Fekete-Karydis Klára t. őrnagy – Lázár Bence százados:

A KIBERVÉDELEM KATONAI DIMENZIÓI

DOI: 10.35926/HSZ.2020.3.4

ÖSSZEFOGLALÓ: *A kibervédelem aktualitása hazai és nemzetközi szinten is megkérdőjelezhetetlenné vált, ami a jelenség körüli stratégiák, képzési programok és szakmai fórumok számának gyors növekedésében is megmutatkozik. Az illegális tevékenységek és a terrorizmus új kapcsolódási pontjai egyúttal azt is megkövetelik a kormányzattól, illetékes szerveitől, ügynökségeitől és tisztviselőitől, hogy csak egy kevesek által értett technológia által megtestesített jelenséget szabályozzanak, és továbbfejlesszék a gyorsan változó technológiákkal szembeni védelmet.. A NATO és az Európai Unió kibervédelmi stratégiájának fejlődése meghatározó iránymutatás a hazai szakirányítási rendszer kialakításához.*

KULCSSZAVAK: *kiberstratégia, kritikus információs infrastruktúra, terrorizmus, kiberbiztonság, NATO, Európai Unió, kibertámadás, hibrid hadviselés, haderőfejlesztés, kibervédelem, Magyar Honvédség*

BEVEZETÉS

Elemi fontosságú, hogy kormányzati és nem kormányzati szinten is minden lehetséges módon megvédjük szűkebb és tágabb kiberkörnyezetünket, ami azért is jelent nagy kihívást, mert ez korunk leggyorsabban fejlődő iparága és legszélesebb körben terjedő technológiája. A kibervédelmi kihívások megfelelő kezeléséhez alapvető fontosságú – mint minden más esetben – a kibertér és az abban előforduló események definiálása, elválasztása, a kibervédelmi fenyegetések tipizálása, a kibertérben tapasztalt incidensek kezeléséből levonható következtetések rendszerezése, a nemzeti és a nemzetközi kiberstratégiai eredmények és kihívások összevetése és végül – mint legfontosabb tényező – e gyorsan változó dimenzió evolúciójának és potenciális jövőbeni incidenseinek prognosztizálása. A Magyar Honvédség tekintetében ez egyet jelent a NATO által a műveletek negyedik dimenziójaként deklarált kibertérre vonatkozó védelmi képességek fejlesztési irányainak azonosításával, illetve a fejlesztések technológiai és humán erőforrásait biztosító eszközök megteremtésének feltételrendszerével.

A NATO KIBERVÉDELMI STRATÉGIÁJA

A Szövetség kibervédelmi alapelveinek lefektetésében és közös struktúráinak, sztenderdjeinek kialakításában a NATO 2007. december 20-án elfogadott Kibervédelmi Politikája (CDP[1]) jelentette az első lépést, majd a bukaresti csúcstalálkozó deklarációjának[2] (2008. április 3.) 47. paragrafusa erősítette meg, hogy a NATO:

[1] NATO Cyber Defence Policy.

[2] 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. NATO E-library, 03. 04. 2008. https://www.nato.int/cps/us/natohq/official_texts_8443.htm (Letöltés időpontja: 2019. 06. 18.)

– elkötelezett a kulcsfontosságú szövetségi információs rendszerek megerősítésében a számítógépes támadásokkal szemben;
– fejleszti a kibervédelmi struktúrákat és hatóságokat, illetve az azok közti kapcsolatokat;
– számítógépes védelem politikája hangsúlyozza, hogy a szövetségeseknek és a Szövetség egészének is meg kell védeniük a kulcsfontosságú információs rendszereket a saját felelősségüknek megfelelően;
– előirányozza a legjobb gyakorlatok megosztását;
– segítségnyújtást biztosít a szövetséges nemzeteknek a számítógépes támadások elleni küzdelemben.

