Paráda István hadnagy:

# A NATO KIBERVÉDELMI IRÁNYELVEINEK FEJLŐDÉSE

ÖSSZEFOGLALÓ: *A folyamatos technológiai fejlődésnek köszönhetően, valamint az újabb biztonsági kihívások és fenyegetések megjelenésével a kiberműveletek a katonai tevékenységek mindennapi részévé váltak. E képességek létjogosultságát és folyamatosan növekvő tendenciáit a NATO, az Európai Unió, az Amerikai Egyesült Államok és Magyarország is felismerte. Hazánk, a Nemzeti Közszolgálati Egyetem (mint felsőoktatási szereplő) és a Magyar Honvédség is jelentős kihívásokkal áll szemben a kiberhadviselésen és a kiberműveleteken belüli képességek fejlesztése, létrehozatala és alkalmazása terén.*

*Bár a NATO mindig is védte kommunikációs és információs rendszereit, a 2002-es prágai csúcstalálkozó vette először napirendre a kibervédelmet. A szövetséges vezetők 2006-ban a rigai csúcstalálkozón felismerték, hogy további védelmet kell biztosítani ezeknek az információs rendszereknek. Az Észtország állami és magánintézményei ellen 2007-ben végrehajtott kibertámadások nyomán a szövetséges védelmi miniszterek ugyanennek az évnek júniusában megállapodtak abban, hogy e területen jelentős munkára van szükség. Ennek eredményeként a NATO 2008 januárjában első alkalommal jóváhagyta a Szövetség kibervédelmi irányelveit. Jelen írás a NATO kibervédelemmel kapcsolatos irányelveit és törekvéseit mutatja be.*

KULCSSZAVAK: *kibervédelem, kiberbiztonság, kiberműveletek, NATO, irányelv*

## BEVEZETÉS

Napjainkban természetes dolog az információs és az infokommunikációs technológia használata. Mindennapi életünk szinte valamennyi szegmensére kihat a pénzügyi tranzakcióktól kezdődően a munkahelyi kötelezettségeinken keresztül az egyszerű szórakozási és pihenési tevékenységeinkkel bezárólag. Természetesen sorolni lehetne a különböző felhasználási lehetőségeket, viszont ha a katonai szegmensre koncentrálunk, akkor világossá válik, hogy az informatikai, távközlési és elektronikai technológia rohamos fejlődése kikerülhetetlenül elérte a hadtudomány területét is. E fejlődés és ennek nyomán a kiberműveletek megjelenése kihatással van a politikai és a gazdasági szektorra, valamint a fegyveres erőkre is.[1] Magyarország NATO-tagállamként betartja és teljesíti a Szövetség alapokmányában foglaltakat.

A kiberirányelvekkel kapcsolatos folyamatok bemutatása előtt fontos rögzíteni a kiberbiztonság definícióját. A kiberbiztonság meghatározása – hivatkozva a Nemzetközi Távközlési Egyesület ITU-T X.1205 jelzésű dokumentumára – a következő.

*„A kiberbiztonság az eszközök, a politikák, a biztonsági koncepciók, a biztonsági garanciák, az iránymutatások, a kockázatkezelési megközelítések, a cselekvések, a képzés,*

[1] Jobbágy Szabolcs: Az információs társadalom, az informatika és a távközlés konvergenciája. Múlt, jelen, jövő. Hadmérnök IV. évfolyam 1. szám, 2009. március, 185–188. http://www.hadmernok.hu/2009_1_jobbagy.pdf (Letöltés időpontja: 2017. 12. 09.)

*a legjobb gyakorlatok, a biztosítékok és a technológiák gyűjteményét jelenti, amelyek a kiberkörnyezet, a szervezet és a felhasználói eszközök védelmére használhatók. A szervezet és a felhasználói eszközök közé tartoznak a számítástechnikai eszközök, a személyzet, az infrastruktúra, az alkalmazások, a szolgáltatások, a telekommunikációs rendszerek, valamint a továbbított és/vagy tárolt információk összessége a kiberkörnyezetben. A kiberbiztonság célja a szervezet és a felhasználók eszközei biztonsági tulajdonságainak elérése és fenntartása a kiberkörnyezetben meglévő biztonsági kockázatokkal szemben."*[2]

## A KIBERVÉDELEM MEGJELENÉSE A NATO-BAN

A NATO 2007 óta kiemelten kezeli a kibervédelem és kiberhadviselés kérdéskörét. Számos adat van a 2007-ben Észtország ellen indított kiberműveletekről, amikor meghatározó jelentőségű szolgáltatásmegtagadást (Denial of Service – DOS) kiváltó támadássorozat történt.

2007 áprilisában Tallinnban egy második világháborús szovjet emlékmű eltávolítását az észtországi orosz lakosság nagy felháborodással fogadta. Ezzel egy időben internetes támadások érték az észt informatikai és távközlési infrastruktúrát, főként az országon kívülről. A valószínűsíthető orosz támadások az Észtország és Oroszország közötti nézeteltéréseknek tulajdoníthatók. Az incidens a hadviselés teljesen új formáira irányította a figyelmet.

