A terrorizmus és indirekt hatása a kiberterében

Simon László[1] – Dr. Magyar Sándor[2]

Absztarkt

A szerzők általános rendszerszintű látásmóddal közelítik meg a terrorista cselekmények hatását kifejezetten Európa kiberterére, induktív módon európai esetekből kiindulva vonnak le általános következtetéseket. Az ISIS[3] azzal fenyeget, hogy halálos kimenetelű kibertámadásokat tervez a jövőben. A terroristák új dimenzióban támadják az egyének biztonságát. Fegyveres harcuk során a gerillákhoz hasonlóan az információt helyezik műveleteik központjába. A média szerint a terroristák harcában az információ és a kommunikáció egyszerre lehet halálos és nem halálos fegyver is. A cikk összegzése szerint az internetet fenyegetésre használó arctalan bűnözők csak indirekt módon olthatnak ki életeket.

Kulcsszavak: terrorizmus, kibertámadás, gerilla hadviselés, információs környezet, információ- és hálózat-centrikus hadviselés hadikultúrája

Abstract

The authors make a general approach and system-wide effect of terrorist attacks specifically on the cyberspace of EU. Inductively starting from European cases and makes an overall conclusion. According ISIS' threat, 'fatal' cyber-attacks are planned for the future. The terrorists are attacking to the security of individuals in a new dimension. During their harmed struggle, they put the information on central of their operations like the guerrillas. The media said the information and the communication can be and not can be deadly weapon at a time in the terrorist war. According to a summary of the article faceless criminals use the internet to the threat, that these acts are killing only.

Keywords: terrorism, cyber-attack, guerrilla warfare, information environment, war culture of information- and network- centric warfare.

[1] *NKE NBI, szakoktató, e-mail: simon.laszlo@uni-nke.hu*
ORCID ID: 0000-0001-6771-8621
[2] *NKE NBI, egyetemi adjunktus, e-mail: magyar.sandor@uni-nke.hu*
Orcid ID: 0000-0002-6085-0598
[3] *ISIS: Az Iszlám Állam elnevezésű terrorszervezet (Islamic State of Iraq and Syria) angol rövidítése.*

Bevezetés

A 20. század második felében a világ technikai környezete forradalmi változásokat élt meg. Az információ és a digitális tudás került a figyelem központjába, továbbá az innovatív ipari fejlesztések előterébe is. Az addig ismert és biztonsági szempontból is jól kontrollált környezetünk teljesen megváltozott. A társadalmi, politikai, gazdasági, szociális és nem utolsó sorban katonai előnyöket is magába rejtő digitális technológia megvalósítása olyan információs és infokommunikációs hálózatok kialakítását jelentette, amelyek nem csak a technikai rendszerekre, de az emberi kapcsolatokra is hatást gyakorolhat.[4] A posztmodern társadalmakban[5] az emberek együttélésének új, határokat nem ismerő, idillikus (szabad, boldog és békés) képe született meg. Az életünket a globalizáció, illetve a személyes és elektronikus kapcsolatok bonyolult viszonyrendszere egyszerre azzal a reménnyel kecsegtette, hogy az információkhoz időben és igényeink szerint, akár korlátlanul is hozzáférhetünk. Ez a technológiai távlatokban is rövid forradalom a 21. századra kiépítette az információs társadalmakat.

A globalizáció és az információs hálózatok elterjedése katalizátorként hatott az 1991-ig fennálló bipoláris világ megszűnésére. Politikai, jogi és biztonsági szempontból a két világhatalom, az Amerikai Egyesült Államok (USA) és a Szovjetunió (SZU) – illetve a hozzájuk kapcsolódó katonai tömbök – viszonylag statikus, de mindenképpen kiszámíthatóbb környezetet jelentettek az országok élete, fejlődése szempontjából. A SZU felbomlása után nem sokkal szertefoszlott az idillikus jövő képe. A 2001. szeptember 11-i terrortámadást követő politikai és katonai lépések – a már említett hálózatokon megjeleníthető információkkal – új fenyegető és gyakorta arctalan ellenséget teremtettek. Az addig hagyományos és reguláris módon folytatott „kis háborúk", illetve fegyveres küzdelmek[6] kiléptek a földrajzi környezet által meghatározott fizikai térből. Az al-Kadia és az Iszlám Állam (ISIS) elnevezésű terrorszervezetek mára ezeken az említett földrajzi

[4] SIMON László: Az információ mint fegyver? In: Szakmai Szemle 2016. 1. sz. pp. 34-60.