A Szövetség állam- és kormányfőinek lisszaboni csúcstalálkozóján (2010. november 19–20.) elfogadott NATO Stratégiai Koncepciója[3] kiemeli a gyorsan fejlődő, egyre gyakrabban jelentkező és egyre kifinomultabb kibertámadások megelőzésére, detektálására és kivédésére, illetve a kibertámadásokat követő helyreállításra alkalmas képességek továbbfejlesztésének igényét. A kiberfenyegetettség előretörése és a kibervédelmi képességek extenzív fejlesztése iránti igény a lisszaboni csúcstalálkozó deklarációjában[4] is tükröződik, hiszen a két és fél évvel korábbi záródokumentumhoz képest már nagyobb terjedelemben és jóval differenciáltabban részletezi a NATO kibervédelmi képességfejlesztésének sarkalatos pontjait. Mivel a kibertérből érkező fenyegetések − legyenek a támadók államok, terroristák, hacktivisták, bűnszövetkezetek vagy bárki más – már ekkor jelentős kihívást jelentettek a Szövetség számára, az állam- és kormányfők a deklarációban feladatot szabtak az Északatlanti Tanács számára egy, a már létező nemzetközi struktúrákra és az érvényben lévő kibervédelmi politikára épülő új kibervédelmi stratégia és az implementációját támogató végrehajtási akcióterv kidolgozására.

A NATO Kibervédelmi Koncepciója (CDC[5]) első verzióját a védelmi miniszterek 2011. márciusi találkozóján mutatták be, és ez képezte a NATO védelmi minisztereinek 2011. június 8-i találkozóján elfogadott NATO CDP – *A hálózatok védelmében*[6] – koncepcionális alapját. Ez az új szakpolitikai dokumentum egy akciótervvel is kiegészült, és a NATO CDP végrehajtási terve részletesen tartalmazza a NATO saját struktúráinak, szervezeti egységeinek, illetve a szövetségesek haderőinek feladatait és végrehajtandó kibervédelmi tevékenységeit. Az előbbi dokumentum jelentősége abban áll, hogy túllépett a korábbi megközelítésen, és kontextusba helyezte a kibervédelmet a Szövetség védelmi és válságkezelési tevékenységében. Egyfelől beemelte a kiberteret a biztonsági környezetről szóló rész tárgyalásába, és egy szintre helyezte a terrorizmus elleni küzdelemmel, illetve a NATO határain kívül eső konfliktusok által generált válságkezelési feladatokkal, másrészt a védelemről és elrettentésről szóló fejezet oszlopos elemévé tette. Az utóbbit úgy kell tekintenünk, mint a NATO gyakorlati kibervédelmének stratégiai megalapozását az informatikai és kommunikációs rendszerek védelmére, illetve a kibertérből érkező és folyamatosan változó fenyegetések elhárítására.

---

[3] Strategic Concept 2010. NATO E-library, 03. 02. 2012. https://www.nato.int/cps/ic/natohq/topics_82705.htm (Letöltés időpontja: 2019. 06. 18.)

[4] Lisbon Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon. NATO E-library, 31. 07. 2012. https://www.nato.int/cps/en/natolive/official_texts_68828.htm (Letöltés időpontja: 2019. 06. 18.)

[5] NATO Cyber Defence Concept.

[6] Defending the Networks – NATO Policy on Cyber Defence. 2011. https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf (Letöltés időpontja: 2019. 07. 13.)

A NATO új kibervédelmi szakpolitikája a Szövetség prioritásait és kibervédelmi tevékenységét, erőfeszítéseit is részletesen kifejti mind a célok megfogalmazását, mind pedig azok megvalósításának módját illetően. A NATO CDP központi eleme a koordinált megközelítés, e köré épül a Szövetség kibervédelmének felépítése, beágyazása a létező védelmi és válságkezelési struktúráiba, valamint gyakorlati megvalósítása a NATO szervezeti egységeinek, tagállamainak és külső partnereinek részvételével, illetve együttműködésében. A dokumentum sarkalatos pontjai:

– prevenció és ellenálló képesség;
– a Szövetség és a tagállamok kritikus kiberképességeinek védelme;
– robusztus kibervédelmi képességek kiépítése;
– a NATO saját hálózatai védelmének centralizálása;
– minimumkövetelmények megfogalmazása a Szövetség feladat-végrehajtása szempontjából kritikus tagállami hálózatok védelme érdekében, illetve a tagállamok ez irányú törekvéseinek, erőfeszítéseinek központi támogatása;
– széles körű összefogás kialakítása a nemzetközi partnerekkel, a privát szférával és a tudományos világgal a kitűzött célok elérése érdekében.

A NATO ezt követően egyre kiterjedtebben és mélyebben foglalkozott a kibervédelemmel mint a kollektív védelem egyik pillérével, mellyel kapcsolatos következtetései és további célkitűzései rendre megjelentek a 2012-es chicagói, a 2014-es walesi, a 2016-os varsói és a 2018-as brüsszeli csúcstalálkozóinak zárónyilatkozataiban is.