Az orosz fél kereskedelmi bojkott bevezetésével fenyegetett, mérsékelte a diplomáciai kapcsolatokat, valamint kibertámadásokat is végrehajtott. Ez utóbbiak célpontjai bankok, közintézmények voltak; a támadások az ország pénzügyi és infokommunikációs hálózatának megbénítását eredményezték: az online pénzügyi tranzakciókban fennakadások keletkeztek, a közigazgatás weblapjai, valamint az adatforgalmat irányító és kezelő közigazgatáshoz tartozó hálózati és kiszolgáló szervereszközök elérhetetlenné, működésképtelenné váltak. Voltak olyan állami intézmények, amelyeket el kellett szigetelni a hálózattól. A támadássorozat – javarészt órás vagy akár többórás DOS jellegű támadások formájában[3] – mintegy két hétig tartott. Az esemény jelzésértékű példa arra, hogy az infokommunikácó milyen fontos szerepet játszik a társadalomban.[4, 5]

## A NATO KIBERVÉDELMI IRÁNYELVEINEK KRONOLÓGIÁJA

Az eseménysorozat egyértelművé tette, hogy a NATO-nak az új kihívásokra reagálnia kell, és fel kell ismernie a megfelelő képességek fejlesztésének szükségességét. Különösképpen

---

[2] ITU-T X.1205 telecommunication standardization sector of ITU (04/2008) series x: data networks, open system communications and security telecommunication security overview of cybersecurity. 8. https://www.itu.int/rec/T-REC-X.1205-200804-I (Letöltés időpontja: 2017. 12. 09.)

[3] Kovács László: Az e-közszolgálatfejlesztés nemzetbiztonsági és hadtudományi kérdései. Nemeslaki András (szerk.): E-közszolgálat fejlesztés: Elméleti alapok és tudományos kutatási módszerek. Nemzeti Közszolgálati Egyetem, Budapest, 2014, 235–236. http://real.mtak.hu/33733/1/E_kozszolgfejlesztes-nemeslaki.pdf (Letöltés időpontja: 2017. 12. 09.)

[4] Bányász Péter – Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. Hadtudomány XXIII. évfolyam 1. elektronikus szám, 2013. június, 191. http://mhtt.eu/hadtudomany/2013/2013_elektronikus/2013_e_Banyasz_Peter_Orbok_Akos.pdf (Letöltés időpontja: 2017. 12. 09.)

[5] Gyányi Sándor: Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem. Doktori (PhD-) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Kar Katonai Műszaki Doktori Iskola, Budapest, 2011, 30–31. http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2012/gyanyi_sandor.pdf (Letöltés időpontja: 2017. 12. 09.)

azért is, mert – az Észak-atlanti Szerződés Szervezete megalakulásakor Washingtonban 1949. április 4-én aláírt Alapokmány 5. cikke, azaz a kollektív védelem értelmében – egy NATO-tagországot ért támadás a szervezet elleni támadásnak tekintendő.

A NATO Alapokmány 5. cikkelye így szól: *„A Felek megegyeznek abban, hogy egyikük vagy többjük ellen, Európában vagy Észak-Amerikában intézett fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek; és ennélfogva megegyeznek abban, hogy ha ilyen támadás bekövetkezik, mindegyikük az Egyesült Nemzetek Alapokmányának 51. cikke által elismert jogos egyéni vagy kollektív védelem jogát gyakorolva támogatni fogja az ekként megtámadott Felet vagy Feleket azzal, hogy egyénileg és a többi Féllel egyetértésben azonnal megteszi azokat az intézkedéseket – ideértve a fegyveres erő alkalmazását is – amelyeket a békének és biztonságnak az észak-atlanti térségben való helyreállítása és fenntartása érdekében szükségesnek tart.”*[6]

Az észt informatikai és távközlési infrastruktúra megbénítását eredményező támadást felismerve a NATO szükségszerűnek látta kiberbiztonsággal és kiberműveletekkel kapcsolatos intézkedések bevezetését.

A Szövetség 2008-ban megalapította a Kooperatív Kibervédelmi Kiválósági Központot (Cooperative Cyber Defence Centre of Excellence – CCDCOE). Az intézmény a kiberműveletek és a kiberbiztonság oktatásával, kutatásával és fejlesztésével foglalkozik, és a műszaki-technológiai aspektusokon kívül vizsgálja az etikai és a jogi kérdésköröket is. Ezenfelül nagyban közreműködik a kibervédelmi stratégiák létrehozásában és fejlesztésében. A CCDCOE alapításának koncepcióját a szövetséges erők transzformációs főparancsnoka 2006-ban hagyta jóvá. A szponzornemzetek tárgyalásai 2007-ben kezdődtek, az egyetértési megállapodást 2008-ban írták alá. Az alapító tagokon kívül folyamatosan csatlakoznak a NATO-tagállamok közül a szponzornemzetek, köztük Magyarország 2010-ben.[7]

A 2007-es események következményeként a nyilatkozatokban is egyre nagyobb hangsúlyt kaptak a kiberbiztonságról, kiberműveletekről alkotott elképzelések. A 2008-as bukaresti csúcstalálkozó nyilatkozata alapján:

*„(47) A NATO továbbra is elkötelezett a kulcsfontosságú szövetségi információs rendszerek kibertámadásokkal szembeni megerősítésében. Elfogadásra került egy Kibervédelmi Irányelv, valamint a struktúra és a hatóság fejlesztése annak végrehajtása érdekében. A kibervédelmi politika hangsúlyozza, hogy a NATO-nak és a nemzeteknek meg kell védeniük a kulcsfontosságú információs rendszereiket a saját felelősségüknek megfelelően. Megosztani a legjobb gyakorlatokat és a segítségnyújtás képességét a szövetséges nemzetekkel a kibertámadások elleni küzdelemben. Bízunk benne, hogy folytatjuk a NATO kibervédelmi képességeinek fejlesztését és megerősítjük a NATO és a nemzeti hatóságok közötti kapcsolatokat.”*[8]

---

[6] Az Észak-atlanti Szerződés, Washington DC, 1949. április 4., 1. 5. Cikk https://www.nato.int/cps/ic/natohq/official_texts_17120.htm?Selectedlocale=hu (Letöltés időpontja: 2017. 12. 09.)

[7] Kovács László – Szentgáli Gergely: National Cyber Security Organization: Hungary. 11. Tallinn, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_HUNGARY_2015-10-12.pdf (Letöltés időpontja: 2017. 12. 09.)

[8] Bucharest Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008. https://www.nato.int/cps/en/natolive/official_texts_8443.htm (Letöltés időpontja: 2018. 02. 21.)

A 2009-es strasbourgi nyilatkozatban már látható a szervezet infokommunikációs rendszerektől való komoly függése, ami természetesen globális szinten minden nagyobb szervezetet érint. Megjelentek az utalások a támadások forrásai beazonosításának nehézségeire. Ezenfelül kitértek a képességek javítására és aktiválására az adott területen.[9, 10]

A lisszaboni csúcstalálkozón 2010-ben elfogadtak egy új stratégiai koncepciót, amelyben az Észak-atlanti Tanácsnak (North Atlantic Council – NAC) feladata volt egy alapos, új NATO kibervédelmi politika kidolgozása és egy végrehajtási terv elkészítése. Az *Aktív szerepvállalás, modern védelem. Az Észak-atlanti Szerződés Szervezetének stratégiai koncepciója tagállamainak védelméről és biztonságáról* című dokumentumból 2010-ben jelentős horderejű intézkedések kerültek napvilágra. Az Alapokmány 5. cikke értelmében a fegyveres támadások kibővítésre kerülnek a kollektív védelem vonatkozásában.[11]

*„4. a. Kollektív védelem. A NATO-tagállamok mindig segítséget nyújtanak egymásnak egy esetleges támadással szemben a Washingtoni Szerződés V. cikkelyével összhangban. Ez az elkötelezettség szilárd és kötelező erejű marad. A NATO elrettent és megvéd minden agresszióval való fenyegetéssel és felmerülő biztonsági kihívással szemben, amelyek az egyes szövetségesek vagy a Szövetség egészének alapvető biztonságát fenyegetik."*[12]

A lisszaboni csúcstalálkozó nyilatkozata az előzőekhez képest részletesebb információkat tartalmazott a kiberbiztonság kérdéskörével kapcsolatban. Megjelent a kibertér fogalma és fontossá vált a kibervédelem a konfliktusok kezelésében. Jelentős szerepet kapott a képességek elérésének felgyorsítása, valamint a tervezési folyamatok szükségessége a szövetségesek segítésére. Továbbá kihangsúlyozottan ügyeltek az információmegosztás, illetve a más szervezetekkel való együttműködés lehetőségére.[13]

A NATO-tagállamok védelmi miniszterei 2011 júniusában jóváhagyták a kibervédelemről szóló újabb, immár második politikai állásfoglalást, valamint az ehhez kapcsolódó cselekvési tervet, amely a gyorsan változó fenyegetésekkel és technológiai környezetekkel kapcsolatos összehangolt erőfeszítéseket rögzítette. A lisszaboni csúcson meghatározott irányelvek és a stratégiai koncepció betartását, megvalósítását és továbbfejlesztését tartalmazta a 2012-ben kiadott nyilatkozat, melyet a chicagói találkozón erősítettek meg. 2012 áprilisában elkezdődött a kibervédelem integrálása a NATO védelmi tervezési folyamatába. A védelmi tervezési folyamat során azonosították a releváns kibertérvédelmi követelményeket.

A 2012. májusi chicagói csúcstalálkozón a szövetségesek vezetői megerősítették elkötelezettségüket, hogy javítsák a Szövetség kibervédelmét oly módon, hogy valamennyi NATO-hálózatot központi védelem alá helyezték, és jelentős fejlesztéseket hajtottak végre a

[9] Tóth András: A prágai NATO-csúcstalálkozót követő határozatok, megállapodások a parancsnoki rendszer és a vezetési rendszer korszerűsítésére, valamint az együttes tevékenység képesség fejlesztésére. Hadmérnök XI. évfolyam 3. szám, 2016. szeptember, 216–217. http://hadmernok.hu/163_17_tothandras.pdf (Letöltés időpontja: 2017. 12. 09.)

[10] Strasbourg / Kehl Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl, 4 April 2009. https://www.nato.int/cps/en/natohq/news_52837.htm?mode=pressrelease (Letöltés időpontja: 2018. 02. 21.)