[5] Az amerikai gondolkodók a 19. század végén arra a felismerésre jutottak, hogy a politika nemcsak nemzetállami kereteken belül, hanem globálisan is értelmezendő. A társadalomelméleti következtetésekben kimondták, hogy az emberek életében politika nem lehet beavatkozó. A posztmodern (modern utáni) felfogásként illetett politikának szolgálóvá és segítővé kell válnia. Európában Jean-François Lyotard a „La condition postmoderne" című 1979-es művében használta a fogalmat először, amikor a késői ipari (posztindusztriális) társadalom és a plurális demokrácia után megjelenő társadalomelméleti lehetőségeket elemezte. In: BOROS János: Jean-François Lyotard, a különbözőség elgondolója, Kísérlet egy tudáselméleti megközelítésre. Jelenkor: Irodalmi és Művészeti Folyóirat, XLII. évf. 3.sz. 1999. pp. 298-306.

[6] RESPERGER István, KISS Álmos Péter, SOMKUTI Bálint: Aszimmetrikus hadviselés a modern korban – Kis háborúk nagy hatással. Zrínyi Kiadó, 2014. pp. 13-44.

területeken megerősödve, a lakosságot megnyerve vagy megfélemlítve, kvázi államként képesek fenntartani hatalmukat. Cikkünkben arra keressük a válaszokat, hogy a szervezetek által végrehajtott támadásokban és a hatalom megszerzése, fenntartása területén milyen szerepe lehet az információs hadviselésnek. Feltevésünk szerint az ellenük eddig alkalmazott hagyományos hadviselés módszerei mellett sokkal jobban kell koncentrálni az információs, illetve az infokommunikációs hálózatok nyújtotta lehetőségekre, mert a kibertér jelenleg a terrorizmus egyik legalkalmasabb eszköze a politikai és a katonai célok elérése érdekében.[7]

Az információs műveletek és környezetük jelentősége a kibertérben

Az információs forradalom egyik következményeként a klasszikusan elkülöníthető társadalmi, természeti és technikai környezetek egyre inkább átfedik egymást. A modern kori problémák megközelítése, illetve hatékony megoldása holisztikus elemzést és értékelést igényel.

Elgondolásunk szerint a tudományos elemzési modellek elsősorban egy adott tudományterület mélységi kutatásait erősítik. Egyes területek érintkezésekor szükséges vizsgálatok interdiszciplináris megközelítése miatt, akaratlanul is ellenmondás, illetve tudományos értelemben vett versenyhelyzet alakulhat ki. A tudomány a kutatási eredmények szigorú kritikája és a vitája során haladhat előre.[8] A kibertér kutatására ez hatványozottan igaz. Minél inkább szeretnénk megismerni azt, annál kevésbé tudunk egy-egy tudományág önálló megállapításaira hagyatkozni. Véleményünk szerint a kibertér egyszerre lehet technikai és társadalmi rendszer, ugyanakkor a természeti struktúrákhoz, organizmusokhoz hasonló, akár természeti törvényszerűségeket mutató virtuális környezetként is felfogható.

Ezt a szemléletet követve az európai kiberteret a Haig Zsolt által választott hármas egységben közelítettük meg.[9] Az információ, a társadalom és a biztonság összefüggéseiben folytatott kutatás alapját így nemcsak a fizikai eszközök (hardverek) működésére és kapcsolataira lehet alapozni, hanem a társadalomra és az életünket meghatározó mindennapi folyamatokra, illetve következményekre is. A terrorista csoportok tevékenységét és a terrort (agressziót) elsősorban ebben a térben folytatott, illetve közvetített folyamatok összhatásaként értelmeztük A terrorszervezetek célja ideológiáktól és vallásoktól függetlenítve közvetve vagy közvetlenül politikai háttérrel bírt. A célpontok tekintetében első

[7] *HAIG Zsolt: Információ, Társadalom, Biztonság. NKE Szolgáltató Kft, 2015. pp. 93-122.*

[8] *BERÉNYI Dénes: Hogy látja ma egy fizikus a világot? http://vigilia.hu/regihonlap/2010/7/berenyi.html (Letöltés ideje: 2017. 09. 15.)*

[9] *HAIG Zsolt: Információ, Társadalom, Biztonság. NKE Szolgáltató Kft, 2015. pp. 93-122.*

sorban a megfélemlítésre, a rettegésre és a pánikkeltésre koncentrált.[10] Az alkalmazott erők, eszközök és módszerek tekintetében rendre végeláthatatlan gyűlöletet, rombolást és káoszt tapasztalhattunk. A 21. század tanúsága szerint a terrorizmus fegyveres támadásai – a csekély erő- és anyagi források kapcsán – az információs fölény elérése mellett elsősorban a lakosság megnyerésére és bevonására irányul. Ebből adódóan mára a Közel-Keleten folytatott fegyveres harc során jelentősen növelték a „közvetett műveleteknek" nevezhető eljárásokat. Ezek rendre indirekt és kognitív hatású, hálózatokban megjeleníthető, bármilyen plusz információtartalmú közlések, illetve szimbolikus értékkel bíró cselekmények (pl.: támadásokhoz kapcsolódó hekkelés, kiszivárogtatás, mém-gyártás, közösségi megosztás). Az USA-ban és Európában végrehajtott terrortámadások esetében sajátságos pszichológiai és információs hatásokat tapasztalhattuk.[11]