Chicagóban alapvetően a lisszaboni feladatokkal kapcsolatban elért eredményeket és további feladatokat bontottak ki, valamint megemlítették a tallinni Kooperatív Kibervédelmi Kiválósági Központot (CCDCOE[7]) és a NATO SHAPE-en működő komputerincidensre reagáló képességét (NCIRC[8]) mint a már létező struktúrákra történő támaszkodás alapelvét.[9] Elkezdődött a NATO döntéshozatali és döntés-előkészítő mechanizmusainak szervezeti átstrukturálása is, melynek célja az egyre növekvő volumenű és jelentőségű kibervédelmi feladatok meghatározása és végrehajtása volt.

A walesi csúcstalálkozó egyetemes megvilágításba helyezte a kibervédelem kérdését, amit olyan dekrétumok jeleztek a találkozó 2014. szeptember 5-i zárónyilatkozatában, mint a nemzetközi jog, a humanitárius jog és az ENSZ Alapokmányának érvényessége a kibertérben, vagy az, hogy a kibertérből érkező támadások veszélyt jelenthetnek az euroatlanti államok prosperitására, biztonságára és stabilitására, és hogy azok indokolttá tehetik a Washingtoni Szerződés 5. cikkelyének életbe léptetését. Új elemként a kibervédelmi oktatás, képzés és a kibervédelmi gyakorlatok továbbfejlesztése jelenik meg alapvető követelményként.[10]

Az egyes államokat érő kibertámadások jogi aspektusainak kezelésében a Szövetségnek már ekkor is rendelkezésére állt a 2013 áprilisában megjelent *Tallinni kézikönyv a nemzetközi*

[7] Cooperative Cyber Defence Centre of Excellence.

[8] NATO Computer Incident Response Capability.

[9] 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. NATO E-library, 01. 08. 2012. https://www.nato.int/cps/ra/natohq/official_texts_87593.htm?selectedLocale=en (Letöltés időpontja: 2019. 06. 18.)

[10] Wales Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. 30. 08. 2018. https://www.nato.int/cps/ic/natohq/official_texts_112964.htm (Letöltés időpontja: 2019. 06. 18.)

jog alkalmazhatóságáról a kiberhadviselésben,[11] mely átfogó elemzést nyújt a legdestruktívabb, fegyveres támadással felérő vagy a fegyveres konfliktusokat kísérő kibertámadások nemzetközi jogi kezeléséhez. Folytatása a *Tallinni kézikönyv 2.0 a nemzetközi jog alkalmazhatóságáról a kiberműveletekben*,[12] amely 2017 februárjában jelent meg, kiegészítve az előző kézikönyv alkalmazási területét. Ez jelenleg a legátfogóbb elemzés a szakterületen,[13] mely egységes jogi keretet ad minden rosszindulatú kiberművelet kezeléséhez. 2017 februárjában elfogadták a walesi csúcstalálkozó által jegyzett kibervédelmi akcióterv frissített változatát is, mely még hatékonyabban támogatja a 2014-ben meghatározott szakpolitika lényegi elemeit, melynek értelmében:

- a kibervédelem a Szövetség alapvető kollektív védelmi feladata;
- a nemzetközi jog a kibertérben is hatályos;
- a NATO fokozza együttműködését az iparral;
- elsődleges prioritás a NATO saját tulajdonú és működtetésű kommunikációs rendszereinek védelme.

Áttörést a 2016. júliusi varsói csúcstalálkozó hozott a NATO kibervédelmi stratégiájában, amikor a Szövetség a kommünikéjében[14] a műveletek negyedik színterévé minősítette a kiberteret, újabb lendületet adva ezzel minden addigi intézkedésének és stratégiai célkitűzésének, meghatározva így a kibervédelem fejlesztésének további irányát. Új elemként jelent még meg ezzel összefüggésben a béke, a biztonság és a stabilitás iránti igény a kibertérben, annak nevesítése, hogy a kibertámadások eredhetnek állami szereplőktől és terroristáktól is, valamint a „NATO Cyber Range" kibővítésére vonatkozó vállalás. A zárónyilatkozat mellett a 2016. július 9-én kiadott varsói nyilatkozat a transzatlanti biztonságról is említést tesz a kiber- és a hibrid támadások közti kapcsolatról mint új jelenségről, melynek kezelése szintén bekerült a Szövetség feladatrendszerébe. A kiberbiztonság és kibervédelem exponenciálisan növekvő fontosságát aláhúzandó a varsói csúcstalálkozó első napján, 2016. július 8-án fogadták el a NATO kibervédelmi vállalását, mely prioritást adott a nemzeti kibervédelmi infrastruktúrák – addig önkéntes vállalásokon alapuló – fejlesztésének.

