Szentgáli Gergely

A NATO kibervédelmi politikájának fejlődése

„A jövő háborúit nem csupán felfegyverzett katonák és bombákat szóró repülőgépek vívják majd. Ezeket a háborúkat egy egérkattintással el lehet kezdeni, akár a világ túlsó végén úgy, hogy e célra készített komputerprogramok bénítsák meg vagy pusztítsák el a kritikus infrastruktúrát az ellenséges országban: a szállítást, a kommunikációt, az energiahálózatot. Megbéníthatják a katonai hálózatokat is, amelyek a csapatok vagy a repülőgépek mozgását irányítanák."[1] *(Liam O'Murchu, Symantec Security Response) Cikkünk azt a kérdést vizsgálja, mit tesz a NATO annak érdekében, hogy a szövetség és tagállamai eséllyel vegyék fel a versenyt a legdinamikusabban fejlődő új biztonsági kihívás, a kibervédelem terén.*

Amit tudunk, és amit nem

Az IBM globális piacvezető informatikai vállalat évközi beszámolója 2011-et a „kibertámadások évének" nevezte az informatikai rendszereket érintő „biztonsági események" (sikertelen és sikeres betörési kísérletek) számának robbanásszerű növekedésére utalva.[2] A trend mind a magánszektor, mind a kormányzati szféra számára riasztó emelkedést mutat, nem csupán számszerűen, hanem az okozott anyagi kárt tekintve összegszerűen is. Az amerikai Nemzeti Nukleáris Biztonsági Hivatal *(National Nuclear Security Administration)* beszámolója szerint naponta 10 milliós nagyságrendű számítógépes biztonsági eseményt regisztrálnak. Thomas D'Agostino igazgató hozzátette, hogy a támadások teljes spektrumával kell számolniuk, megjegyezve, hogy a számtalan magányos elkövető mellett komoly kormányzati aktivitás is megfigyelhető. A kibertámadások súlyosságát megerősítve, Richard Clarke, a Fehér Ház korábbi antiterrorista tanácsadója szerint kevesebb mint 15 perc alatt nagyon komoly, halálos áldozatokkal is járó pusztítást lehetne véghezvinni az Egyesült Államokban anélkül, hogy egyetlen terrorista vagy ellenséges katona lépte volna át az államhatárt.

A Symantec és a Norton 2011-es Kiberbűnözési jelentése *(Cybercrime Report)* az elkövetett bűncselekmények által okozott globális kárt éves szinten 114 milliárd dollárra becsülte, amelyet további 274 milliárd dollár másodlagos veszteség egészített ki az időveszteség és szolgáltatás-kiesés következtében. A Norton 24 ország 18–64 év közötti lakosai körében végzett széles körű felmérése alapján extrapolált adatai szerint a 431 millió áldozatot érintő és összesen 388 milliárd dollár veszteséget okozó kiberbűnözési szektor így nagyobb kárt okoz, mint a globális marihuána-, kokain- és heroinkereskedelem összesített értéke[3] (amely az ENSZ 2005-ös és 2011-es kábítószer-jelentései alapján mintegy

1 Clayton, Marc: *The new cyber arms race.* The Christian Science Monitor, 2011. 03. 07. (2012. 02. 11.)
2 Bővebben: *Cyber Security Threat Landscape*. IBM, 2012. (2012. 08. 21.)
3 *Cybercrime Report 2011.* Norton-Symantec, 2011. (2012. 10. 01.)