A katonai területen kidolgozott és alkalmazott műveletek vizsgálatához stratégiákat, doktrínákat, műveleti eljárásokat, egyéb szabályzatokat találhatnak az érdeklődők. A hadtudomány ezen a területen az ellenséges cselekmények felderítésére, akadályozására, megelőzésére, illetve a hasonló információs tartalmú közdelem megvívására és megnyerésére már több kérdéskörben is adott katonai és sok esetben, polgári értelemben is sikeres válaszokat.[12]

A 2016. július 07-08-án a varsói NATO csúcson is kinyilvánításra került, hogy a számítógépes támadások veszélyt jelentenek a Szövetség biztonságára, amire ugyanolyan hatásuk lehet, mint a hagyományos fegyvereknek. Ezért a különböző katonai jellegű műveletek miatt a lehetséges légi, szárazföldi és tengeri hadszínterek mellett a kibertér is hadszíntérnek[13] tekinthető.[14] Az életet egyre több

---

[10] Bővebben: KIS-BENEDEK József: Dzsihadizmus, radikalizmus, terrorizmus. Zrínyi Kiadó, 2016. p. 279.

[11] Bővebben: SIMON László: A fokozódó terrorizmus Európában és annak hatása a katonai tömegrendezvények biztosítására. In: Szakmai Szemle, 2015. 2. sz. pp 145-162.

[12] MUNK Sándor: Hadtudományi kutatók és kutatási területeik, 1. rész: A hadtudomány részterületeinek empirikus vizsgálata. Hadtudomány, 2015. 1-2. sz., pp. 4-16.

[13] „Hadszíntér: háromkiterjedésű földrajzi térség, amelyben a hadviselő (összeütköző) felek haderőiket összevonják,
szétbontakoztatják, és egységes hadászati elgondolás és terv alapján haditevékenységet folytatnak." … „A
haditechnikai fejlődés ma már problematikussá teszi a hadszínterek elhatárolását, mivel azok a szemben álló
hadviselő felek országainak teljes mélységére kiterjedhetnek, valamint a kozmikus térségre is." SZABÓ József
(szerk.): Hadtudományi lexikon. 1. köt. 472. o.

[14] „Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea." Warsaw Summit Communiqué, 70-71 pont.

számítógépes rendszer támogatja, amelyek kiesésének hatása – különös tekintettel a kritikus- infrastruktúrákra, információs infrastruktúrákra – fokozott kockázatot jelent a nemzetek számára.

Az információs műveletek tárgykörének ismerete segíti a terrorizmus indirekt hadviselésének stratégiai és lokális szintű megértését. A Magyar Honvédség 2014-ben kiadott információs műveletek doktrínája[15] – a NATO AJP-3.10 doktrínában[16] foglaltakkal megegyezően – az alábbi információs műveletek sorolja fel:

- Lélektani műveletek (angolul: Psychological Operations – PSYOPS);
- Megjelenés, viselkedés, arculat (a.: Presence, Posture, Profile – PPP);
- Műveleti biztonság (a.: Operational Security – OPSEC);
- Információs biztonság (a.: Information Security – INFOSEC);
- Megtévesztés (a.: Deception)
- Elektronikai hadviselés (a.: Electronic Warfare – EW)
- Fizikai megsemmisítés (a.: Physical Destruction – PD)
- Kulcsfontosságú vezetőkkel való érintkezés (a.: Key Leaders Engagement – KLE);
- Műveletek számítógépes hálózatokkal (a.: Computer Network Operations – CNO);
- Civil-katonai kapcsolatok (a.: CIMIC).

Rózsa Tibor 2016-os doktori értekezésében – hivatkozva többek között a technológia és a nemzeti haderők fejletségi szintjeire – teljes áttekintést nyújt a műveletek taktikai szintű, lokális alkalmazhatóságáról. Kutatásai kapcsán kiemelte, hogy az információ katonai felhasználásának fejlődési iránya az indirekt hadviselés[17] előretörésével, illetve annak stratégiai szintű alkalmazásával teljesedhet ki: *„Lényege, hogy a háború fő célkitűzései, illetve az elérni kívánt végállapot nemcsak a célpontok fizikai megsemmisítésével, hanem stratégiai hatások kiváltásával, többek között információs műveletek alkalmazásával is megvalósíthatók.*

http://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber (Letöltés ideje: 2017. 07. 31.)

[15] Ált/57 Információs Műveletek Doktrína 1. kiadás, a Magyar Honvédség kiadványa 2014.

[16] AJP 3-10. Allied Joint Doctrine for Information Operations pp. 1-3. http://info.publicintelligence.net/NATO-IO.pdf (Letöltés ideje: 2017. 09. 15.)