Kialakuló hagyományként a NATO brüsszeli csúcstalálkozójának első napján, 2018. július 11-én is kiadtak egy nyilatkozatot a transzatlanti biztonságról és szolidaritásról,[15] mely előkelő helyen, a harmadik legfontosabb feladatként jeleníti meg a Szövetség és az egyes tagállamok kibervédelmi képességeinek továbbfejlesztését immár külön paragrafusban, elkülönülten a hibrid fenyegetésektől.

---

[11] Michael N. Schmitt (Gen. ed.): Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, 03. 2013. https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE (Letöltés időpontja: 2019. 06. 18.) DOI: https://doi.org/10.1017/CBO9781139169288

[12] Michael N. Schmitt (Gen. ed.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 02. 2017. https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9 (Letöltés időpontja: 2020. 03. 22.) DOI: https://doi.org/10.1017/9781316822524

[13] Tallinn Manual 2.0 – The most comprehensive guide for policy advisors and legal experts on how existing International Law applies to cyber operations. CCDCOE. https://ccdcoe.org/research/tallinn-manual/ (Letöltés időpontja: 2020. 03. 22.)

[14] Warsaw Summit Communiqué – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016. NATO E-library, 29. 03. 2017. https://www.nato.int/cps/su/natohq/official_texts_133169.htm (Letöltés időpontja: 2019. 06. 18.)

[15] Brussels Declaration on Transatlantic Security and Solidarity. NATO E-library, 11. 07. 2018. https://www.nato.int/cps/en/natohq/official_texts_156620.htm (Letöltés időpontja: 2019. 06. 18.)

A csúcstalálkozót záró 2018. július 12-i deklaráció[16] konkrét javaslatokat és fejlesztési irányokat fogalmaz meg a terrorista-, kiber- és hibrid fenyegetések hármasának kezelésére, valamint olyan, már használatban lévő fogalmakkal kapcsolatban, mint a kiberbiztonság, kibervédelem, kiberbűnözés, kibertámadás és kiberfenyegetés. Emellett bevezették a kiber ellenálló képesség[17] és a rosszindulatú kibertevékenység[18] fogalmakat is, továbbá egyes országok – Jordánia, Oroszország, Szíria, Ukrajna – vonatkozásában is előtérbe kerültek a kiber- és hibrid műveletek. Ez a dokumentum már tekintélyesnek mondható eredményekről[19] és további intézményi építkezésről is beszámol a kibervédelem területén a Szövetségen belül[20] és külső partnereivel[21] kapcsolatban egyaránt, mely alapvetően a már létező struktúrára épül, melynek meghatározó intézményei a:

- NATO Kibervédelmi Menedzsment Tanács;[22]
- NATO Konzultációs, Ellenőrzési és Parancsnoki Tanács;[23]
- NATO Kibervédelmi Bizottság;[24]
- Kibervédelmi Menedzsment Hatóság;[25]
- NATO Kommunikációs és Információs Ügynökség:[26]
  - NATO Számítógépes Incidensre Reagáló Képesség/Műszaki Központ;[27]
  - NATO Vezetés, Irányítás, Kommunikáció, Számítógép, Hírszerzés, Megfigyelés és Felderítés;[28]
- Kooperatív Kibervédelmi Kiválósági Központ;[29]
- NATO SHAPE Kibertér Műveleti Központ;[30]
- NATO–Ukrajna Hibrid Hadviselés Elleni Platform.[31]

Az NCIA 2019. február 19-én elindította a „kibervédelmezők közösségét”,[32] mely hivatalosan a Kibervédelmi Együttműködési Központ[33] nevet viseli. A kezdeményezést Jens Stoltenberg NATO-főtitkár jelentette be 2018-ban a Szövetség egyik fő kiberbiztonsági célkitűzésének támogatására, nevezetesen egy információmegosztási, képzési és szakértői hub kialakítása érdekében, mely a tagállamok között már létező egyetértési megállapodásokra épül.[34]

---

[16] Brussels Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11–12 July 2018. NATO E-library, 30. 08. 2018. https://www.nato.int/cps/ic/natohq/official_texts_156624.htm (Letöltés időpontja: 2019. 07. 13.)

