ELŐADÁSOK

Kis-Benedek József

Információs hadviselés korunk alacsony intenzitású konfliktusaiban

Az információs hadviselés helye, szerepe a biztonságpolitikában, valamint a mai fegyveres és nem fegyveres küzdelmekben

A hadviselés karaktere az elmúlt évtizedben jelentősen megváltozott, de semmiképpen nem lehet azt kijelenteni, hogy az út végén vagyunk. A hadviselés módja és az azt szolgáló technológia olyan ütemben fejlődik, hogy a lépéstartás még a témában jártas szakemberektől is megköveteli a változások folyamatos, naprakész követését. Az információs hadviselés támadásban és védelemben egyaránt megjelenik. Hiba lenne azonban a tevékenység leszűkítése csak katonai területre, hiszen ettől lényegesen szélesebb. Ez persze nem jelenti azt, hogy a katonai területen ne lennének sajátosságok (elég, ha csak a szenzorok által nyújtott adatokra, a számítógépes terrorizmusra, a pszichológiai hadviselésre, a médiaháborúra, vagy a műholdak rombolására gondolunk).

A különböző nemzeteknél egymás után jelennek meg a számítógépes védelemmel kapcsolatos szervezetek, parancsnokságok, a NATO esetében pedig talán nem véletlen, hogy Tallinban hozták létre a Számítógépes Védelem Kiválósági Központját (Cooperative Cyber Defence Centre of Excellence). Az egységes NATO-fellépést illetően fontos kérdés annak eldöntése, hogy az 5. cikkely mikor és milyen feltételek teljesülése esetén kerülhet alkalmazásra. Az állásfoglalás kialakítását illetően – úgy vélem – általános szabályt nehéz meghatározni, hiszen minden eset egyedi elbírálást követel.

A téma fontosságát jelzi, hogy a közelmúltban szervezett biztonságpolitikai fórumokon, mértékadó források által készített tanulmányokban foglakoznak az információs hadviseléssel. Az évente megszervezett müncheni biztonságpolitikai fórumon például 2011-ben az első alkalommal került szóba a számítógépes terrorizmus fenyegetése. Ennek veszélyét *Clinton*, amerikai külügyminiszter egy szintre helyezte a terrorizmussal és a tömegpusztító eszközökkel.

Ma már az internet a kritikus infrastruktúra részének számít, ezért indokolt az ennek megfelelő kezelése. A számítógépes bűnözés a világon évente 1600 milliárd dollár veszteséget okoz. Tekintve, hogy a tendencia növekszik, senki sem lehet közömbös a fenyegetés kezelését illetően.

A biztonságpolitikával foglalkozók előtt nem ismeretlen *Joseph Nye*, a Harvard egyetem professzora, aki szerint a cybertér biztonsági fenyegetése markánsan három területen jelentkezik. Ezek: az internetbűnözés, a gazdasági kémkedés és a terrorizmus. A gazdasági kémkedéssel kapcsolatban érdemes megemlíteni, hogy kínai hackerek több mint 3000 vállalatot támadtak meg. A cél egyértelmű: információszerzés.

Az Egyesült Államok 2011-ben elfogadott új Nemzeti Katonai Stratégiája szerint a cybertér minden területen hatékony fellépést követel. Mivel a kihívás nem katonai természetű, igen fontos kérdés a stratégiai parancsnokságok kapcsolata a kormányzati és nem kormányzati (NGO) szervezetekkel, de az iparral és természetesen a nemzetközi élet szereplőivel is. Az együttműködés célja világos: új normákat kell felállítani, új képességeket, és ha szükséges szervezeteket kell létrehozni a szaktudás kifejlesztése érdekében. Úgy vélem, hogy ezen a területen az oktatás, a képzés és a továbbképzés szerepét nem kell külön hangsúlyoznom, hiszen ez magától érthető. A védekezés alapelve változatlan: felfedés, elrettentés, megtagadás és az infrastruktúrák többoldalú védelme. Ami viszont folyamatosan változik: a módszer.

Ha az aszimmetrikus műveletek és az információs hadviselés kapcsolatát vizsgáljuk, akkor megállapítható, hogy az aszimmetrikus hadviselést folytatók másképpen gondolkodnak, szerveznek és tevékenykednek, mint a hagyományos hadviselést folytatók azért, hogy saját előnyüket és az ellenség gyengeségét kihasználják. Ez egy új képesség, amit a szembenálló fél többnyire nem is vesz észre. Az információs műveletek eszközt jelentenek az aszimmetrikus műveletek ellen, ezért a stratégiai tervezés részét képezik. A műveletek eszközöket biztosítanak a kívülről, vagy belülről érkező támadások felfedéséhez, a támadásokra való reagáláshoz, a helyreállításhoz, de a behatolástól való elrettentéshez is.