Kibertörténelem
1973 – Az amerikai DARPA *(Defense Advanced Research Projects Agency)* kutatást kezdeményez számítógéprendszerek közötti hálózati kapcsolat létrehozása céljával
1984 – William Gibson tudományos-fantasztikus író kitalálja a kibertér *(cyberspace)* kifejezést
1994 – James Der Derian először használja a kiberelrettentés *(cyber deterrence)* fogalmát a Wired magazinban
2007 – Az Idahói Nemzeti Laboratórium szimulációjában igazolják, hogy egy ipari létesítmény elleni kibertámadás fizikai kárt is képes okozni
2007 – Áprilisban és májusban 22 napon át támadták Észtország kormányzati és közigazgatási informatikai hálózatait
2008 – A grúz–orosz háborút orosz kibertámadás vezeti be a grúz kormányzati információs infrastruktúra ellen
2010 – Működésbe lép az Egyesült Államok Kibervédelmi Stratégiai Parancsnoksága, a Pentagon hivatalosan is hadszíntérként kezeli a kiberteret
2010 – Az iráni nukleáris létesítmények ellen alkalmazott Stuxnet az első olyan katonai jellegű támadás, amely fizikai kárt okoz
2011 – Fokozódik a kibertérben működő, különböző célokat megfogalmazó nemzeti és nemzetközi civil szerveződések, hackercsoportok (Anonymus, LulzSec, Iranian Cyber Army) tevékenysége
(Bővebben lásd Szentgáli Gergely: *2006 óta történt jelentős incidensek a kibertérben.* biztonságpolitika.hu, 2011. 10. 24.)

288 milliárd dollárra rúg[4]). Természetesen ez csak játék a számokkal, hiszen a közölt adatok csupán merész becslések, és fel sem mérhető a fel nem ismert, be nem jelentett vagy fel nem mért bűncselekményekből keletkező kár összege. Mindezt pedig nem is lenne értelme összehasonlítani azzal a kockázattal, amit a kibertér katonai dimenziója rejt magában, és amelyre a világ technikailag fejlett országainak választ kell adniuk.

„A következő a probléma – fogalmazta meg találóan James Mulvenon, a washingtoni nonprofit Cyber Conflict Studies Association alapítója tavaly – a kibertéri konfliktusok történetében 1946-ban járunk. Itt állunk ezzel a hatásos új fegyverrel, de még nem rendelkezünk a koncepcionális és doktrinális háttérrel arra vonatkozóan, hogyan használjuk, például elrettentésre. A Stuxnet 2010-ben kicsiben demonstrálta a digitális szuperfegyver erejét, mint a hirosimai atombomba 1945-ben a nukleáris fegyverekét. De ami rosszabb, hogy ma ezzel a fegyverrel nem csupán az amerikaiak és a szovjetek rendelkeznek – emberek milliói és millió birtokolják a képességet világszerte, ellenőrizetlenül."[5] Így egyelőre biztosan csupán egy dolgot tudunk: lépéskényszerben vagyunk. Kérdés, hogy ki, milyen irányban, és a források szűkössége idején milyen hatékonysággal lesz képes választ adni a napról napra sokasodó kihívásokra.

Az első NATO-tapasztalat

A NATO először az 1999-es koszovói bombázás során szembesült a kiberhadviselés eszközeivel.[6] A katonai beavatkozás 1999. március 24-én indult Slobodan Milošević csapatai ellen. A bombázás legitimitása önmagában is aggályos volt, tekintve, hogy az ENSZ Biztonsági Tanácsa nem adott felhatalmazást a támadás megkezdésére, mindezek ellenére elindultak a katonai műveletek. A támadást követően szerbiai hackerek támadták meg

4 *World Drug Report 2011*. UNODC, New York, 2011. (2012. 10. 01.)
5 Clayton, Marc: i. m.
6 Healey, Jason – Bochoven, Leendert van: *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*. Atlantic Council, Issue Brief, 2012. 02.