[17] Cyber Resilience.

[18] Malicious Cyber Activities.

[19] Brussels Summit Declaration: 70. bek.

[20] Uo. 29.

[21] Uo. 56., 66. bek.

[22] Cyber Defence Management Board.

[23] Consultation, Control and Command (NC3) Board.

[24] NATO Cyber Defence Committee.

[25] Cyber Defence Management Authority (CDMA).

[26] Communications and Information Agency (NCIA).

[27] NATO Computer Incident Response Capability/Technical Centre (NCIRC/TC).

[28] NATO Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR).

[29] Cooperative Cyber Defence Centre of Excellence.

[30] Cyberspace Operations Centre.

[31] NATO-Ukraine Platform on Countering Hybrid Warfare.

[32] Cyber Defenders’ Community.

[33] Cyber Security Collaboration Hub.

[34] New NATO hub will gather the Alliance’s cyber defenders. NATO E-library, 12. 02. 2019. https://www.nato.int/cps/en/natohq/news_163358.htm (Letöltés időpontja: 2019. 06. 18.)

EU–NATO-EGYÜTTMŰKÖDÉS

Az EU (CERT[35]) és a NATO (NCIRC) kibervédelmi együttműködése a Kibervédelmi Technikai Megállapodás[36] 2016. február 10-i aláírásával kezdődött. Még ugyanabban az évben intézményesült a két szervezet stratégiai együttműködése, mely a NATO varsói csúcstalálkozója margóján a Donald Tusk és Jean-Claude Juncker, az Európai Tanács, illetve az Európai Bizottság elnökei, valamint Jens Stoltenberg NATO-főtitkár által 2016. július 08-án aláírt közös nyilatkozatban manifesztálódott.[37] A deklaráció hét együttműködési területet jelölt meg, melyek:

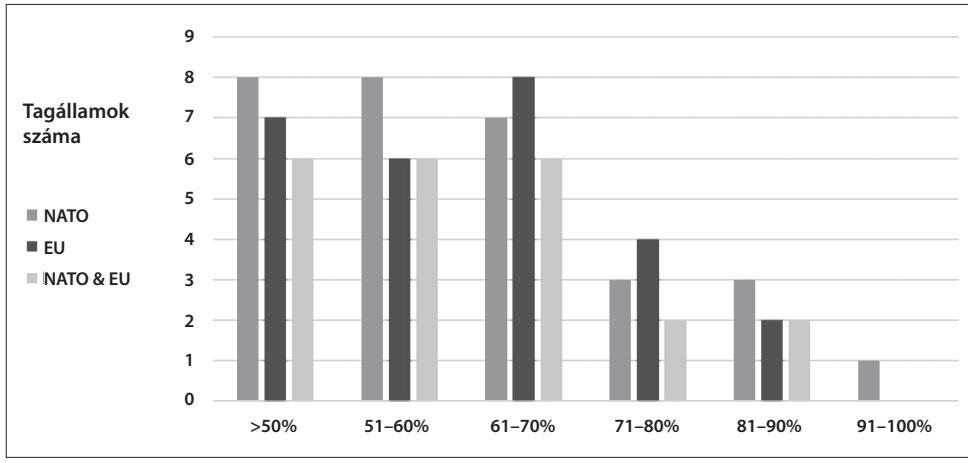
– a hibrid fenyegetések elleni küzdelem;
– műveleti együttműködés, beleértve a tengerészeti és a migrációval kapcsolatos műveleteket;
– kiberbiztonság és -védelem;
– védelmi képességek;
– védelmi ipari kutatás;
– közös gyakorlatok végrehajtása;
– a keleti és a déli partnerek képességépítési erőfeszítéseinek támogatása.

A hét területen mindösszesen 74 konkrét javaslatot fogadtak el, illetve hajtottak végre. Közülük kiemelt szerepet kapott a hibrid fenyegetések elleni küzdelem – a 74-ből 20 projekt erre a területre fókuszál –, valamint a kiberbiztonság és a kibervédelem, melyek szinte minden prioritási területen végigvonulnak.

