997-ben egy Srí Lanka-i terrorszervezet – az Ealam Tamil Tigrisei – követték el. Két évvel később, 1999-ben szerb hackerek támadták meg a NATO-parancsnokság szervereit, és átmenetileg sikerült elérhetetlenné tenniük, illetve propagandacéllal átalakítaniuk több NATO-weboldalt. Szintén nagy port vert fel a *Moonlight Maze* (Holdfénylabirintus) fedőnevű támadás, melyet az akkori amerikai védelmi miniszterhelyettes, John Hamre szerint Oroszország intézett az amerikai védelmi minisztérium szerverei ellen. Kína is már több esetben kísérelt meg támadást amerikai számítógépes rendszerek ellen. Az egyik leghíresebb a *Titan Rain* (Titán eső) fedőnevű szisztematikus támadássorozat volt, amelynek célpontjai amerikai katonai és ipari számítógép-hálózatok voltak. Ez utóbbi két támadás közös jellemzője, hogy céljuk nem a közvetlen károkozás, hanem a védelmi rendszerek kiépítettségének és működésének tesztelése, feltérképezése volt.

A cybertérből érkező információs támadások várható hatékonyságának feltérképezésére már 1996-ban megkezdődtek a kísérletek az Egyesült Államokban. Egy ilyen kísérlet forgatókönyve az alábbi feltevésre épült.

Fejlett információs technológiával és erőforrásokkal rendelkező ipari ország információs támadást indít egy ugyancsak fejlett ipari ország ellen. Az információs műveletek folyamán stratégiai célú információs csapásokat intéztek számítógépes rendszerek és központok ellen, zavarták és pusztították a távbeszélő hálózatokat és a telefonközpontokat, továbbá az energiaellátó, szállítási, banki és egyéb kritikus infrastrukturális elemeket.

E tevékenységek eredményeként az elektronikus értéktőzsdék vásárlási és fizetési rendszerei összeomlottak. Az alapvetően fontos állami és katonai távközlési rendszerek lebénultak. A cellás rendszerű nemzeti rádiótelefon-rendszer szétesett.

Alvó programokat aktivizáltak a katonai logisztikai rendszerek számítógép-hálózataiban, aminek következtében komoly zavarok keletkeztek a fegyveres erők ellátásában. A polgári TV-csatornák adását megzavarták, megszakították, és idegen propagandaműsorok jelentek meg a képernyőkön. A vezetésbe helyezett bizalom erősen megrendült. Akadozó utánszállítások mel-

DDoS – elosztott szolgáltatás-megtagadással járó támadás. Egy számítógép-hálózati szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése ártó, támadó szándékkal, elosztottan, több forrásból.

lett felvásárlási láz tört ki. Az informatikai, elektronikai és lélektani hadviselési csapásokkal megtámadott ország vezetési rendszere és az ország működőképessége kettő-négy nap alatt összeomlott. Fontos megjegyezni, hogy e feladatokat korlátozott és minimális fizikai pusztítás, rombolás és személyi veszteség mellett hajtották végre.

2007 tavaszán azonban már nem csak kísérleti szinten láthattunk példát információs támadásra. Az igen fejlett informatikai kultúrával rendelkező Észtországban 2007. április 27-én zavargások törtek ki a tallinni szovjet hősi emlékmű eltávolítása miatt. Az első túlterheléses (DDoS) támadások jelei néhány nappal az első tüntetések után jelentkeztek a parlament, kormányhivatalok, minisztériumok, bankok, telefontársaságok és médiacégek szerverei ellen. A célpontok kiválasztása, a támadások összehangoltsága, precíz kivitelezése és hatékonysága arra mutatott, hogy e támadások hátterében szervezett erők állnak. Néhány esetben szakértők megállapították, hogy a támadások orosz szerverektől indultak, amit az orosz hatóságok természetesen tagadtak. Ugyanakkor a megtámadott szerverek jellegéből adódóan nyilvánvaló, hogy a támadások célja egyértelműen a balti állam kritikus információs infrastruktúrájának bénítása volt. Az ország online adatforgalmát irányító kulcsfontosságú szerverek naponta omlottak össze, sok állami intézmény hálózatát kénytelenek voltak ideiglenesen leválasztani az internetről. Az elektronikus banki forgalom és kereskedelem részint megszűnt, részint erősen akadozott. Egyes szakértők szerint a cybertámadás sokkal súlyosabb gazdasági károkat okozott Észtországnak, mint amit azok a kereskedelmi szankciók okoztak volna, amikkel Oroszország a krízis első heteiben fenyegetőzött.