[17] Rózsa értekezésében csak a hagyományos hadviselést érinti, pedig az indirekt hadviselés a gerilla hadviselés hadikultúrájának is része. In: RÓZSA Tibor: Az információs műveletek alkalmazásának lehetőségei a Magyar Honvédség feladatrendszerében. NKE Doktori (PhD) Értekezés 2016, http://hhk.uni-nke.hu/uploads/media_items/rozsa-tibor-ezredes-az-informacios-muveletek-alkalmazasanak-lehetosegei-a-magyar-honvedseg-feladatrendszereben.original.pdf (Letöltés ideje: 2017. 09. 15.)

Ebből adódóan a műveletek hatásalapú megközelítése a tervezett végállapot elérésére koncentrál és ennek szem előtt tartásával foglalja rendszerbe a műveletek tervezését, végrehajtását és értékelését."[18]

A magyar katonai doktrína értelmezése szerint az információ „felhasználásával" kapcsolatos műveletek során – például a NATO-nak, egy ad-hoc szövetségnek, illetve adott nemzetnek (nemzeteknek) – a stratégiai célok elérése érdekében a képességeknek megfelelően összehangolt kommunikációs tevékenységet kell folytatnia magasabb műveleti szinteken is. A nemzeti feladatok végrehajtása során a stratégiai kommunikáció szintjén egységesen kell kezelni a nyilvános diplomácia, a tömegtájékoztatás, katonai és közkapcsolati tájékoztatás, valamint együttműködés, továbbá az információs műveletek és a lélektani műveletek egymásra ható eszközrendszerét.

Az országokban, így hazánkban is rendelkezésre álló számítógépes és infokommunikációs hálózatok ez alapján egy speciális műveleti környezetként értelmezhetők. Ebben a térben megjelenő káros (nem jogkövető) cselekményeket folytató egyéneket (csoportokat) így nemcsak bűnözőkként kell vizsgálnunk.

Az internet, mint média szerepe egyre növekszik. Az online hírek gyors terjedése, a különféle internetes hírportálok hírvadászata a megfélemlítéseknek hatékony, gyors forrása tud lenni, mindamellett, hogy az olvasókat befolyásolni tudják. A verseny a hírek mielőbbi megjelenítéséért sok esetben azt eredményezi, hogy a valóságtartalom ellenőrzése nem történik meg. Az internetes társadalom befolyásolása a híroldalakon keresztül az úgynevezett álhírekkel (hoax) is megvalósulhat, ami ugyanúgy képes a közvélemény befolyásolására a „virtuális fegyvertárban" szerepeltetve, mint a valós életben a robbanószerek.

Az interneten folytatott befolyásolás már az országok választási rendszereiben is jelen van, amelyről egyre több hír[19] kerül napvilágra. Ezen tevékenységek bizonyítása azonban nehéz, sokszor lehetetlen feladat.

A kibertér egyik sajátossága, hogy a felhasználók és közösségeik, így a terrorista szervezetek rejtett kommunikációt, információ megosztást tudnak folytatni rajta, olyanokat, amelyek felderítése rendkívül nehéz. Az adatok átvitelének ellenőrzése a túlmutat a közfelfogás szerinti hangfelismerés és a lehallgatások eddigi rendszerén. A védelem területén ki kell terjeszteni a gondolkodásunkat többek között az internetalapú hangkommunikációra, a titkosított csatornákra, a szteganográfiára, a különféle csetelési lehetőségekre is, amelyek akár a többszereplős internetes játékok üzenőfelületein is folyhatnak.

A klasszikus pont-pont közötti információcsere (az egyszerű adó-csatorna-vevő modell) valós és virtuális elemei, már nem egyértelműen azonosíthatók. A

[18] *Uo. pp. 35-36.*

[19] *MTI: Orosz napilap mutatta be hogyan befolyásolták az amerikai választásokat 2017.10.17. In: www.Sg.hu, https://sg.hu/cikkek/it-tech/127765/orosz-napilap-mutatta-be-hogyan-befolyasoltak-az-amerikai-valasztasokat (Letöltés ideje: 2017.10.18.)*

felhőszolgáltatások elterjedése további lehetőségek tárházát hozta elő a védendő információ rejtésének.

A kibertér felületet nyújt a terrorista szervezeteknek a toborzásokhoz. Széles körben tudják a világhálón rejtve és nyíltan is hozzáférhetővé tenni ideológiájukat, propaganda videóikat, amelyekkel bizonyos körülmények között élők sok esetben azonosulni tudnak. A kiképző táborokba az interneten történő toborzás hatására számos fiatal indul meg, akik sok esetben visszafordíthatatlan szélsőséges radikalizálódáson esnek át.