A haderők ma már képesek az aszimmetrikus támadások *egy része* ellen védekezni, de – tekintettel arra, hogy az információs műveletek terén a módszerek gyakran változnak – a kihívások természetesen folyamatosan léteznek. A kihívások kezelésében a legfontosabb tényező a gyorsan fejlődő technológiákkal történő lépéstartás és a kiképzettség. A technológia ugyan segít, de korántsem elegendő a bizonytalanság kezelésében.

Az információs hadviselés rövid története

Az információs hadviselés katonai területen a ’80-as évek közepétől jelent meg, előtte inkább az elektronikus hadviselés elnevezést alkalmaztuk. A Falkland-szigetek birtoklásáért folytatott 1982-es háborúban viszonylag nagy intenzitással használták az eljárást. Az akkori művelet azonban speciálisnak tekinthető, ugyanis izolált szigetekről volt szó, kommunikációt szinte csak a haderők alkalmaztak és szinte mindent cenzúráztak.

Az 1991-es Öbölháborúban a hangsúly inkább a technológián és nem az információn volt. A háború és a média kapcsolata ekkor jutott el arra a szintre, hogy a haderők vezetése kénytelen volt tudomásul venni a médiával történő „foglalkozás” nélkülözhetetlenségét. Ez a rendszeres tájékoztatásokkal kezdődött, majd a későbbiek folyamán az tovább tökéletesedett. Bebizonyosodott, hogy a média a katonai műveleteket segítheti, de komoly károkat is okozhat azoknak. Fokozatosan alakult ki a

tájékoztatások rendszere (akár napi gyakorlata), majd a média képviselőinek „beágyazása" (embedded journalist) a katonák közé.

A '90-es években a kommunikációs technikák és a számítástechnika olyan gyors fejlődésen ment keresztül, hogy a korszerű háború egyben médiaháborúvá is vált. Ismeretes a *CNN-effektus,* amit napjainkra már inkább az *al Dzsazíra-effektus* vált fel, több szakemberrel és nagyobb lehetőségekkel.

„9/11" tapasztalatai azzal járultak hozzá az információs hadviseléshez, miszerint ugrásszerűen megnőtt a nemzeti tájékoztatás iránti igény. Ez a jelenség azóta fokozódott, és még érzékenyebbé vált. A tudósítók beépítése az információs hadviselés részévé vált, ahol a tájékoztatást adók célirányosan hívják meg a média képviselőit, gyakran személyes kapcsolatokat is kiépítenek. Arra is nagy figyelmet fordítanak, hogy a tájékoztatást adók alaposan felkészüljenek, igyekezzenek magukat elfogadtatni. Ha ugyanis a tájékoztatás nem korrekt módon történik, akkor a média megtalálja a módját annak, hogyan tájékozódjon.

A 2003-ban kezdődött iraki háborúban az információs műveletek a teljes infoszféra ellen folytak. Ennek része volt az a taktika is, hogy a háború ürügyeként szolgáló téves premisszákat (iraki tömegpusztító eszközök megléte) bizonyítsák a világ előtt. Ez az eljárás tévesnek bizonyult, ami általános bizalomvesztést okozott kormányok, de főként azok vezetői iránt. Kis túlzással az is elmondható, hogy az információs hadviselésben a fegyverek helyett számítógépeket, lőszer helyett adatcsomagot, a szögesdrót helyett pedig tűzfalat alkalmaztak. Tömeges e-mail és telefonüzeneteket küldtek iraki politikai, gazdasági és katonai vezetők részére, amelyben felszólították őket, hogy szakítsanak *Szaddám Huszeinnel.* 8 millió röpcédulát dobtak le repülőgépekről, amelyben felszólították a katonákat, hogy adják meg magukat és akkor túlélik a háborút. Elektronikus támadást indítottak erőművek, kommunikációs rendszerek és számítógépes hálózatok ellen, amelynek célja az iraki katonák megtörése, valamint a polgári lakosság befolyásolása.

James R. Wilkinson tábornok, az Egyesült Államok Központi Parancsnoksága (US Central Command) egyik vezetője szerint az információs hadviselés célja a háború rövidítése. Ez a megállapítás többé-kevésbé elfogadható, sőt azzal is kiegészíthető, hogy bizonyos esetekben a háborút késleltetheti, esetleg meg is akadályozhatja.