a NATO weboldalait – a folyamatos DDoS-támadások[7] következtében több alkalommal hosszú időre elérhetetlenné is vált a szövetség honlapja. A támadásokért felelős Fekete Kéz elnevezésű szerb hackercsoport mindezek mellett több kormányzati oldalra elhelyezte politikai üzeneteit, és több alkalommal megpróbáltak betörni a NATO parancsnoki szervereibe – nagyrészt sikertelenül. Bár a légierő számítógépes hálózatába sikeresen bejutottak, titkos információkhoz nem férték hozzá. A Belgrádban található kínai nagykövetség bombázásának hatására kínai, majd később orosz hackerek is csatlakoztak, akik szintén túlterheléses támadásokkal és deface-technikával szabotálták mind a NATO, mind pedig az amerikai nagykövetségek honlapjait. A From Russia With Love elnevezésű orosz hackercsoport volt a zászlóshajója a NATO elleni támadásoknak, statisztikák szerint legalább 14 katonai és állami weboldalt törtek fel szerb hackerekkel együtt az 1999-es balkáni háború alatt.

Nagyrészt a koszovói beavatkozást követő kiberincidensek segítették hozzá a döntéshozókat ahhoz, hogy felismerjék a kibernetikai biztonság fontosságát, aminek eredményeképpen a 2002-es prágai csúcstalálkozón elfogadott robosztus képességfejlesztési csomag részeként elindították a NATO kibervédelmi programját is, amelynek részét képezte a kibervédelmi reagáló képesség *(NATO Computer Incident Response Capability)* kialakítása is. A képesség célja az volt, hogy a mögötte álló technikai központ érzékelje a NATO rendszereibe történő behatolásokat. Ezzel kezdetét vette az Észak-atlanti Szerződés Szervezetének felkészülése a 21. század egyik leghangsúlyosabb biztonsági kérdésének kezelésére.

Két fontos lecke

Kétségtelen, hogy a legnagyobb hatást a 2007-es Észtország elleni kibertámadás-sorozat gyakorolta a NATO kibervédelmi politikájára. Az észt fővárosban, Tallinnban található szovjet második világháborús emlékmű eltávolítása miatt zavargások törtek ki, és összecsapások történtek a helyi orosz kisebbség és a rendőri erők között. Az orosz diplomácia tiltakozását is kiváltó lépés hatására a kibertámadások már másnap este elindultak. A 2007. április 27. és május 27. között végrehajtott támadások az ország teljes infrastruktúráját érintették. Az információs technológiai fejlettség szempontjából élvonalba tartozó Észtország legfontosabb bankjait, illetve kormányzati rendszereit támadták, amelynek következtében sok esetben elérhetetlenné vált az elektronikus ügyintézés számtalan formája. A támadók huzamosabb időre ellehetetlenítették a pénzfelvételt, illetve blokkolták a legnagyobb hírportálokat. Az akciók szofisztikált mivolta egyértelmű kormányzati támogatást feltételezett, amit az orosz fél a mai napig tagad. A támadássorozat elsőként mu-

7 A Distributed Denial of Service (DDoS), magyarul az elosztott szolgáltatásmegtagadással járó támadás lényege, hogy a támadás nem egy pontból, hanem több számítógépet használva nagyobb erővel történik, és ezáltal komolyabban terheli a célpont rendszerét. A DDoS-támadásokat botnetek segítségével hajtják végre. A botnetnek, magyarul zombihálózatnak nevezett virtuális számítógép-hálózat lényege, hogy a behatoló által megfertőzött számítógépek erőforrásait egy központi vezérlő számítógép irányítása alá rendelik, ami parancsokkal irányítja a megfertőzött gépeket, a „zombikat". Rendszerint trójai programmal vagy egyéb vírussal veszik át az irányítást a célpont felett, mindezt természetesen a felhasználó tudta nélkül. A zombihálózatok segítségével a támadó képes megsokszorozni erejét, pontosan ezért alkalmas DDoS-támadások végrehajtására vagy éppen nagy mennyiségű kéretlen üzenet (spam) küldésére.

tatta meg, hogy élesben hogyan nézhet ki a kiberháború, és kétségtelen, hogy számtalan politikai és katonai vezetőt elgondolkodtatott.