[11] Szentgáli Gergely: A NATO kibervédelmi politikájának fejlődése. Bolyai Szemle XXI. évf. 2. szám, 2012, 80–85. http://archiv.uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf (Letöltés időpontja: 2017. 12. 09.)

[12] Aktív szerepvállalás, modern védelem – a NATO új stratégiai koncepciója magyar nyelven. 2010. december 08. http://old.biztonsagpolitika.hu/?id=16&aid=965&title=aktiv-szerepvallalas-modern-vedelem-a-nato-uj-strategiai-koncepcioja-magyar-nyelven (Letöltés időpontja: 2017. 12. 09.)

[13] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon 19–20. November 2010. https://www.nato.int/cps/ua/natohq/official_texts_68580.htm (Letöltés időpontja: 2018. 02. 21.)

számítógépes incidenskezelő képesség (Computer Incident Response Capability – NCIRC) területén. A Lisszabon utáni kibervédelmi koncepció, politika és cselekvési terv elfogadásával elkezdődött annak megvalósítása is. Integrálták az újabb kibervédelmi intézkedéseket a Szövetség struktúráiba és eljárásaiba, és az egyes nemzetekre vonatkozóan továbbra is elkötelezettek maradtak a nemzeti szintű kibervédelmi képességek azonosításában és megvalósításában, amelyek erősítették a Szövetség együttműködését és interoperabilitását, beleértve a NATO védelmi tervezési folyamatait is. Elkötelezettek maradtak a kiberbiztonsági fenyegetések kezelésére a tekintetben, hogy eseti alapon a nemzetközi szervezetekkel, többek között az EU-val, az Európa Tanáccsal, az ENSZ-szel és az Európai Biztonsági és Együttműködési Szervezettel (EBESZ) konkrét együttműködés valósuljon meg.[14]

2014 februárjában a védelmi miniszterek feladatul szabták, hogy a Szövetség dolgozzon ki egy új, fokozott kiberbiztonsági politikát a kollektív védelem, a szövetségesek támogatása, az irányítás, a jogi megfontolások és az iparral való kapcsolatok tekintetében.[15]

2014 áprilisában a NAC megváltoztatta a Védelmi Politikai és Tervezési Bizottság/Kibervédelem elnevezését, és annak új neve Kibervédelmi Bizottság lett. 2014 májusában a NCIRC elérte teljes működőképességét, ami fokozott védelmet biztosított a NATO-hálózatok és -felhasználók számára. A szeptemberi walesi csúcstalálkozón a szövetségesek támogatták az új kibervédelmi politikát, és jóváhagytak egy új cselekvési tervet, amely a politikával együtt hozzájárul a Szövetség alapvető feladatainak teljesítéséhez. A politikát és végrehajtását a Szövetségen belül mind politikai, mind technikai szinten szoros felülvizsgálat alatt tartották, és a kiberfenyegetésnek megfelelően frissítették. 2014. szeptember 17-én a NATO ajánlást kezdeményezett a magánszektorral folytatott együttműködésre a kiberfenyegetésekkel és -kihívásokkal szemben. A walesi csúcstalálkozón elfogadott NATO Ipari Kiber-együttműködés (Industry Cyber Partnership – NICP) című dokumentumot egy kétnapos kiberkonferencián mutatták be a belgiumi Monsban a szövetségi vezetők, ahol 1500 ipari vezető és politikai döntéshozó gyűlt össze a kiber-együttműködés megvitatására. Az NICP felismerte az iparági partnerekkel való összefogás fontosságát annak érdekében, hogy a Szövetség elérhesse a kibervédelmi politika által kitűzött célokat.

A NATO és az EU 2016. február 10-én megkötötte a kibervédelemről szóló technikai megállapodást, miszerint mindkét szervezet megfelelő segítséget nyújt a kibertámadások megelőzéséhez és a reagáláshoz. Ez a technikai megállapodás az NCIRC és az EU számítógépes vészhelyzeti reagáló csoport (Computer Emergency Response Team – CERT-EU) között keretet biztosít az információcseréhez és a legjobb gyakorlatok megosztásához a válságkezelő csoportok között.

2016. június 14-én a védelmi miniszterek megállapodtak abban, hogy a varsói csúcstalálkozón dimenzióként ismerik el a kiberteret. Ez a Szövetség jelenlegi működési területeinek – levegő, víz, szárazföld és világűr – a kiegészítése egy újabbal. A kiberteret illetően számos meghatározással találkozhatunk, a sok közül egyet emelnék ki. Az Amerikai Egyesült Államok Védelmi Minisztériumának hivatalos szótára alapján a kibertér *„az információs környezetben az egymással kölcsönös függőségben lévő információs infrastruktúrák hálózata és a bennük lévő adatok által létrehozott globális tartomány, amely magában foglalja az*

[14] Chicago Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012. https://www.nato.int/cps/en/natohq/official_texts_87593.htm (Letöltés időpontja: 2018. 02. 21.)

[15] Szenes Zoltán: Új bor a régi palackban? A walesi NATO-csúcs. Hadtudomány 2014/3–4. szám, 3–6. http://mhtt.eu/hadtudomany/2014/3_4/2014_3_4_1.pdf (Letöltés időpontja: 2017. 12. 09.)