Az Egyesült Államokban már 1999-ben naponta 80–100 támadást érzékeltek. A támadók közül azok az egyéni támadók a legveszélyesebbek, akik törvényes hozzáféréssel rendelkeznek az informatikai rendszerekhez. Az ellenük folytatott védekezés ebből adódóan csak intézményes formában lehetséges. A fegyveres erők esetében rendszeres támadások folynak a kapcsolódó hálózatok (például kereskedelmi műholdak, az INTELSAT, az INMARSAT) ellen is. A kedvenc célok nem változtak. Ezek a hírközpontok, vezetési pontok, radarállomások és a légvédelmi központok. Sajátosságként állapítható meg, hogy tettükért az elkövetők nem vállalják a felelősséget.

A védekezés lehetséges módszerei között ki kell emelni a műveleti biztonságot, a megtévesztést, a pszichológiai műveleteket, az elektronikus ellentevékenységet és végső esetben a fizikai megsemmisítést. Ennek természetesen feltétele a megfelelő kommunikációs és számítógépes infrastruktúra és a kiképzés.

A Közel-Keleten az elmúlt évek aszimmetrikus háborúi során minden esetben éltek az információs hadviselés eszközeivel.

Lássunk erre néhány példát:

– 2009 januárjában, a Gázai-övezet elleni izraeli támadás során, az izraeli fél megszakította a gázai rádió adását és a lakosság az izraeli katonai rádió adását hallhatta. Ebben figyelmeztették a lakosságot, hogy a Hamasz embereitől különüljenek el. Ezt az üzenetet számos mobiltelefonra is elküldték.
– Hasonló esetekkel találkozhatunk Libanonban és Szíriában, ahol izraeliek mobiltelefonokra küldtek üzeneteket, megnehezítve ezzel az iszlám szélsőségesek tevékenységét. Izrael rendszeresen hackeli a Hezbollah TV- és rádióadásait. Célja a Hezbollah lejáratása.
– Szíriába több ezer üzenet érkezett mobiltelefonokra azzal a szöveggel, hogy Izrael 10 millió dollárt fizet annak, aki segítséget nyújt eltűnt izraeli katonák felkutatásában. Érdekesség, hogy a szír hírszerzés ebből azt a következtetést vonta le, miszerint Izrael ügynököket toboroz, a lakosság viszont úgy vélte, hogy a szír hírszerzés keresi az Izraellel együttműködőket.
– 2011-ben az egyiptomi katonák irányított röplapokat osztottak szét (ami azt jelenti, hogy meghatározott személyek kapták) és SMS-eket küldtek az alábbi szöveggel: *„Jogotok van arra, hogy civilizált módon kifejezzétek véleményeteket […] Elismerjük a polgárok követelésének jogosságát, nem fogunk a polgárok ellen erőszakhoz folyamo*dni".[1] A tüntetések szervezése során felhasználták az internetet, a Facebookot és természetesen a mobiltelefonokat. Amikor a hatóság leállította az internetforgalmat, akkor kezdték alkalmazni az írásos utasítás módszerét az aktivistáknak, a röplapokon konkrét feladatokat határoztak meg. Ilyen utasítás volt például, hogy a tüntetés legyen békés, tilos a rendőrség provokálása, nem szabad összekeveredni a garázda elemekkel. A hadsereg ugyanakkor a rend és nemzeti vagyon védelmezőjeként lépett fel. A bemutatott tevékenység tehát úgy értékelhető, hogy az információs hadviselés lehet egyben a humánmozgósítás és az irányítás eszköze is.

Az iráni atomprogram elleni hackertámadás

Az információs hadviselés aktuális példája az iráni atomprogramot késleltető hackertámadás, amely több éves, összehangolt konspiratív akciók sorozatából áll. A művelet során a fedett és nyílt elemek keverednek egymással. A történések nyílt források alapján az alábbiakban összegezhetők.

2008 elején *Bush*, volt amerikai elnök, engedélyt adott titkos művelet végrehajtására, amelynek célja Natanzban az iráni elektromos és számítógépes rendszerek zavarása. A zavarást vírusbevitellel tervezték végrehajtani oly módon, hogy a centrifugák működését megzavarják, de a kezelők az ellenőrzés során azt az üzenetet kapják, hogy a rendszer normálisan működik.