Az egy évvel később lezajlott orosz–grúz konfliktus szintén rávilágított az információs műveletek és a kiberhadviselés erősödő szerepére. Az ötnapos háború során elsőként alkalmaztak a fizikai térben zajló katonai műveletekkel összhangban kifinomult kibertéri műveleteket. Az elsődleges célpontok a kormányzati weboldalak, a kritikus infrastruktúrák és a bankrendszer voltak. A folyamatos túlterheléses támadásokkal a legfontosabb hírportálokat tulajdonképpen „kiberblokád" alá vonták a támadók. A támadások összehangoltsága, feltételezett magas szintű technikai háttere, kidolgozottsága és intenzitása mind szintén arra utaltak, hogy állami akcióról van szó. Az orosz fél itt is következetesen tagadta, hogy bármi köze lenne a támadásokhoz, annak ellenére, hogy számos alkalommal visszavezették a behatolásokat Oroszországig, továbbá külön orosz internetes fórumokat üzemeltettek a háború alatt, ahol megjelölték a grúz célpontokat. Magyarán a hadsereg hackerei és a lakosság soraiból kikerülő támadók összehangolásáról volt szó.

A kezdeti lépések

Már a NATO védelmi minisztereinek 2007. június 14-i brüsszeli találkozóján megfogalmazódott az igény, hogy egységesíteni kellene a tagállamok kibervédelmi törekvéseit. Ennek eredményeként 2008 januárjában a NATO elfogadta új *Kibervédelmi irányelvét*,[8] a folyamat továbbvitelét pedig később a bukaresti csúcstalálkozón az állam- és kormányfők is támogatták. Az új fenyegetések meghatározása és a hozzájuk kapcsolódó feladatszabás mellett deklarálták a NATO informatikai rendszerek megerősítésének szándékát, és az államok jövőbeni együttműködését elősegítő lépéseket sürgettek. A NATO történetében első alkalommal foglalták hivatalos keretbe az informatikai biztonság kérdését:

„A NATO továbbra is elkötelezett, hogy megerősítse a szövetség kulcsfontosságú információs rendszereit a kibertámadásokkal szemben. Nemrég elfogadtunk egy Kibervédelmi irányelvet, és továbbra is fejlesztjük az ezt megvalósító szervezeteket és hatóságokat. A Kibervédelmi irányelv hangsúlyozza, hogy a NATO-nak és a tagállamoknak is meg kell védeniük kulcsfontosságú informatikai rendszereiket saját felelősségi körükben; meg kell osztaniuk a bevált gyakorlati megoldásokat, és biztosítaniuk kell azokat a képességeket, amelyekkel az erre vonatkozó felkérést követően egy szövetséges állam segítségére siethetnek egy kibertámadás elhárítására. Bízunk benne, hogy folytatódik a szövetség kibervédelmi képességeinek fejlesztése és a kapcsolatok erősítése a NATO és a nemzeti hatóságok között." (A NATO bukaresti csúcstalálkozójának Zárónyilatkozata, 47. pont.[9])

E lépésekkel összhangban hozták létre 2008 májusában a NATO Kooperatív Kibervédelmi Kiválósági Központját *(Cooperative Cyber Defence Centre of Excellence)*. Jelzésértékkel bír, hogy a Központ Tallinnban, Észtország fővárosában jött létre. A szervezet illeszkedik a szövetség további 15 kiválósági központjának sorába, amelyek a Szövetséges Transzformációs Parancsnokság *(Allied Command Transformation)* alárendeltségében működnek, funkcionálisan azonos céllal: az adott terület szakértőit támogatják, és

8 Lásd például: *Cyber security*. NATO, 2013. 02. 11. (2012. 10. 01.)

9 *Bucharest Summit Declaration*. NATO, 2008. 04. 03. (2012. 10. 01.)

a NATO tagállamainak az adott kérdéssel kapcsolatos képességeit fejlesztik. Mindazonáltal az intézmény nem képezi a NATO parancsnoki struktúrájának részét, csupán a katonai szervezetnek része, finanszírozását pedig azok a „szponzorországok" biztosítják, amelyek részt vesznek a központ munkájában. A szponzorországok Észtország, Németország, Olaszország, Litvánia, Lettország, Szlovákia és Spanyolország mint alapítók, míg 2010-ben Magyarország, 2011 novemberében pedig az Amerikai Egyesült Államok és Lengyelország csatlakozott hozzájuk. Törökország még 2008-ban jelentette be igényét a csatlakozásról, egyelőre azonban még nem vált teljes jogú taggá.

