Tóth Tivadar

TERRORIZMUS, INFORMATIKA, HADVISELÉS

MOTTÓ:
„Míg Bin Laden ujja egy AK 47-es ravaszán van, addig unokaöccséé egy számítógépes egéren”
(NATO tükör 16 2001/2002. tél)

A hadseregek tevékenységüket megváltozott illetve folyamatosan változó társadalmi, politikai, földrajzi és információs környezetben folytatják. Szóhasználatukban olyan új fogalmak jelentek meg, mint az információs háború, információs fölény, információs műveletek, információs színtér, stb. Ahogy az elmúlt században a katonai siker alapfeltételének tartották a hadszíntéren a légi-fölény megszerzését, úgy a ma és a jövő hadserege számára várhatóan ugyanilyen alapvető lesz az információs színtéren az információs fölény megszerzése.

E publikáció célja a katonai szervezet (Magyar Honvédség) és az őt körülvevő információs környezet vizsgálata, a terrorizmus és az információs háború (cyber war) szemszögéből. Arra kívánok rámutatni, hogy napjainkban mennyire fontos a felkészülés az információs színtéren történő támadások ellen.

A magyarországi rendszerváltozást követően beindult politikai, gazdasági folyamatok és a világpolitikai helyzet alakulása a Magyar Honvédség számára is kihívásokat jelent melyeknek meg kell felelnie. Feladatokat kell végrehajtani nemzeti és nemzetközi színtéren, így egy megváltozott nemzeti és globális információs környezetben is.

Az egyik legnagyobb probléma a világ szinte minden országa számára a terrorizmus jelenti. Az egyes államoknak aszimmetrikus katonai kihívással kell szembenézniük, ahol erősen eltérő felkészültségű, felszereltségű és indíttatású az ellenfél. A szeptember 11-i, a Világkereskedelmi Központ és a Pentagon elleni támadások egyik tanulsága véleményem szerint, hogy a terrorizmus bizonyos esetekben óriási anyagi, haditechnikai és mentális különbségek kiegyenlítésére is képes lehet. Ennek új területe a globális információs környezet és infrastruktúra, illetve ezek nemzeti és katonai megfelelője. Az információs infrastruktúra, illetve ennek részei a civil társadalomnak és a katonai szervezetek minden elemének (modern társadalmak esetében) elengedhetetlen összetevőivé váltak. Ha az informatikai infrastruktúra sérül, az egész rendszer megrendülését vonhatja maga után.

A közvélemény az információs háborút a hagyományos hadviseléssel összevetve egyfajta fehérgalléros bűnözésnek, közvetlen fizikai vagy emberveszteséggel nem járó, békeidős tevékenységnek tartja. Ezzel szemben ma már hatalmas veszélyeket rejt magában, ha valaki nem készül fel kellőképpen az ilyen természetű támadás ellen.

A polgári infrastruktúrák könnyen támadhatóak a hozzájuk kapcsolódó vagy őket irányító információs rendszereken (Pl.: Internet) keresztül, és arra gondolva, hogy egy terület energiaellátásának átmeneti bénulása például a kórházak esetében azonnali fizikai károkat is okozhat, világossá teszi, hogy ez milyen veszélyeket rejt magában. Ebből következik, hogy az információs társadalom megjelenése egy új hadszínteret hozott létre, ahol az egyéb téren erősen eltérő képességű ellenfelek közti harc kiegyenlített feltételek mellet folyhat. A világ sok államában stratégiai kérdés az információs infrastruktúrák védelme illetve a felkészítés az ellene való

tevékenységre. Például a kínai, orosz, izraeli hadsereg már évek óta, köztudottan kiképzési programjában tartja az ellenfél számítástechnikai eszközei, hálózatai elleni tevékenységre való felkészítést.

„A NATO-tagországok számítógépes információs rendszerei valószínűleg folyamatos célpontjai a nem hagyományos ellenség támadásainak, akinek fő célja a fizikai pusztítás és rombolás, és aki minden fellelhető gyengeséget kihasznál.” (NATO tükör 16 2001/2002. tél)

Míg a NATO koszovói légicsapásai idején, 1999-ben az akkori tagországok honlapjai elleni támadások még valószínűleg spontán, és hatásukat tekintve jelentéktelen cselekmények voltak, ma már szervezett, komoly célpontok támadása várható.

A NATO szakirodalmak az információs háború (kibernetikai háború) három fontos szintjét említik.

— információs háború katonai műveletek kiegészítéseként;
— korlátozott információs háború;
— korlátlan információs háború[1].