Az USA Belbiztonsági Minisztériuma még 2008-ban tanulmányozni kezdte a Siemens P.C.S.-7, (Process Control System-et), amely a szenzorok és a gépek működését hangolja össze. (Megjegyzés: Iránba a Siemens cég szállította az ipari számító-

1 Forrás: MTI, 2011. 02. 11.

gépek ellenőrző berendezéseit). A szabályozó rendszer sebezhetősége a szakemberek számára nyílt titok volt. 2008 tavaszán a német Siemens-cég közös projektet indított az Egyesült Államok Nemzeti Laboratóriumában, Idahoban, a számítógépek irányító rendszerének ellenőrzésére. A Siemens képviselői úgy tudták, hogy a projekt célja termékeik ellenőrzése volt egy esetleges számítógépes támadás esetére, míg az amerikai cél a Siemens-rendszerek működésének megismerése volt. *Langner*, a Siemens cég számítógépes részlegének volt pszichológusa szerint a féreg a vezérlő egység csak egy specifikus konfigurációjában lépett működésbe és olyan folyamatot indított el, ami csak centrifugáknál fordul elő. A művelet célja nem üzenetküldés volt, hanem katonai stílusú célmegsemmisítés.

2009 nyarán Európában és az Egyesült Államokban új vírus jelent meg, ami rendkívül komplexnek és találékonynak minősült. A szakemberek rövid időn belül tanulmányozni kezdték. Az eredményeket 62 oldalon összegezték egy Chicagóban tartott tudományos konferencián, de az összeállított anyag további sorsa nem ismert, a honlapról is eltűnt.

Az iráni atomprogram ellen hozott ENSZ-határozat értelmében a vezérlő és elektromos szabályozó egység szállítása is szankció alá esik. A Wikileaks által kiszivárogtatott információkból ismertté vált, hogy az Egyesült Államok Külügyminisztériuma 2009-ben táviratot küldött Dubaiba: akadályozzák meg 111 doboz eljutását Bandar Abbasba. A csomagok szabályozó egységeket tartalmaztak.

2009-ben Izrael a dimonai atomerőműben kísérleteket kezdett az Iránihoz hasonló centrifugán a Stuxnet-vírussal. A kísérlet célja annak modellezése: miként lehet a vírust úgy bejuttatni a rendszerbe, hogy a berendezések ne semmisüljenek meg, hanem csak *rombolás, késleltetés*, *szabotázs* történjen. A támadás nem az összes számítógépet, hanem csak azok egyötödét érte.

Kérdésként merülhet fel, vajon hogyan került a centrifuga Dimónába. Ez hosszabb történetre nyúlik vissza, de ismert, hogy *A. Q. Khan*, pakisztáni atomtudós, 1976-ban Hollandiában ellopott egy kisméretű kísérleti centrifugát, majd hazatérését követően a gyártási technológiát eladta Iránnak, Líbiának és Észak-Koreának. Az izraeli hírszerzés nyugdíjas dimonai kutatók segítségével beépült az iráni dúsító programba.[2] Tény, hogy a dimonai projektről sem Izrael, sem az Egyesült Államok nem nyilatkozik. Ugyanakkor azonban politikai vezetők szájából elhangoztak olyan vélemények, amelyek arra engednek következtetni, hogy a projekt létezik, bár jó néhány kérdés továbbra is titokban marad.

Clinton, amerikai külügyminiszter és *Meir Dagan*, a Moszad volt igazgatója szinte egy időben nyilatkoztak, melynek lényege, hogy Iránnak technológiai problémái vannak, amely az atomprogramot 2015-ig késleltetheti.

Gary Samore, *Obama* elnök tömegpusztító fegyverek alkalmazásával foglalkozó stratégiai tanácsadója Iránról az alábbiakat nyilatkozta a sajtónak: *„Örömmel hallom, hogy Iránnak problémái vannak a centrifugáikkal. Az USA és szövetségesei mindent megtesznek annak érdekében, hogy még bonyolultabb legyen a helyzetük”*.[3]

---

2 Forrás: Avner Cohen *The Worst-Kept Secret 2010* című könyve.

Érdekességnek számít, hogy *984* számítógép kapott üzenetet, Irán pedig azt jelezte az ellenőröknek, hogy *984* gépet kivontak a rendszerből. *Ahmedinezsád*, iráni elnök is megszólalt 2010 novemberében: „… *néhány centrifugánál számítógépes támadás kisebb problémákat okozott*". Hozzátette azt is, hogy szakértőik ezt felfedték. Ez a nyilatkozat ugyanakkor bizonyítékot szolgáltatott a projekt kivitelezőinek arról, hogy az irániak felfedték a vírus jelenlétét.

A leírt példa, ha nem is tárgyalja részletesen a projekt megvalósítását, arra mindenképpen jó, hogy felvessük azt a kérdést: vajon képes-e az információs hadviselés helyettesíteni egy háborút. (A kérdés eldöntését az olvasóra bízom, azonban a történet segít a válasz megtalálásában.) Jelen esetben nem biztos, hogy helyettesítésről beszélhetünk, azt a jövő dönti el. Késleltetésről azonban mindenképpen szó lehet.

3 Forrás: New York Times, 2011. 01. 16.