Az így több ország együttműködésének eredményeképpen létrejövő központ feladatai közé tartozik többek között a tagállami kiberképességek kialakításának elősegítése; tagállami doktrínák, koncepciók és stratégiák kidolgozásának támogatása; az információbiztonság oktatása, folyamatos képzések és gyakorlatok lebonyolítása; valamint a kibernetikai védelem és a kiberhadviselés jogi vonatkozásainak elemzése, a nemzetközi jogi keretek kialakításához szükséges lépések végrehajtása. A szervezet tehát nem a NATO kibernetikai támadóerejét jeleníti meg, hanem mint kutatási és oktatási központ kíván működni.

A központ mellett a NATO létrehozta a kibervédelmi problémákkal foglalkozó hatóságot *(Cyber Defence Management Authority)* is, ami az illetékes tanácsnak *(Cyber Defence Management Board)* alárendelve végzi feladatát. A brüsszeli székhelyű szervezet feladata a szövetségi szintű centralizált kibervédelem irányításának megteremtése, a NATO-t és a tagállamokat érő támadásokra való reagálás, valamint tagállami szintű segítségnyújtás a nemzeti kibervédelem kialakításában. Ehhez kapcsolódva a már említett kibervédelmi reagáló képesség technikai központjának *(NATO Computer Incident Response Capability Technical Centre)* alárendelve alakították ki az úgynevezett Gyorsreagálású Csapatot *(Rapid Reaction Team),* amely sok esetben nemzeti szinten nyújt segítséget a támadások ellen, gyorsan települve a megtámadott országban. Alkalmazásáról a kibervédelmi tanács szintjén döntenek. A képesség állandó magját 6 szakértő adja, akiket a fellépő problémához mérten egészítenek ki további nemzeti, illetve NATO-szakemberekkel, akik minden szükséges felszereléssel – telekommunikációs készülékek (például műholdas telefonok), digitális nyomrögzítésre alkalmas eszközök stb. – rendelkeznek. A csapat 2012 végére éri el a teljes műveleti képességét.[10]

A hatóság mellett kialakításra kerültek nemzeti szinten a *Computer Emergency Response Teamek*, azaz a CERT-ek. A CERT-koncepció 1988-ban jelent meg – függetlenül a NATO-tól – a Carnegie Mellon Egyetemen, az Egyesült Államokban, azzal a céllal, hogy olyan szakértői csoportot hoznak létre, amelynek feladata a nemzeti hálózatok felügyelete és adott esetben a védelme, lehetőleg minél gyorsabban reagálva a bekövetkezett támadásokra (valós idejű védelem). Manapság több mint 250 ilyen CERT létezik – többek között Magyarországon is –, és bevett gyakorlattá vált, hogy az államok pénzügyi támogatásával ezek a csoportok látják el a nemzeti kibervédelmi felügyeletet. A bukaresti csúcstalálkozó után a védelmi miniszterek támogatták azt az ötletet, hogy minden tagállam alapítsa meg a saját reagáló csapatát, ezzel is erősítve a NATO Kibervédelmi Hatóságának munkáját.