*internetet, a távközlési hálózatokat, a számítógépes rendszereket, valamint a beépített feldolgozó és vezérlő elemeket".*[16]

Ez a felismerés nem változtatja meg a NATO küldetését vagy mandátumát, amely védekező. Akárcsak a cselekvés minden területén, a NATO a nemzetközi joggal összhangban jár el. A Szövetség elismerte az egyéb nemzetközi fórumokon tett erőfeszítéseket is, melyek arra irányultak, hogy kidolgozzák a felelősségteljes állami magatartás normáit és a bizalomépítő intézkedéseket, és elősegítsék a nemzetközi közösség átláthatóbb és stabilabb kiberterének a létrehozását.

A 2016. júliusban rendezett varsói csúcstalálkozón a szövetséges állam- és kormányfők ismét megerősítették a NATO védekező megbízatását és a már elismert kiberteret a műveletek egyik területeként, amelyben a NATO-nak hatékonyan meg kell védenie magát, mint ahogyan azt teszi a többi négy dimenzióban. A szövetségesek is kötelezettséget vállaltak arra, hogy nemzeti hálózataik és infrastruktúráik kibervédelmét előtérbe helyezzék. Minden tagállam tiszteletben fogja tartani azt a felelősségét, hogy javítsa rugalmasságát, illetve gyors és hatékony reagálását a kibertámadásokra, beleértve a hibrid környezetet is. A NATO és az EU 2016. december 6-án több mint 40 olyan intézkedést fogadott el, amelyek elősegítik a két szervezet együttműködését, beleértve a hibrid fenyegetések elleni küzdelmet, a kibervédekezést és a közös szomszédságuk stabilabbá és biztonságosabbá tételét. A kibervédelem területén a NATO és az EU közös gyakorlatokat tart, elősegítik a kutatást, a képzést és az információk megosztását.

*„(70.) A kibertámadások egyértelműen kihívást jelentenek a Szövetség biztonsága szempontjából, és ugyanolyan károsak lehetnek a modern társadalmak számára, mint a hagyományos támadások. Walesben megállapodtunk abban, hogy a kibervédelem része a NATO kollektív védelmi feladatainak. Most Varsóban megerősítjük a NATO védelmi mandátumát, és elismerjük a kiberteret olyan műveleti területnek, amelyben a NATO-nak olyan hatékonyan kell megvédenie magát, mint a levegőben, a szárazföldön és a tengeren. Ez javítani fogja a NATO azon képességét, hogy ezeken a területeken védje és végezze műveleteit, és minden körülmények között megőrizze cselekvési és döntéshozatali szabadságát. Továbbá támogatja a NATO szélesebb körű elrettentését és védelmét: a kibervédelem továbbra is beépül a működési tervezésbe és a Szövetség műveleteibe és küldetéseibe, és együtt fogunk dolgozni, hogy hozzájáruljanak a sikerhez. Ezenkívül biztosítja a NATO-kibervédelem hatékonyabb megszervezését és az erőforrások, készségek és képességek jobb kezelését. Ez a NATO hosszú távú alkalmazkodásának része. Továbbra is végrehajtjuk a NATO-nak a kibervédelemre vonatkozó továbbfejlesztett politikáját, és megerősítjük a NATO kibervédelmi képességeit, kihasználva a legújabb élvonalbeli technológiákat. (71.) Biztosítjuk, hogy a szövetségesek megfeleljenek a 21. századra szabott követelményeknek. Napjainkban a Kibervédelmi Vállaláson (Cyber Defence Pledge) keresztül elköteleztük magunkat nemzeti hálózataink és infrastruktúráink kibervédelmének növelése mellett. Támogatjuk a NATO kibervédelmi gyakorlat (Cyber Range) képességét és hatókörét, ahol a szövetségesek készségeket építhetnek, növelhetik a szakértelmet és megismerhetik a legjobb gyakorlatokat."*[17]

A védelmi miniszterek egy frissített kibervédelmi és egy cselekvési tervet fogadtak el 2017. február 16-án a kibertér műveleti területként történő végrehajtására. Ez növeli a szövet-

[16] Joint Publication 3-12 (R) Cyberspace Operations. 5. Feb 2013, 69. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (Letöltés időpontja: 2017. 12. 09.)

[17] NATO Summit Guide Warsaw, 8–9. July 2016, 124–128. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf (Letöltés időpontja: 2017. 12. 09.)

ségesek együttműködési képességét, képességeinek fejlesztését és az információk megosztását. Ugyanezen a napon a NATO és Finnország fokozták az elkötelezettségüket a kiberbiztonsági együttműködésről szóló politikai keretmegállapodás aláírásával. A megállapodás lehetővé teszi a NATO és Finnország számára, hogy jobban védjék hálózatukat és javítsák annak rugalmasságát. A védelmi miniszterek 2017. november 8-án elvben egyetértésüket fejezték ki egy új Kiberműveleti Központ (Cyber Operations Center) létrehozásáról az adaptált NATO parancsnoki struktúra körvonalazásának részeként. Ez erősíti a NATO kibervédelmét, és segít a kiberintegrációs tervezésben és működésben. A miniszterek megállapodtak abban is, hogy integrálják a szövetségesek nemzeti kiberképességeit a NATO-missziókba és -műveletekbe. A szövetségesek fenntartják a hozzájárulások teljes tulajdonjogát, ahogyan a szövetségesek a NATO-missziókban a tankok, a hajók és a repülőgépek tulajdonjogait.