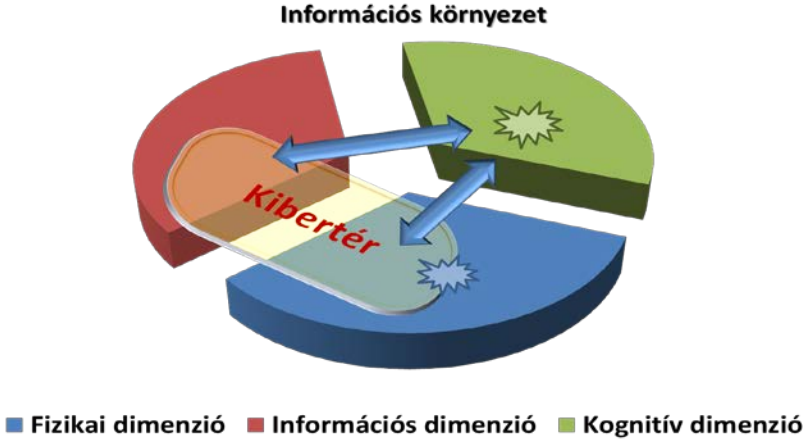
Az internetes felhasználók tömegei elől rejtett, illetve kevésbé ismert és használt deep (mély) WEB, dark (sötét) WEB lehetőséget nyújt a terrorszervezeteknek az illegális fegyverkereskedelemre, a különféle támadási technikák – például robbanószer előállításának – népszerűsítésére. A felderítés, védelemvalójában egy macska-egér játékhoz hasonló. A „jó" oldal az eseményeket követni, de a valós személyek felfedése rendkívül nehéz és költséges az interneten átmenő forgalom nagysága és a titkosító technológiák alkalmazása miatt. A hekker oldal képes a piacon szereplő eszközök, technológiák tesztelésére és a sérülékenységek felfedése után azok használatára, amely sok esetben „zero day" sérülékenységként még hónapokig használható, azok felfedezéséig és a védekezési technika publikálásáig.

A kibertérben folytatott ellenséges tevékenységek, üzenetek megjelenítése során az elkövetői körben növekvő számba jelennek meg magukat dzsihadistáknak valló harcosokból álló közösségek. Nem csak bűnügyi szempontú, egyedi, illetve csoport-motiváció alapján, „szükségleteik kielégítése céljából" cselekszenek, hanem mint katonák, harcosok. Az ő esetükben a katonai többnemzeti megoldások során eddig alkalmazott módszerek kibővítése és elmélyítése lehet a megoldás. A kulturális felfogások sokszínűsége miatt ez egyre komplexebb és folyamatosan frissülő megközelítést igényel. Az eltérő motívumú elkövetők ellen folytatott kommunikációs és információs tevékenységeknek katonai értelemben koherensnek kell lennie. Kölcsönösen erősítenie kell egymást a részvevőknek úgy, hogy a hordozott üzenetek minden szinten (pl.: politikai, katonai, stratégiai, regionális, helyi értelemben) egyeztetett, valamint a végrehajtásban közreműködő, „nem csak katonák" számára is érthető és egységes legyen.[20]

A terrorizmus kapcsán jelentkező konfliktusok rendezésének, illetve az abból fakadó válságok kezelésének bonyolult rendszerében a katonai és nem katonai elemek kooperációját kell megvalósítani. Ezzel párhuzamosan az egymásra ható feladatok végrehajtásának egységes felfogása egyre bonyolultabb információs megközelítést, illetve tervezést igényel. A harcoló felek környezetét, a célokat és a célközönséget is egységként kell kezelnünk, mint a fegyveres küzdelmek esetében.

[20] *Ált/57 Információs Műveletek Doktrína 1. kiadás, a Magyar Honvédség kiadványa 2014.*

A legkülönbözőbb társadalmi, technikai, vagy akár ideológiai hálózatokba kapcsolt individuumok miatt nemcsak a fizikai erőszakkal, hanem az információ közvetlen hatásaival is foglalkoznunk kell. A földrajzi és a virtuális tér kapcsolata olyan „hadszíntér", amelyben a kognitív tartomány támadhatóságának felértékelődésével kell szembe néznünk. Ebben a bennünket is körülvevő speciális információs környezetben a terrorszervezetek egyre növekvő hatékonyságot tudnak felmutatni. Az egyének bonyolult társadalmi, környezeti és technikai kapcsolatrendszere, valamint a közvetített üzenetek célba juttatása miatt az általunk már említett „közvetett műveletek" információ és hálózat-centrikussá váltak. A hálózatokat alkotó rendszerek támadása, illetve védelme – amely eddig leginkább technikai értelemben valósult meg – kibővül a kapcsolódó kognitív térben folytatható műveletekkel (1. ábra). Mivel a hálózatok működése a felhasználóik nélkül értelmüket veszítik, ezért mára az egyének biztonsága többletjelentéssel bír. Ebben a hálózat alapú információs környezetben egyszerre és egymásra hatva vannak jelen a felhasználók, mint állam- és választópolgárok, illetve az életüket meghatározó állami és társadalmi szervezetek (pl.: kulturális, közlekedési, oktatási, gazdasági, humanitárius hálózatok), és nem utolsó sorban az adott közösségek meghatározó szimbólumok is.