1. táblázat *NATO- és EU-tagállamok osztályozása GCI-érték*[38] *szerint (Saját szerkesztés a Nemzetközi Telekommunikációs Szövetség – ITU – adatai*[39] *alapján)*

	91–100%	81–90%	71–80%	61–70%	51–60%	41–50%	31–40%
NATO	US	CA	NO	IS	TR	ME	AL
NATO EU		EE	UK	DE	CZ	PT	MT
		FR	NL	BE	LU	LT	SK
				DK	HR	GR	SL
				LV	RO		
				IT	BG		
				PL	HU		
					ES		
EU			FI	IE		CY	
			SE	AT			

[35] Computer Emergency Response Team – Számítógépes Vészhelyzet-elhárítási Csoport.
[36] Technical Agreement on Cyber Defence.
[37] Joint declaration – by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. NATO E-library, 05. 12. 2017. https://www.nato.int/cps/en/natohq/official_texts_133163.htm (Letöltés időpontja: 2020. 03. 22.)
[38] Global Cybersecurity Index – Globális Kiberbiztonsági Index.
[39] Global Cybersecurity Index (GCI) 2017. International Telecommunication Union (ITU). https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf (Letöltés időpontja: 2019. 06. 18.)



1. ábra *A NATO- és az EU-tagállamok osztályozása GCI-érték szerint (Saját szerkesztés az ITU adatai*[40] *alapján)*

2. táblázat *A NATO- és az EU-tagállamok egymáshoz viszonyított GCI-értékei (Saját szerkesztés az ITU adatai*[41] *alapján)*

	91–100%	81–90%	71–80%	61–70%	51–60%	41–50%	31–40%	Összes
NATO (db)	1	3	3	7	8	4	4	29
NATO átlaga (%)	91,9	87,8	77,6	65,6	57,5	47,7	35,5	61,6
EU (db)	0	2	4	8	7	4	3	28
EU átlaga (%)	–	83,3	75,4	65,2	57,4	47,5	36,8	60,7
NATO és EU (db)	0	2	2	6	7	3	3	22
NATO és EU átlaga (%)	–	83,3	77,2	65,1	57,4	49,6	36,8	58,0

A politikai dialógus elmélyítése érdekében folytatódtak a releváns miniszteri találkozókra történő kölcsönös meghívások. 2018. július 10-én újabb közös nyilatkozatot[42] írtak alá a két szervezet vezetői a brüsszeli NATO-csúcstalálkozó előtt. Az együttműködés eredményeként megkezdődött a két szervezet között a kibertámadásokra vonatkozó valós idejű figyelmez-

[40] Uo.

[41] Uo.

[42] Joint Declaration on EU-NATO Cooperation – by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. NATO E-library, 10. 07. 2018. https://www.nato.int/cps/en/natohq/official_texts_156626.htm (Letöltés időpontja: 2019. 06. 21.)

tetések cseréje,[43, 44] valamint a kibertámadások, illetve hibrid fenyegetések közös kezelését elősegítő gyakorlatok bevezetése. Az EU és a NATO elkötelezettsége további rendkívül fontos területeken[45] is eredményes:

– az interoperabilitás előmozdítása az egységes kibervédelmi követelmények és szabványok révén;
– a képzés és a gyakorlatok terén folytatott együttműködés erősítése;
– a kibervédelem kutatási és technológiai innovációs együttműködésének előmozdítása;
– a kiberkezelés folyamatos érvényesítése a válságkezelési eljárásokban és folyamatokban.

A 3. táblázatból kitűnik, hogy a szabályozás és a képességfejlesztés naprakészsége, illetve annak hiánya rövid időn belül rapid és jelentős változásokat eredményezhet, ezért is kiemelten fontos, hogy a kibervédelem folyamatosan benne legyen a stratégiai gondolkodásban, hiszen az ellenálló képesség és a stratégiai függetlenség csak mindenre kiterjedő megközelítéssel érhető el a kiberbiztonság területén.

3. táblázat *A legjobb kibervédelmi képességgel rendelkező országok (Saját szerkesztés az ITU*[46] *adatai alapján)*

2017			2015		
Rangsor	Ország	Index	Rangsor	Ország	Index
1.	Szingapúr	0,925	1.	USA	0,824
2.	USA	0,919	2.	Kanada	0,794
3.	Malajzia	0,893	3–5.	Ausztrália Malajzia Omán	0,765
4.	Omán	0,871	6–7.	Új-Zéland Norvégia	0,735
5.	Észtország	0,846	8–14.	Brazília Észtország Németország India Japán Dél-Korea UK	0,706
6.	Mauritius	0,830	15–19.	Ausztria Magyarország Izrael Hollandia Szingapúr	0,676

[43] EU and NATO for defence of Europe: coherent, complementary and interoperable. EU External Action, 11. 07. 2018. https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/48265/eu-and-nato-defence-europe-coherent-complementary-and-interoperable_en (Letöltés időpontja: 2019. 06. 18.)