Komoly eredmény a Cambridge University Press által kiadott Tallinn Manual 2.0, amely egy átfogó elemzés arról, hogyan vonatkozik a jelenlegi nemzetközi jog a kiberműveletekre. A Tallinn Manual 2.0 kidolgozását irányította és megkönnyítette a NATO CCDCOE.

Az eredeti Tallinn Kézikönyv középpontjában a legsúlyosabb kiberműveletek álltak, amelyek elutasítják az erő alkalmazását a nemzetközi kapcsolatokban, valamint feljogosítják az államokat arra, hogy fegyveres konfliktus esetén gyakorolják az önvédelem jogát. A Tallinn Manual 2.0 jogi elemzést ad a leggyakoribb kiberincidensekről, amelyek napi szinten megjelennek, és az erőszak vagy fegyveres konfliktus küszöbértékeinek határán helyezkednek el. Mint ilyen, a 2017-es kiadás kiterjed a nemzetközi jog teljes spektrumára, amely a kiberműveletekre alkalmazandó a fegyveres konfliktusok jogára vonatkozó békeidőjogi intervallumokban. A nemzetközi jogi elvek széles körének elemzése és a kibertérben zajló eseményeket szabályozó rendszerek magukban foglalják az általános nemzetközi jog alapelveit, mint például a szuverenitás és a joghatóság gyakorlásának különböző alapjait. Ezenkívül számos speciális nemzetközi terület működik, beleértve az emberi jogokat, a légi és a térjogot, a tengerjogot, a diplomáciai és a konzuli jogot a kiberműveletek összefüggésében.

Michael Schmitt professzor, a CCDCOE vezető munkatársa és az Amerikai Egyesült Államok haditengerészeti háborús kollégiumának professzora irányította a Tallinn Manual 2.0 kezdeményezést. A NATO CCDCOE vezérigazgatója, Liis Vihul volt a mű szerkesztője, emellett a szervezet jogi és informatikai szakemberei is támogatták az erőfeszítéseket. A kézikönyv kibővített kiadása is – az elődjéhez hasonlóan – csak a szerzők véleményét képviseli, nem pedig a NATO, a CCDCOE, a szponzoráló nemzetek vagy bármely más állam vagy szervezet nézeteit.[18]

## A NATO KIBERVÉDELMI IRÁNYELVE (CYBER DEFENCE POLICY)[19]

A NATO jelenleg érvényben lévő kibervédelmi irányelvét (Cyber Defence Policy – CDP) a tagállamok képviselői a walesi csúcstalálkozón, 2014 szeptemberében hagyták jóvá. A CDP megállapítja, hogy a kibervédelem része a Szövetség fő erőfeszítésének, azaz a kollektív védelemnek, és megerősíti, hogy a nemzetközi jog a kibertérben is érvényesül, valamint fokozni kell az együttműködést az iparral. A fő prioritás a Szövetség tulajdonában lévő és általa üzemeltetett kommunikációs rendszerek védelme.

[18] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf (Letöltés időpontja: 2017. 12. 09.)

[19] NATO Summit Guide Warsaw.

A CDP tükrözi a szövetséges döntéseket olyan kérdésekben is, mint az egyszerűsített kibervédelem irányítása, a szövetséges országoknak nyújtott segítség, valamint a kibervédelem műveleti tervezésbe történő integrálása (beleértve a polgári vészhelyzeti tervezést is). A szakpolitika meghatározza a figyelemfelkeltő, az oktatási, képzési és gyakorlati tevékenységek előrehaladásának módjait, és ösztönzi a további előrehaladást a különféle együttműködési kezdeményezésekben, beleértve a partnerországokat és a nemzetközi szervezeteket érintőket is.

A szövetségesek ismételten elkötelezték magukat az információmegosztás és a kölcsönös segítségnyújtás hatékonyságának növelésében, a kibertámadások megelőzésében, mérséklésében és a válaszlépésekben. A NATO kibervédelmi politikáját kiegészíti egy konkrét célokat megfogalmazó cselekvési terv, amely számos témát foglal magában a képességfejlesztés, az oktatás, a képzés és a gyakorlatok, valamint a partnerségek területén.

A szövetségesek 2016-ban a varsói csúcstalálkozón ígéretet tettek a nemzeti hálózatok és infrastruktúrák kibervédelmének megerősítésére. A NATO katasztrófavédelmi képességeinek folyamatos hozzáigazítása mellett a NATO hosszú távú alkalmazkodásának részeként ez javítani fogja a Szövetség kibervédelmét és annak rugalmasságát. Varsóban a szövetségesek ismét megerősítették a NATO védelmi jellegét és kiberteret mint a műveletek egyik dimenzióját, ahol a NATO-nak szintén hatékonyan meg kell védenie magát. Mivel a legtöbb válság és konfliktus ma már a kibertérben is zajlik, ezért a kibertér dimenzióként történő kezelése lehetővé teszi a NATO számára, hogy jobban védje és vezesse le küldetéseit és műveleteit.