1.ábra: Az információs környezet (saját szerkesztés)

A kibertér a jelenlegi racionális felfogás szerint fizikai és információs dimenziójából áll. Az információs környezetben ezt egészíti ki a kognitív dimenzió. A kibertérben folytatott harcot a kiberhadviselés katonai értelmezése írja le: Az információs fölény részeként értelmezhető kiberfölény kivívása *„az információs*

hadviselésen belül folytatott kiberhadviseléssel valósítható meg."[21] Már az értelmezés is azt mutatja, hogy a racionális megközelítésen túl, a kibertérben folytatott küzdelem nem csak a fizikai rendszerek pusztításáról, illetve katonai értelemben az ellenséges célpontok fizikai megsemmisítéséről szól. A fegyveres harc közvetlen hatásai mellett értékelésünk szerint megjelenik egy elvont, kognitív elem is, amely e küzdelem közvetett hatását is magába foglalja. A társadalom, a gazdaság, az oktatás, az egészségügy vagy például a közszolgáltatás egyes elemeinek, illetve a közösségek szimbólumainak összekapcsolt erőszakostámadása, pontosan a közvetett hatásaiban éri el a félelmeink növekedését. Az általunk közvetett támadásként értelmezhető műveleteket követően a fizikai állapot vis--szaállítása, a szabályok felülvizsgálata, illetve módosítása, valamint a védelem újraszervezése (egy új kórház, egy iskola vagy egy felhőkarcoló felépítése) az emberek biztonságérzetét már nem fogja tudni teljes mértékben visszaállítani. Jelenkori tapasztalatainkat a terrorizmus és az ellene folytatott küzdelem napról, napra bővíti. Az információk közvetett hatására válnak egyesek radikálissá és agresszívvá. Vannak olyanok, akik – közvetlen kapcsolat nélkül – az ISIS vagy az al-Kaida mint terrorjelenség nevében gyilkolnak. Teszik ezt úgy, hogy repülőgépeket vagy teherautókat használnak fel, amelyek hagyományos értelembe véve még fegyvernek sem minősülnek.

A kibertérben folytatott tevékenységek jogi kérdései

Az Európai Unió kiberbiztonsági stratégiája számos átfogó kérdéssel foglalkozik, melyek az alábbiak:

- *„kibertámadásokkal szembeni ellenálló képesség elérése;*
- *a számítástechnikai bűnözés drasztikus csökkentése;*
- *kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (KBVP) tekintetében;*
- *kiberbiztonsági ipari és technológiai erőforrások kifejlesztése;*
- *összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára, és az Unió alapértékeinek támogatása."* [22]

A fentieket figyelembe véve a stratégia csak védekező képességeket tartalmaz. A kibertámadás felvetése napirenden kívül esik, amelyet katonai értelemben – terrorista és extrémista szervezetekkel szembeni fellépés, aktív beavatkozások és válaszlépések nélkül – nehéz értelmezni.

[21] *HAIG Zsolt: Információ, Társadalom, Biztonság. NKE Szolgáltató Kft, 2015. pp. 95.*

[22] *Az Európai Unió kiberbiztonsági stratégiája http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52013JC0001 (Letöltés ideje: 2017. 09. 15.)*

A kibertérben folyó műveleteket jogi aspektusból vizsgálva a támogatás megelőző csapással, aktív támadással történő esete jogszabályi oldalról nem definiált. Ez egyrészt abból adódik, hogy nehezen bizonyítható a kibertérben folyó tevékenység, a másik oldalról pedig a tevékenységek főleg a támadás megelőzésére, felderítésére vagy a kár elhárítására irányulnak. Ezért katonai értelemben gyakran kérdésként merül fel, hogy a kibervédelem támadás nélkül hozhat-e védelmi szempontból megfelelő eredményt, vagy szervezeti szinten kell felállítani olyan támadó képességet, amely egy esetleges rosszindulatú beavatkozás esetén képes a rendszereket ért támadás hatásának csökkentésére, esetlegesen a támadó fél semlegesítésére.

A nemzeti kiberbiztonsági stratégiában foglaltak szerint célként került rögzítésre, hogy Magyarország *„rendelkezzen hatékony megelőzési, észlelési, kezelési (reagálási), válaszadási és helyreállítási képességekkel a magyar kiberteret érintő rossz szándékú kibertevékenység, fenyegetés, támadás, illetve vészhelyzet, valamint a vétlen információszivárgás ellen,”*[23] A tevékenységek itt is védelmi jellegűek, az aktív védelem említése nélkül.

A honvédelmi miniszter éves értékelő és feladatszabó vezetői értekezlete előkészítésének és végrehajtásának feladatairól szóló 84/2014. (XII. 23.) HM utasításban már megjelent jogszabályi oldalról a kibertérből származó információszerző képesség (Cyber Intelligence) fejlesztése, amely nem összetéveszthető a nyílt forrású információszerzéssel (Open Source Intelligence).