10 Lásd: *NATO Rapid Reaction Team to fight cyber attack.* NATO, 2012. 03. 13. (2012. 10. 01.)

Célkeresztben a NATO

A koszovói beavatkozás óta számtalan alkalommal támadták a NATO hálózatait. Az alapvetően magányos hackerekhez köthető támadásokon túl – sok esetben előre bejelentett módon – nagyobb hackercsoportok is megpróbáltak szabotálni egyes weboldalakat, szervereket. Miután 2011-ben a NATO egyre nagyobb veszélyt, illetve nemzetbiztonsági kockázatot jelentő csoportosulásnak nevezte az Anonymous hackercsoportot, a hackerek több szövetségi weboldal ellen is túlterheléses támadást indítottak. Állításuk szerint a líbiai hadművelet alatt több NATO-szervert is feltörtek, amelyekről nagy mennyiségű adatot töltöttek le. Bár hivatalosan nem erősítették meg a behatolást, a különböző fórumokon közétett adatok alapján valószínűsíthető, hogy valóban sikerrel jártak a „hacktivisták". A LulzSec hackercsoport szintén kivette a részét a támadásokból: a NATO online könyvtárának felhasználó-adatbázisát feltörve 12 000 felhasználónevet és jelszót hoztak nyilvánosságra.

E lépésekkel párhuzamosan indult útjára a Szövetséges Transzformációs Parancsnokság felügyeletével az úgynevezett globális közös terek *(Global Commons)* projekt, amely azokkal a földrajzi és virtuális dimenziókkal foglalkozik, amelyek egyetlen országhoz sem köthetőek, azonban fontos szerepet játszanak a nemzetközi közösség, így a NATO biztonságában: ilyen a légtér, a világűr, a tengerek és óceánok, valamint maga a kibertér is. E dimenziók közül a kibertér a legösszetettebb, tekintve, hogy alapvetően virtuális összetevőkből áll, azonban a fizikai eszközök jelenléte, birtoklása is elengedhetetlen a sikeres információs műveletek végrehajtásához – pontosan ez az összetettség az, ami a kibertér sebezhetőségét adja.

Aktualizált válaszok a változó kihívásokra

Következő lépésként a 2010. novemberi lisszaboni csúcstalálkozón a tagállamok elfogadták a NATO új Stratégiai Koncepcióját, amelyben az új típusú kihívások között a kiberbiztonság kérdése is helyet kapott: „A kibertámadások egyre gyakoribbá, szervezettebbé és a kormányok, vállalkozások, gazdaságok és potenciálisan a közlekedési és ellátási hálózatok, valamint más kritikus infrastruktúrák számára is egyre nagyobb károkat okozóvá válnak. Elérhetik azt a küszöböt, ami már a nemzeti és euro-atlanti prosperitást, biztonságot és stabilitást veszélyezteti. Külföldi haderők és titkosszolgálatok, szervezett bűnözők, terrorista és/vagy szélsőséges csoportok egyaránt lehetnek egy ilyen támadás végrehajtói." (A NATO Stratégiai Koncepciója, 2010, 12. pont)[11]

A Stratégiai Koncepcióhoz igazodva a tagállamok védelmi miniszterei 2011. június 8–9-i brüsszeli találkozójukon frissítették a Kibervédelmi irányelvet. Az új irányelv mellé elfogadtak egy, az elméletet gyakorlatba átültető akciótervet is. Az ehhez kapcsolódó konkrét elképzelések és eszközök tára nem nyilvános, azonban bizonyos pontokat a sajtó számára is nyilvánossá tettek:

- a tagállamok vezetői felismerték, hogy a kibervédelem elengedhetetlen a NATO kollektív védelme és a válságkezelés érdekében;
- a megelőzés, a rugalmasság és az informatikai eszközök védelme kiemelten fontos a NATO-tagállamok számára;
- cél a kibervédelmi képességek kialakítása és a NATO saját hálózatainak megóvása központosított védelemmel;

11 Berzsenyi Dániel et al. (szerk.): *Aktív Szerepvállalás, Modern Védelem - Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságáról.* biztonságpolitika.hu, 2010.

– segíteni kell a tagállamokat, hogy elérjék a kibervédelem minimális szintjét, ezzel csökkentve a nemzeti kritikus infrastruktúrák sebezhetőségét;
– együtt kell működni más partnerekkel, nemzetközi szervezetekkel, a magánszektorral és a tudomány képviselőivel.