Bár kezdetben NATO-szakértők is részt vettek a támadások felderítésében, azok jellegéből adódóan a támadó(k) azonosítása szinte lehetetlen volt. Számos támadót lehetett ugyan azonosítani orosz területen, de annak egyértelmű igazolása, hogy kormányzati szerverek voltak, sikertelennek bizonyult. Általánosan elterjedt nézet szerint orosz hazafias érzelmű hackerek olyan botnet hálózatot hoztak létre, amelybe orosz gépeken kívül számos más ország területén lévő számítógépeket is beszerveztek a tudtuk nélkül (zombi gépek), és ezeken keresztül hajtották végre a támadásokat.

Az Észtország ellen végrehajtott DDoS-támadás is bizonyítja, hogy az információs támadások hatalmas kockázatot jelentenek az egyes országok kritikus információs infrastruktúráira és rajtuk keresztül a nemzetek biztonságára. Ez a biztonsági kockázat tovább növekszik abban az esetben, ha a kritikus információs infrastruktúrákat terrorista szervezetek támadják a cybertérből. A terrorszervezetek esetében is igaz, hogy a globális információs infrastruktúráknak köszönhetően a világ bármely pontjáról megtámadhatnak a világ másik pontján lévő hálózatot vagy rendszert. Mindezt ráadásul úgy tehetik meg, hogy rendkívül kis kockázatot kell csak vállalniuk, hiszen láthattuk, hogy a támadások azonosítása, illetve bizonyítása is komoly nehézségekbe ütközik. Megjelenik tehát a cyberterrorizmus veszé-

A **botnet** olyan virtuális számítógép-hálózat, amelyben a számítógépek valamilyen rosszindulatú program hatására egyszerre, koordináltan fejtenek ki valamilyen tevékenységet (például DoS vagy DDoS támadás, tömeges spamküldés stb).

Zombi gép: a felhasználó tudta nélkül különböző rosszindulatú, például trójai programok telepítődnek a számítógépre, amelyek azután részlegesen vagy teljes egészében átveszik az irányítást a gép felett, és onnan különböző támadásokat és egyéb – adathalász (pfishing) stb. – tevékenységeket végeznek.

lye: akcióiknak megelőzésére, illetve kivédésére a jövőben szintén komoly erőkkel fel kell készülnünk.

Ilyen felkészülési, megelőzési folyamat már a NATO-ban is elindult, éppen az Észtország elleni cybertámadás hatására. A NATO-tagállamok védelmének összehangolása érdekében Észtország kezdeményezte egy Cybervédelmi Kiválósági Központ *(Cyber Defence Centre of Excellence)* felállítását. A bukaresti NATO-csúcson zajlott egyeztetéseket követően a szervezetet várhatóan nyolc ország (az Egyesült Államok, Németország, Olaszország, Spanyolország, Észtország, Lettország, Litvánia és Szlovákia) részvételével Tallinnban fogják megalakítani. E szervezet a tagállamokat érő számítógépes támadások megelőzésével, illetve kivédésével foglalkozik majd. A központ fő céljai közé tartozik, hogy a nemzetközi együttműködést javítsa, közös végrehajtó szerveket hozzon létre, illetve segítsen kidolgozni egy általánosan érvényes cybervédelmi doktrínát. A védelemmel párhuzamosan a központ természetszerűleg különböző kutatási programokat is folytatna. A kutatások során előtérbe kerülhet a mesterséges intelligencia alapú technológiák alkalmazási lehetőségeinek vizsgálata és kifejlesztése az informatikai védelem területein. Ennek során a hálózati és számítógép alapú védelmi rendszerekben olyan intelligens eljárások alkalmazási lehetőségeinek kifejlesztése a cél, ahol például a behatolás-detektálás, valamint a válaszreakciók nagymértékben automatizálhatók. A kutatás kitérhet a szabály alapú védelmi rendszerekben alkalmazható ellenőrzött és öntanuló eljárásokra, az intelligens szimulációs lehetőségek kialakításának vizsgálatára a behatolást jelző rendszer, illetve a behatolás-védelmi rendszer *(Intrusion Detection System – IDS; Intrusion Prevention System – IPS)* területén. E munka során előtérbe kerülhet a hálózatok támadási módszereinek szimulációval történő vizsgálata, valamint a hálózati védelem jogi szempontjainak elemzése is.