## A NATO KIBERVÉDELMI VÁLLALÁSA (CYBER DEFENCE PLEDGE)[20]

A NATO biztonsági fenyegetéseinek új realitása elismeréseként a szövetséges állam- és kormányfők vállalást tesznek annak biztosítására, hogy a Szövetség lépést tartson a gyorsan fejlődő kiberfenyegetésekkel, és hogy a tagállamok képesek lesznek megvédeni magukat a kibertérben is. Megerősítik nemzeti felelősségüket a washingtoni szerződés 3. cikkével összhangban a nemzeti infrastruktúrák és hálózatok kibervédelme és a szövetséges államok biztonsága és kollektív védelme kapcsán, összhangban a Walesben elfogadott megerősített CDP-vel. Biztosítják, hogy az erős és rugalmas kibervédelem lehetővé teszi a Szövetség számára, hogy teljesítse alapvető feladatait. Összekapcsolódásuk azt jelenti, hogy csak annyira erősek, mint a leggyengébb elemük. Együtt fognak dolgozni, hogy jobban védjék hálózataikat, és ezzel hozzájáruljanak a szövetséges műveletek sikeréhez. Támogatják a szövetségesek és az EU munkáját a kiberbiztonság fokozásában, ami hozzájárul az ellenálló képesség erősítéséhez az euroatlanti térségben, és támogatják a további NATO–EU kiberbiztonsági együttműködést. Megerősítik a nemzetközi jog alkalmazhatóságát a kibertérben, és elismerik a releváns nemzetközi szervezetekben végzett munkát, beleértve a felelősségteljes állami magatartás önkéntes normáit és a bizalomépítő intézkedéseket a kibertérben. Elismerik a NATO együttműködésének értékét a partnerországokkal, az iparral és az egyetemekkel, többek között az NICP révén. Hangsúlyozzák a NATO szerepét a kibervédelem terén, többek között multinacionális projektek, oktatás, képzés, gyakorlatok és információcsere megvalósítása alapján a nemzeti kibervédelmi erőfeszítések támogatása érdekében. Biztosítják szövetségeseiknek a kibertudatosság, kiberképzettség, kiberbiztonság elérhetőségét.

[20] NATO Cyber Defence Pledge. https://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en (Letöltés időpontja: 2017. 12. 09.)

A szövetséges állam- és kormányfők kötelezettséget vállalnak a nemzeti hálózatok és infrastruktúrák kibervédelmének további erősítésére. A NATO katasztrófavédelmi képességeinek − a NATO hosszú távú alkalmazkodása részeként történő − folyamatos adaptálásával együtt ez megerősíti a Szövetség kibervédelmét és általános ellenálló képességét. Vállalásaik között szerepel többek között a nemzeti infrastruktúrák és hálózatok védelmi lehetőségeinek teljes körű kifejlesztése. Ez magában foglalja a védelmi szervezeteken belül a kibervédelem megoldását a legmagasabb stratégiai szinten, a kibervédelem további integrálását a műveletekbe és a lefedettség kiterjesztését a bevethető hálózatokra.

A vállalás része a források kiosztása nemzeti szinten a kibervédelmi képességek megerősítése érdekében, továbbá a nemzeti kibertérben érdekelt felek közötti kölcsönhatás, az együttműködés elmélyítése és a tapasztalatok cseréje érdekében történő megerősítése. Ezen túlmenően magában foglalja még a kiberfenyegetésekkel kapcsolatos ismeretek, beleértve az információk és értékelések megosztása hatékonyságának növelését. Tartalmazza az alapvető kiberhigiéniai készségeket és tudatosságot, azok legkifinomultabb és legbiztonságosabb kibervédekezésen keresztül történő fokozását. A kiberoktatás támogatását, az oktatási intézmények számának és minőségének növelését, a bizalom és a tudás kiépítését a Szövetségen keresztül. A vállalás tartalmazza a kibervédelmi kötelezettségvállalások végrehajtásának felgyorsítását, beleértve azokat a nemzeti rendszereket is, amelyektől a NATO függ. A követelések teljesítésének nyomon követése érdekében az elfogadott mutatók alapján éves értékelést készítenek, és a következő csúcson áttekintik a haladást.

## EREDMÉNYEK ÉS KÖVETKEZTETÉSEK

Jelen publikáció a kibervédelmi irányelv fejlődésének folyamatát, a legmeghatározóbb kiváltó eseményeket foglalta össze. Az előzőekben leírtakból egyértelműen látszik, hogy a NATO felismerte az új biztonsági kihívásokat, és lépéseivel reagálni kíván a bekövetkezett eseményekre és a folyamatosan változó helyzetre. Ezen túlmenően fejleszteni akarja az eddig elért és alkalmazott képességeit a kérdéskörrel kapcsolatban, illetve támogatni kívánja az oktatási, a tudományos és a kutatási irányvonalait. Ezenfelül szakmai támogatást kíván nyújtani tagállamainak és saját szervezetének megfelelő képességek biztosításával, valamint elismeri a civil, illetve a magánszféra szakértelmét, és együttműködést valósít meg velük és más nemzetközi szervezetekkel.