Az új politikával a kibernetikai védelem kérdése integrált részévé vált a NATO védelmi tervezési folyamatának is, és szervezeti változások is történtek e téren. A döntéshozó-irányító és végrehajtó szervek tekintetében a legfontosabb politikai döntéshozó szerv – mint minden más kérdésben, így a kibervédelem kérdésében is – az Észak-atlanti Tanács *(North Atlantic Council)* maradt. A Tanács elé a Védelempolitikai és Tervezési Bizottság *(Defence Policy and Planning Committee)* terjeszti be a védelmi kérdésekkel kapcsolatos javaslatokat. A kibervédelem technikai és végrehajtási aspektusaival, illetve a tagállamok és a NATO-műveletek technikai támogatásával kapcsolatban a felelős szerv a NATO Tanácsadó, Vezetési és Irányítási Ügynökség *(NATO Consultation, Command and Control Agency – NC3A)* lett, amely a NATO Tanácsadó, Vezetési és Irányítási Tanácsának *(Consultation, Command and Control Board – NC3B)* köteles beszámolni. Az ügynökség 1996-ban jött létre a SHAPE Technikai Központ *(SHAPE Technical Centre),* illetve a NATO Híradástechnikai és Információrendszerek Ügynökség *(NATO Communications and Information Systems Agency)* összevonásával.[12]

Kibertámadások és a washingtoni szerződés 5. cikkelye

A kibertámadások tisztázatlan elkövetői háttere, problémás visszakövethetősége és a nemzetközi szabályozás hiánya következtében meghatározó kérdés, hogy egyes támadástípusok milyen elbírálás alá esnek, majd milyen választ váltanak ki mind politikai, mind katonai téren. Az új irányelv szerint egy esetleges kibertámadás alapvetően politikai támadásnak minősül, azaz nem esik az 5. cikkely rendelkezése alá, és ennek értelmében a válasz is politikai kell, hogy legyen. Egy ilyen támadás után a NATO és a tagállamok vezetői döntenek, nem pedig a reagáló erők parancsnokai. Magyarán a NATO megtartja rugalmasságát az ügyben, hogy hogyan kezel egy kibertámadási komponenst is tartalmazó válságot.

A NATO 2011. december 13–15. között megrendezett kibervédelmi gyakorlatán a szövetségi és tagállami informatikai hálózatok ellen irányuló nagyarányú kibertámadást és a védekezést modellezték. A Cyber Coalition 2011 gyakorlaton a szövetség központi szervezeteinek tagjai mellett 23 NATO-tagállam és hat partnerország közel kétszáz képviselője részvételével, az Európai Unió megfigyelőinek jelenlétében tesztelték és gyakorolták az újonnan kialakított technikai megoldásokat és nemrég érvénybe léptetett eljárásokat.

Bár tagadhatatlan, hogy a nemzetközi jog, a fegyveres konfliktusok joga és az 5. cikkely kapcsolata a kibernetikai támadásokkal igencsak homályos. A kiberbűncselekmények, illetve a kibertámadások jogi elbírálása és kereteinek kialakítása jelenleg is folyamatban van. A NATO komoly erőfeszítéseket tesz ezzel kapcsolatban, a szakértők pedig nagy várakozással tekintenek a Kooperatív Kibervédelmi Kiválósági Központ által kidolgozás alatt álló *A kiberhadviselés nemzetközi jogának kézikönyve (Manual on International Law Applicable to Cyber Warfare)* című, 2013 tavaszán megjelenő dokumentumra, amely jelentős segítséget nyújthat az ilyen irányú kérdésekben való eligazodásnál.

12 *Defending the networks – The NATO Policy on Cyber Defense.* NATO, 2011. (2011. 10. 01.)

Merre tovább?