Kibertérben jelentkező események megelőzése érdekében eseménykezelő központok üzemelnek nemzetközi együttműködésben,[24] melyek feladata a tájékoztatások, riasztások megtétele mellett az eseménykezelések, hatósági feladatok ellátása. Az úgynevezett CERT-ek szerepe a jövőben tovább növekszik az internet alapú technológiák, a dolgok internete (IoT) terjedésével párhuzamosan.

A nem katonai értelmű támadó szándék a Büntető Törvénykönyvről szóló 2012. évi C. törvényben megjelenik az információs rendszer vagy adat megsértése fejezetben, amelyben definiálásra kerül az információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belépés szankciója.[25]

A katonai oldal kihívásai

A kibertér a hagyományos hadszínterekhez képest jelentős különbséget mutat. A virtuális térben való jelenlét teljesen más felkészültséget igényel, mint akár a

[23] *Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat.*

[24] *Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény.*

[25] *A Büntető Törvénykönyvről szóló 2012. évi C. törvény 423. §164 (1).*

szárazföldi, légi, vagy a haditengerészeti területen. A „kiberkatonák” esetében a „túlélés” legkevésbé a fizikai képességeken mutatkozik meg, az informatikai tudás, az általuk használt célszoftverek és eljárások ismerete esetükben a meghatározó. A fizikai követelmények teljesítése sok, a feladatnak és beosztásnak megfelelő jelöltet rostál ki.

Kihívásként jelentkezik a kimagasló tudással rendelkező informatikusok felvétele és katonai pályán tartása, mivel a civil életben a keresetük többszörösét érhetik el és a kötött jogszabályok a külsős fizetések szintjéig történő eltérítést nem teszik lehetővé.

A pályán tartást nehezítik, hogy folyamatos képzések lennének szükségesek a megfelelő hatékonyság eléréséhez, azonban azok igen költségesek és tovább növelik a katona tudásának piaci versenyképességét. Így csak a legnagyobb hivatástudattal rendelkezők informatikusok maradnak a szervezetek keretein belül. A megfelelő képzések biztosítják a szoftver kritikus biztonsági hibák, biztonságos programozás elsajátítását.

Észtország példájára az önkéntes kibervédelmi tartalékos rendszer[26] megoldást nyújthat a kiberterroristák által végrehajtott műveletek elhárításához, illetve a szükséges ellenreakciók megtételéhez, azonban ez komoly tervező feladatot igényel. Az önkéntes tartalékos kibervédelmi egység létrehozásának indokait Krasznai Csaba 2011-ben már összefoglalta.[27]

A kibertámadások ugyanúgy veszélyeztetik a kritikus információs rendszereket, mint ahogy a katonai műveleteket is. Célzott támadásokkal a haderő béke és tábori rendszereit is veszélyeztethetik a terrorista szervezetek kibercsoportjai. A kiszivárgott kiberfegyverek, vagy a napjainkban egyre gyakoribb zsarolóvírusok és kampányaik valós veszély hordoznak. Kassai Károly véleménye szerint a „kibervédelem” területű gondolkodás a honvédelmi szakterületen a miniszteri utasításban meghatározott információbiztonsági politika komplex továbbfejlesztését jelenti. A kihívások a következő területekre csoportosíthatók:

- szabályozási környezet kialakítása (érintett szervezetek hatáskörének, feladataink kijelölése, beleértve a különleges jogrend speciális esetét);
- az elektronikus adatkezelő hálózatok biztonsági szintjének emelése (technikai jellegű feladatok);
- kibertámadások elleni képességfejlesztés (az elektronikus

[26] *KASKA, Kadri - OSULA, Anna-Maria, - STINISSEN Jan: The Cyber Defence Unit of the Estonian Defence League, Tallinn 2013. https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf (Letöltés ideje: 2017. 09. 15.)*

[27] *KRASZNAI Csaba: A magyar elektronikus közigazgatási alkalmazások információbiztonsági megoldásai. ZMNE 2011. (PhD értekezés) http://krasznay.hu/presentation/szerzoi_ismerteto_krasznay.pdf (Letöltés ideje: 2017. 09. 15.)*

eseménykezelés és az elektronikus információvédelmi feladatok felügyeleti kérdései);
- a szaktudás növelése (felhasználók és üzemeltetők szerint specializált képzések, beleértve a kibervédelmi gyakorlatok kérdését is);
- kutatás és fejlesztés (nemzeti és nemzetközi szintű lehetőségek felhasználása);
- együttműködés (egyszerűen megfogalmazva: akivel csak a kétoldalú előnyök mentén az elképzelhető).[28]

Következtetés

Az országok és emberi közösségeik eltérő erőforrása, stratégiai és taktikai elképzelése, továbbá a kulturális és többek között vallási sokszínűsége számos eddig ismeretlen folyamatot eredményezett. A már említett infokommunikációs hálózatok segítségével a média élre tört az emberek tájékoztatása terén, és bemutatta a tudás „Janus-arca" mellett a távoli konfliktusok, szélsőségek és erőszak sokak számára értelmezhetetlen valóságát. A posztmodern társadalmak korára az európai polgárok, mint individuumok („biztonsági objektumok") mindennapjait egyre inkább a hálózatokban áramló adatok és információk megismerése, megosztása, illetve birtoklása határozta meg.