[44] NATO and EU leaders sign joint declaration. NATO E-library, 10. 07. 2018. https://www.nato.int/cps/en/natohq/news_156759.htm (Letöltés időpontja: 2019. 07. 17.)

[45] European Union and NATO work together to tackle growing cyber threats. EU External Action, 11. 12. 2018. https://eeas.europa.eu/headquarters/headquarters-homepage/55217/european-union-and-nato-work-together-tackle-growing-cyber-threats_en (Letöltés időpontja: 2019. 06. 18.)

[46] Global Cybersecurity Index (GCI) 2017.

2017			2015		
Rangsor	Ország	Index	Rangsor	Ország	Index
7.	Ausztrália	0,824	20–22.	Lettország Svédország Törökország	0,647
8–9.	Georgia Franciaország	0,819	23–27.	Hongkong Finnország Katar Szlovákia Uruguay	0,618
10.	Kanada	0,818	28–33.	Kolumbia Dánia Egyiptom Franciaország Mauritius Spanyolország	0,588
11.	Oroszország		34–36.	Olaszország Marokkó Uganda	0,559
12–13.	Japán Norvégia	0,786	37–40.	Azerbajdzsán Lengyelország Ruanda Tunézia	0,529
⋮			41–43.	Csehország Georgia Oroszország	0,500
51–55.	Magyarország	0,534	⋮		

ÖSSZEGZÉS

A NATO kibervédelmi stratégiájának és az ebből adódó intézmény- és képességfejlesztési kapacitásainak bővítése és kiterjesztése 2007-ben kapott először hangsúlyt. 2010-ben, a Szövetség állam- és kormányfőinek lisszaboni csúcstalálkozóján elfogadott NATO Stratégiai Koncepciójával kezdődött az a korszak, amely a 21. századi kihívások fényében egy új időszak kezdetét jelölte. Az azt követő öt év a kormányzati és a privát szférában működő szervezetek ellen irányuló hekkertámadások és a 2008 óta létező kriptovalutákra irányuló lopások sorozatát hozta. Ezek újra és újra ráirányították a figyelmet arra, hogy a kibertérben a hacktivisták, a szervezett bűnözés, a terroristák és az állami szereplők is elkövethetnek és elkövetnek olyan bűncselekményeket, melyek különböző irányokból és különböző módszerekkel támadhatják néha sikeresen egy-egy szervezet, állam vagy akár a Szövetség kiberbiztonsági infrastruktúráját, illetve azok tárolt adatait és eszközeit.

A meghatározó gyártók, pénzügyi szolgáltatók, kereskedelmi láncok, internetes szolgáltató cégek és a már használatban lévő kriptovaluták tekintetében megvalósult bűncselekmények fényében a NATO-tagállamok korán felismerték, hogy a kritikus infrastruktúra védelmét fokozottan, a 21. századi kihívások fényében pedig új eszközökkel is biztosítani szükséges a nemzetbiztonsági érdekek védelmében és a biztonság katonai erőkkel biztosítható feltételeinek megfelelően. Ezért 2011-ben megkezdődött az az építkezés, mely amellett, hogy választ ad az új kihívásokra, 2016-ban áttörést hozott a kibervédelem katonai vetületében.

Ennek egyik sarkalatos pontja a NATO kibervédelmi stratégiájának és intézményi fejlesztésének a már létező és hatékonyan működő intézményrendszer alapján történő építkezés volt. Ez egyre diverzifikáltabb formában jelent meg a 2011-es CDC-ben, a NATO védelmi minisztereinek 2011. június 8-i találkozóján elfogadott NATO CDP – *A hálózatok védelmében* című dokumentumban, a NATO–EU kibervédelmi együttműködésének kezdetét deklaráló 2016-os közös dekrétumban és megállapodásban, valamint a 2019-ben végrehajtott szervezeti fejlesztésekben. Ezeknek köszönhetően a Szövetség nemcsak válaszolni képes immár a kiberbiztonsági kihívásokra, de sokkal inkább azok központi bástyájává vált a tagállamok nemzetbiztonsági érdekei és azok kritikus infrastruktúrája védelmében. A terrorizmus elleni harc hosszú évtizedek óta a NATO fókuszpontjában áll, a kibertér azonban csak az ezredforduló után vált a terroristák által is célpontnak tekintett működési területté. A Szövetség már 2010-ben felismerte, hogy a kibertérben is meg kell védeni a tagállamok polgárainak biztonságát, és ennek biztosítására először 2011-ben tett határozott, markáns vállalást, majd 2016 nyarán a hadviselés negyedik dimenziójává nyilvánította a kiberteret.