Az új kibervédelmi irányelv alapvetően a védekezésre helyezi a hangsúlyt. Ugyanakkor élénk vita folyik arról, hogy érdemes és időszerű lenne komolyabb módon feltérképezni az ellencsapások lehetőségét, illetve kialakítani egy mérvadó támadóképességet is. Az amerikai stratégiák már létező hadszíntérként kezelik a kiberteret, és megjelenítik a támadóerő kialakításának igényét, ezért fontosnak tartják a kijelölt erők célirányos kiképzését is. Hivatalosan a NATO nem rendelkezik offenzív kiberképességekkel, pontosan ezért okozott meglepetést, amikor kiderült, hogy a líbiai beavatkozással kapcsolatban több katonai vezető is támogatott volna egy előzetes kibernetikai csapást. Bár valószínű, hogy a később elvetett tervet elsősorban az amerikai erők hajtották volna végre, kétségtelen, hogy jó lehetőség lett volna, hogy a NATO is kipróbálja magát ezen a téren. Végül azonban nem került sor offenzív kibernetikai lépésre, feltehetően azért sem, mert a bombázás előestéjén, illetve a hadművelet kezdeti szakaszában a szövetségnek is több támadást el kellett szenvednie különböző független nemzetközi hackercsoportoktól.

Mindenesetre az előremutató, hogy a központi kibervédelem kialakítása, pontosabban a szövetségi szintű informatikai rendszerek, hálózatok és infrastruktúrák védelmének biztosítása mellett párhuzamosan megjelenik a törekvés arra, hogy a tagállamok önállóan is képesek legyenek a saját nemzeti kibernetikai biztonságuk szavatolására. Emellett nem lehet eléggé hangsúlyozni a nem állami szereplőkkel történő együttműködés fontosságát. Ahogyan az az új irányelvben is megjelent, a különböző kutatóműhelyektől kezdve az egyetemeken át a védelmi iparig a NATO-nak megfelelő figyelmet kell fordítania e területek képviselőire, tekintve, hogy számos, a nem katonai vagy állami szférához köthető szereplő is komoly segítséget nyújthat mind tagállami, mind szövetségi szinten. Jól mutatja ezt a nyitást az is, hogy 2012 márciusában 58 millió eurót szavaztak meg a döntéshozók, hogy a NATO Tanácsadó, Vezetési és Irányítási Ügynökség koordinálásával a civil szférából szerződjenek információvédelmi cégekkel, fejlesztőkkel arra, hogy fokozzák a szövetség hálózatainak biztonságát, illetve modernizálják a már meglévő infrastruktúrát.

Fontos partner lehet a jövőben az Európai Unió is, tekintve, hogy a két szervezet tagsága, ebből kiindulva az infrastruktúrák is sok esetben fedik egymást, így azok védelme mindkét szervezet közös érdeke kell hogy legyen. Ebben az együttműködésben elsődleges partner az Európai Hálózat- és Információbiztonsági Ügynökség *(European Network and Information Security Agency – ENISA)*. Az ügynökség elsődleges feladata – hasonlóan a Kooperatív Kibervédelmi Kiválósági Központhoz – a tanácsadás, az oktatás és az együttműködés elősegítése a hálózat- és információbiztonság területén. Azon felül, hogy monitorozza az unió közös hálózatait és tájékoztatja a Bizottságot az esetleg fenyegetésekről, a tagállamokkal is szoros kapcsolatban áll. Magyarország esetében a Nemzeti Hálózatbiztonsági Központ *(PTA CERT-Hungary)* tölti be az úgynevezett Nemzeti Kapcsolati Pont szerepét. Az ügynökség tehát szintén nem operatív munkát végez, azonban létezése elengedhetetlen a hatékony koordináció érdekében. Az elmúlt időszakban aktív párbeszéd indult az EU és a Kooperatív Kibervédelmi Kiválósági Központ között is, és tekintettel a probléma akut jellegére, várhatóan a chicagói NATO-csúcstalálkozót követően is bővülni és mélyülni fog a nemzetközi együttműködés.