Összegzés

Az információs műveleteket és azon belül kiemelten a cyberhadviselést elemezve arra a következtetésre juthatunk, hogy nem hagyhatjuk figyelmen kívül az információs szférából érkező támadásokat, melyek az ország kritikus információs infrastruktúrái ellen irányulnak. Azt is szem előtt kell tartanunk, hogy ezek a támadások – az aszimmetrikus fenyegetéseknek megfelelően – nemcsak egy másik ország fegyveres erejétől származhatnak, hanem akár egyes személyektől, csoportoktól vagy különböző terrorista szervezetektől is.

Az Észtország internethálózata ellen 2007 áprilisában és májusában folytatott összehangolt támadás szemléletesen bizonyította, hogy egy információtechnológiailag fejlett ország milyen veszélyeknek van kitéve az információs szférából érkező összehangolt támadások részéről. Ezért napjainkban a legfejlettebb információs társadalmak esetében komolyan kell venni a „digitális Pearl Harbornak” elnevezett, szándékosan előidézhető elektronikai és informatikai rendszerösszeomlás veszélyét. Ellene alternatív és tartalék információs infrastruktúrákkal, rendszerekkel és hálózatokkal, valamint komplex védelem megteremtésével lehet eredményesen felvenni a harcot. A magánszféra erőforrásainak számbavétele szintén elengedhetetlen ezen a területen. Az ország valamennyi információs erőforrását, vagyis a köz- és a magánszféra erőforrásait egyaránt számításba kell venni, ha az esetleges támadó információs műveletek

ellen eredményesen kívánunk felkészülni és fellépni.

Fontos annak hangsúlyozása, hogy a cybertérből érkező információs támadásokat és agressziókat ugyanolyan veszélyforrásnak kell tekinteni, mint a többi nemzetközi, globális, regionális és nemzeti veszélyteményezőket, veszélyforrásokat. Ennek megfelelően elhárításukra országos, az információs infrastruktúrák összetettségéből és földrajzi kiterjedéséből adódóan regionális – vagy akár globális – szinten és méretekben kell felkészülni.

(Az írás a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíjának támogatásával készült.)

Irodalom

Haig Zsolt – Várhegyi István: A vezetési hadviselés alapjai. *Egyetemi jegyzet*. Budapest, 2000, ZMNE.

Fahrenkrug, David T.: Cyberspace Defined. http://www.au.af.mil/au/archive/0209/Articles/CyberspaceDefined.html (letöltve: 2008. február 24.)

Wheatley, Margaret J.: Vezetés és a modern természettudomány – rendszer a káoszban. SHL Kiadó, Budapest, 2001.

Magyar Honvédség Összhaderőnemi Doktrína. 2. kiadás. *Magyar Honvédség kiadványa*. MH DSZOFT kód: 11313. Budapest, 2007.

JP 3-13 Joint Doctrine for Information Operations. 1998.

Waltz, Edward: Information Warfare Principles and Operations. Boston – London, 1998, Artech House.

Air Force Cyber Command. Frequently Asked Questions. http://www.afcyber.af.mil/library/factsheets/factsheet.asp?id=10688 (letöltve: 2008. február 24.)

Haig Zsolt – Kovács László – Makkay Imre – Seebauer Imre – Vass Sándor – Ványa László: Az információs társadalom veszélyforrásai. A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban. *Tanulmány*. MEH Informatikai Kormánybiztosság, 2002.

Magyar Narancs – http://www.mancs.hu/index.php?gcPage=/public/hirek/hir.php&id=14820 (letöltve: 2007. június 25.)