Az információs hadviselésnek két fő célja van. A saját képességek erősítése illetve az ellenfél képességeinek gyengítése. Az információs hadszíntéren folyó tevékenységek minden szintjén ezek a fő irányelvek.

INFORMÁCIÓS HÁBORÚ KATONAI MŰVELETEK KIEGÉSZÍTÉSEKÉNT

Célja a katonai információs infrastruktúra védelme és támadása. A tevékenység a hagyományos hadszíntér egyik eleme (információs rendszerek) ellen folyik, alapvetően szembenálló katonai szervezetek közti harc.

KORLÁTOZOTT INFORMÁCIÓS HÁBORÚ

A tevékenység kilép a katonai keretek közül. A globális és nemzeti információs infrastruktúrák, mint közvetítő közeg igénybevételével ugyanezen elemek ellen folyik a tevékenység. Az elsődleges cél a civil információs rendszerek gyengítése, bénítása, az eszközök tényleges fizikai megsemmisítése nélkül. A különféle vírus támadások tipikus eszközei ennek a szintnek.

KORLÁTLAN INFORMÁCIÓS HÁBORÚ

Itt már nemcsak a polgári és katonai infrastruktúra bénítása a cél, hanem ezek minél szélesebb körű megsemmisítése és ezen keresztül mindenféle más infrastruktúra támadása is. A hadviselés e fajtájának három fő jellemzője van:

— hatókörét és célpontjai tekintve átfogó, nem tesz különbséget a katonai és civil célpontok vagy a hátország és a harcvonal között;
— a korlátlan kibernetikai háborúnak fizikai következményei és áldozatai vannak. Ezek közül néhány olyan támadások eredménye, amelynek szándékosan a csonkítás és a pusztítás volt a célja, néhány pedig annak a pusztulásnak a következménye, ami a civil vezetési

[1] NATO tükör.

és irányítási képességekben következik be olyan területeken, mint a légi közlekedés irányítása, sürgősségi ellátás, vízgazdálkodás és energiaellátás;
— a gazdasági és társadalmi hatás — az emberéletekben bekövetkezett veszteségeken túl — mélyreható lehet.

Megszűnik a különbség hátország és hadműveleti terület között, megrendül a kormányba vetett bizalom, könnyen belső válság robbanhat ki.

TÖRTÉNÉSEK AZ INFORMÁCIÓS HADSZÍNTÉREN

1988. október 16-án az Indiai PTI hírügynökség feltételezése szerint pakisztáni hírszerző műveletként támadás érte az indiai hadsereg hivatalos WEB site-ját, a „Kashmir egy paradicsom!"-ot. A WEB oldal vendégkönyvét telítették India ellenes szövegekkel.[2] Az oldal címét kicserélték az „Állítsátok meg Indiát és mentsétek meg Kashmirt!" szövegre. Fotókat helyeztek el Indiaiak által meggyilkolt Kashmiri aktivistákról.

1998. október 2-án a Kosovo Information Centre, az albán nemzetiségű Dr. Ibrahim Rugova-val rokonszenvező honlapjára törtek be a szerb Crna Ruka (Fekte Kéz) terrorszervezet hackerei. A Szerb nemzeti címert és egy angol nyelvű üzenetet helyeztek el az oldalon: "Üdvözlünk a legnagyobb hazugok és gyilkosok Web lapján". A honlap helyreállítása után újabb támadás történt, ekkor a következő üzenet jelent meg: „Ezt az oldalt a szerb Fekete Kéz hackerei törték fel. Sokáig éljen nagy Szerbia!" Korábban szerb számítógépes kalózok (bevallásuk szerint egyetemisták) kényszerítettek egy svájci Internet szolgáltatót egy koszovói albán hírújság a „Glas Kosova" eltávolítására a szolgáltató szerveréről. Mikor a szolgáltató megbízottja tárgyalásokat fojtatott a hackerekkel azok észlelve, hogy figyelik őket, megrongálták a svájci szolgáltató egyik számítógépét.

Belorussziában Alekszander Lukasenkó elnök Web oldalán helyeztek el egy képet, amin az elnök fotója először Hitlerré, majd Sztálinná alakul.

Lengyelországban egy fiatal hacker betört a Gazdasági minisztérium honlapjára. Az „eseményt" a miniszterelnök, Wlodzimierz Cimoszewicz sem hagyta szó nélkül: „Engem elszomorít, amikor azt olvasom, hogy a hacker most egy magán cégnél dolgozik. Szívesen alkalmaznám a kormányzatnál."