A kibertér, mint új hadszíntér számos feladat elé állítja a jövő katonai gondolkodását. Az információs műveletek komplexitása képességek felállítását, erősítését igénylik. A kibertérben folytatott műveletekhez szükséges technikai és humán erőforrás igényeket fel kell mérni és tudatosan ki kell alakítani.

Felhasznált irodalom

- 1139/2013. (III. 21.) Korm. határozat - Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- 2013. évi L. törvény - az állami és önkormányzati szervek elektronikus információbiztonságáról
- 2012. évi C. törvény - a Büntető Törvénykönyvről szóló
- BERÉNYI Dénes: Hogy látja ma egy fizikus a világot? (2010) http://vigilia.hu/regihonlap/2010/7/berenyi.html (Letöltés ideje: 2017. 09. 15.)
- BOROS János: Jean-François Lyotard, a különbözőség elgondolója, Kísérlet egy tudáselméleti megközelítésre, Jelenkor: Irodalmi és Művészeti Folyóirat, XLII. évf. 3.sz. 1999. pp. 298-306. ISSN 1588-0885

[28] *KASSAI Károly: Kibervédelem és a Magyar Honvédség. Hadmérnök, VII. évfolyam, 4. szám, p. 137-138.*

- HAIG Zsolt: Információ, Társadalom, Biztonság, NKE Szolgáltató Kft, 2015. pp. 93-122. ISBN 978 615 5527 08 1
- KASKA, Kadri - OSULA, Anna-Maria, - STINISSEN Jan: The Cyber Defence Unit of the Estonian Defence League, Tallinn 2013. https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf (Letöltés ideje: 2017. 09. 15.)
- KASSAI Károly: Kibervédelem és a Magyar Honvédség, Hadmérnök, VII. évfolyam, 4. szám, p. 137-138.
- KIS-BENEDEK József: Dzsihadizmus, radikalizmus, terrorizmus, Zrínyi Kiadó, 2016. p. 279. ISBN 978 963 327 739 3
- MUNK Sándor: Hadtudományi kutatók és kutatási területeik, 1. rész: A hadtudomány részterületeinek empirikus vizsgálata, Hadtudomány, 2015. 1-2. sz., pp. 4-16. ISSN 1215 4121
- RESPERGER István - KISS Álmos Péter - SOMKUTI Bálint: Aszimmetrikus hadviselés a modern korban – Kis háborúk nagy hatással Zrínyi Kiadó, 2014. pp. 13-44. ISBN 978 963 327 592 4
- RÓZSA Tibor: Az információs műveletek alkalmazásának lehetőségei a Magyar Honvédség
- SIMON László: A fokozódó terrorizmus Európában és annak hatása a katonai tömegrendezvények biztosítására, In: Szakmai Szemle, 2015. 2. sz. pp 145-162. ISSN 1785-1181
- SIMON László: Az információ mint fegyver? In: Szakmai Szemle 2016. 1. sz. pp. 34-60. ISSN 1785-1181
- SZABÓ József (szerk.): Hadtudományi lexikon. 1. köt. Magyar Hadtudományi Társaság, Budapest, 1995. ISBN 0469000676354
- Sz.n.: AJP 3-10. Allied Joint Doctrine for Information Operations pp. 1-3. http://info.publicintelligence.net/NATO-IO.pdf (Letöltés ideje: 2017. 09. 15.)
- Sz.n.: Ált/57 Információs Műveletek Doktrína 1. kiadás, a Magyar Honvédség kiadványa 2014. feladatrendszerében, NKE Doktori (PhD) Értekezés 2016, http://hhk.uni-nke.hu/uploads/media_items/rozsa-tibor-ezredes-az-informacios-muveletek-alkalmazasanak-lehetosegei-a-magyar-honvedseg-feladatrendszereben.original.pdf (Letöltés ideje: 2017. 09. 15.)
- Sz.n.: Az Európai Unió kiberbiztonsági stratégiája. http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52013JC0001 (Letöltés ideje: 2017. 09. 15.)
- Sz.n.: Orosz napilap mutatta be hogyan befolyásolták az amerikai választásokat. MTI. 2017.10.17., https://sg.hu/cikkek/it-tech/127765/orosz-napilap-mutatta-be-hogyan-befolyasoltak-az-amerikai-valasztasokat (Letöltés ideje: 2017.10.18.)