Fontos eredmény, hogy a kibervédelem része a NATO kollektív védelmi feladatainak. Továbbra is alapvető a NATO védelmi jellege, és elismerték a kiberteret a műveletek egyik dimenziójaként, amelyben a NATO-nak olyan hatékonyan kell megvédenie magát, mint a levegőben, a szárazföldön és a tengeren. A szövetségesek kibervédelmi vállalást tettek, hogy hangsúlyozzák a kibervédelem fontosságát. A NATO megerősíti a kiberoktatásra, -képzésre és -gyakorlatokra vonatkozó képességeit. A szövetségesek elkötelezettek az információmegosztás és a kölcsönös segítségnyújtás fokozásában, a kibertámadások megelőzésében, mérséklésében és az általuk okozott károk helyreállításában. A közös kihívások fényében a NATO és az EU erősítik a kibervédelem terén folytatott együttműködésüket, különösen az információcsere, a képzés, a kutatás és a tapasztalatátadás területén. A NATO fokozza együttműködését az iparral.[21]

[21] NATO Summit Guide Warsaw.

Véleményem szerint a NATO időben felismerte a kibervédelem és a kiberműveletek fontosságát. Jelentős erőfeszítéseket tett és fog tenni az ehhez kapcsolódó képességek kialakítására és fejlesztésére, így Magyarországnak és a Magyar Honvédségnek is hasonlóképpen kell eljárnia. Fontos megjegyezni: a Magyar Honvédségen belül a kiberbiztonsági képességek megteremtése létfontosságú lehet a jövőben elvégzendő feladatok szempontjából.

## FELHASZNÁLT IRODALOM


Aktív Szerepvállalás, Modern Védelem – a NATO új stratégiai koncepciója magyar nyelven. 2010. december 08. http://old.biztonsagpolitika.hu/?id=16&aid=965&title=aktiv-szerepvallalas-modern-vedelem-a-nato-uj-strategiai-koncepcioja-magyar-nyelven

Az Észak-atlanti Szerződés, Washington DC, 1949. április 4. https://www.nato.int/cps/ic/natohq/official_texts_17120.htm?Selectedlocale=hu

Bányász Péter – Orbók Ákos: *A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében.* Hadtudomány XXIII. évfolyam 1. elektronikus szám, 2013. június. http://mhtt.eu/hadtudomany/2013/2013_elektronikus/2013_e_Banyasz_Peter_Orbok_Akos.pdf

Bucharest Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008. https://www.nato.int/cps/en/natolive/official_texts_8443.htm

Chicago Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012. https://www.nato.int/cps/en/natohq/official_texts_87593.htm

Gyányi Sándor: *Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem.* Doktori (PhD-) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Kar Katonai Műszaki Doktori Iskola, Budapest, 2011. http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2012/gyanyi_sandor.pdf

ITU-T X.1205 telecommunication standardization sector of ITU (04/2008) series x: data networks, open system communications and security telecommunication security overview of cybersecurity. https://www.itu.int/rec/T-REC-X.1205-200804-I

Jobbágy Szabolcs: *Az információs társadalom, az informatika és a távközlés konvergenciája. Múlt, jelen, jövő.* Hadmérnök IV. évfolyam 1. szám, 2009. március. http://www.hadmernok.hu/2009_1_jobbagy.pdf

Joint Publication 3-12 (R) Cyberspace Operations. 5. Feb 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

Kovács László: *Az e-közszolgálatfejlesztés nemzetbiztonsági és hadtudományi kérdései.* In: Nemeslaki András (szerk.): E-közszolgálat fejlesztés: Elméleti alapok és tudományos kutatási módszerek. Nemzeti Közszolgálati Egyetem, Budapest, 2014. http://real.mtak.hu/33733/1/E_kozszolgfejlesztes-nemeslaki.pdf

Kovács László – Szentgáli Gergely: *National Cyber Security Organization: Hungary.* Tallinn, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_HUNGARY_2015-10-12.pdf

LISBON SUMMIT DECLARATION, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon on 20. November 2010. https://www.nato.int/cps/en/natohq/official_texts_68828.htm

NATO Cyber Defence Pledge. https://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en

NATO Cyber Defence, Public Diplomacy Division (PDD) – Press & Media Section July 2016. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf

NATO Summit Guide Warsaw, 8–9 July 2016. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf

Strasbourg / Kehl Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl, 4 April 2009. https://www.nato.int/cps/en/natohq/news_52837.htm?mode=pressrelease

Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon 19–20. November 2010. https://www.nato.int/cps/ua/natohq/official_texts_68580.htm

Szenes Zoltán: Új bor a régi palackban? A walesi NATO-csúcs. Hadtudomány, 2014/3–4. http://mhtt.eu/hadtudomany/2014/3_4/2014_3_4_1.pdf

Szentgáli Gergely: *A NATO kibervédelmi politikájának fejlődése.* Bólyai Szemle XXI. évf. 2. szám, 2012. http://archiv.uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf

Tóth András: *A prágai NATO-csúcstalálkozót követő határozatok, megállapodások a parancsnoki rendszer és a vezetési rendszer korszerűsítésére, valamint az együttes tevékenység képesség fejlesztésére*. Hadmérnök XI. évfolyam 3. szám, 2016. szeptember. http://hadmernok.hu/163_17_tothandras.pdf

Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales 05. Sep. 2014. https://www.nato.int/cps/ic/natohq/official_texts_112964.htm