A Taiwan i televízióban a Védelmi Minisztérium Információs és Kommunikációs hivatalának vezetője bejelentette, hogy válaszul a Kínai Hadsereg elektronikus támadásaira egy ezer vírusból álló készletet hoztak létre, amit szükség esetén fel is fognak használni.[3]

Malajziai Kuala Lumpurban két 20 éves fiatal az egész várost megbénító pánikot keltett, amikor elárasztották az Internetet hamis hírekkel arról, hogy menekültek tömegei kaptak munkavállalási engedélyt és megindultak a város felé.

2000-ben az arab izraeli konfliktus eszkalálódott teljes körű információs háborúvá. Izraeli hackerek megtámadták a Hezbollah csoport oldalait Londonban, mire válaszul a Hezbollah betört az izraeli Külügyminisztérium Honlapjára.[4].

---

[2] BBC News: Sci-Tech India opens virtual front in Kashmir.htm, 2000. január 10.
[3] BBC News: 2000. január 10.
[4] Newsfactor: Fanatics with Laptops The Coming Cyber War.htm, 2002. május 16, Homepage: www.newsfactor.com

MIT TEHETÜNK?

Pillanatnyilag nincs és valószínűleg soha nem is lesz teljes védelem az információs rendszerek elleni támadással szemben. Felkészülni a károk csökkentésére azonban lehet és kell is.

A legteljesebb védelmet az információs hálózat izolációja, fizikai elkülönítése biztosítja. A legérzékenyebb információk és rendszerek védelmére zárt, belső hálózatokat kell létrehozni, ha ezt a tevékenység jellege lehetővé teszi. E megoldás hátránya, hogy a környezettel nincs elektronikus információ csere. Ilyen megoldást használtak az USA hadserege a délszláv konfliktus idején. A megoldást „Légkábel”-nek nevezték. Egy információs tiszt az Internetre kapcsolt számítógépről leolvasott adatokat begépelte a belső hálózat számítógépébe, így az teljes védelmet élvezett a hacker támadásokkal szemben.

Ha fontos a környezet információs rendszereivel a kapcsolat, akkor valamilyen titkosítási eljárással védhetjük meg az adatainkat. Ekkor azonban csak az információt tudjuk védeni az infrastruktúrát már nem.

A rendszert és az információt is védik a különféle „tűzfalak” (Firewall). Ezek a belső és a külső hálózat közé telepített szoftveres vagy hardveres eszközök a hálózaton áramló digitális formátumú adatok figyelésével, azonosításával védenek. Egyfajta egyirányú szelepként működnek. A védett hálózatból kifelé szabad az adatáramlás, befelé korlátozott.

Figyelmeztető, monitoring rendszerek telepítésével a betörést ugyan nem gátoljuk meg, de az illetéktelen behatolásról értesülve óvintézkedéseket foganatosíthatunk.

A fenti eljárások természetesen csak megfelelő adatkezelési fegyelem és biztonsági rendszabályok betartása mellett hatékonyak. Alapvető fontosságúak az alábbiak:

- minden felhasználó rendelkezzen egyéni nehezen visszafejthető, rendszeresen módosított jelszóval;
- felismert támadást követően azonnal konfiguráljuk újra a hálózatot;
- folyamatosan ellenőrizzük, frissítsük rendszereinket;
- gondos naplózással feltérképezhetőek a rendszereinket ért támadások;
- a gyanús tisztázatlan eredetű elektronikus adatokat utasítsuk vissza.

A fenti megoldások a már megkezdett vagy végrehajtott támadások elleni védekezés eszközei. Hasonlóan a hagyományos hadviseléshez, itt is hatékony lehet a megelőzés, az elrettentés. Meg kell gondolni, hogy informatikai támadásra csak hasonló választ adhatunk-e, vagy adminisztratív és erőszakos eszközök alkalmazásával megfelelő elrettentő hatást érhetünk-e el?

Megállapíthatjuk, hogy technikai és tudományos fejlődésnek üdvös hatásai mellett komoly veszélyei is vannak. Az információs háború eszköztárát ellenségeink, mint hatékony fegyvert fogják ellenünk használni. Ennél is veszélyesebb lehet, ha ezek a terroristák eszközeivé válnak. Az információs színtéren való védekezést, tevékenység tervezését feltétlenül be kell építeni az aktuális biztonságpolitikába. Még nincs későn!

FELHASZNÁLT IRODALOM

[1] NATO tükör 16 2001/2002. tél, http:// www.nato.int
[2] Defense Technical Information Center Homepage, URL: http://www.dtic.mil/
[3] Fanatics with Laptops The Coming Cyber War.htm, 2002 május 16., www.newsfactor.com
[4] BBC Homepage: URL: http://news.bbc.co.uk
[5] NATO on-line library Homepage:http://www.nato.int/docu/