2016-ban a Szövetség még együtt, egymással szoros kölcsönhatásban jelentkező kihívásként kezelte a kiber- és a hibrid hadviselést, ami tulajdonképpen ma is helytálló az átfedések miatt. 2018-ra azonban ugrásszerűen megnőtt a kibertérben okozott pénzügyi és a versenyszférát sújtó károk összege, de mivel a pénzügyi szektor nemzeti és globális szinten is a kritikus infrastruktúra meghatározó eleme, ezért 2018-ban szétválasztották a kiberhadviselést és a hibrid hadviselést.

A NATO állam- és kormányfőinek először a 2014-es csúcstalálkozóján tett dekrétumukban jutott kifejezésre ama felismerés, hogy a kibertér biztonsága a stabilitás és a prosperitás szempontjából is meghatározó jelentőségű, s ez egyre határozottabb formában jelent meg a kihívásokra adott válaszok és az intézményi építkezés szempontjából 2016-ban is.

A fentiek tekintetében a kibervédelmi képességek folyamatos fejlesztése a szövetségi intézményekben és a tagállamokban is természetes igényként jelent meg 2014-ben. Ezt 2018-ban már a NATO és az EU együttműködése egyik kiemelt feladataként is megfogalmazták, és azóta is egyre diverzifikáltabb formában jelenik meg a kormányzati és a nemzetközi intézmények napirendjében és feladatrendszerében.

2018 óta is folyamatosan, bár a Szövetség szerepvállalásának és a nemzetközi összefogásnak köszönhetően csökkenő ütemben jelentkeznek támadások a kibertérben a kritikus infrastruktúra és a katonai biztonság tekintetében. A kibertámadások diverzifikálódását és a NATO elkötelezettségét figyelembe véve biztosra vehető, hogy 2020-ban is a NATO napirendjén lesznek a kibervédelemmel kapcsolatos kérdések, és vélhetően újabb szintre emelkednek a Szövetség, a nemzetközi közösség és a tagállamok ez irányú vállalásai.

FELHASZNÁLT IRODALOM

Brussels Declaration on Transatlantic Security and Solidarity. NATO E-library, 11. 07. 2018. https://www.nato.int/cps/en/natohq/official_texts_156620.htm

Brussels Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11–12 July 2018. NATO E-library, 30. 08. 2018. https://www.nato.int/cps/ic/natohq/official_texts_156624.htm

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. NATO E-library, 03. 04. 2008. https://www.nato.int/cps/us/natohq/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. NATO E-library, 01. 08. 2012. https://www.nato.int/cps/ra/natohq/official_texts_87593.htm?selectedLocale=en

Defending the Networks – NATO Policy on Cyber Defence. 2011. https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf

EU and NATO for defence of Europe: coherent, complementary and interoperable. EU External Action, 11. 07. 2018. https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/48265/eu-and-nato-defence-europe-coherent-complementary-and-interoperable_en

European Union and NATO work together to tackle growing cyber threats. EU External Action, 11. 12. 2018. https://eeas.europa.eu/headquarters/headquarters-homepage/55217/european-union-and-nato-work-together-tackle-growing-cyber-threats_en

Global Cybersecurity Index (GCI) 2017. International Telecommunication Union (ITU). https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf (Letöltés időpontja: 2019. 06. 18.)

Joint declaration – by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. NATO E-library, 05. 12. 2017. https://www.nato.int/cps/en/natohq/official_texts_133163.htm

Joint Declaration on EU-NATO Cooperation – by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. NATO E-library, 10. 07. 2018. https://www.nato.int/cps/en/natohq/official_texts_156626.htm

Lisbon Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon. NATO E-library, 31. 07. 2012. https://www.nato.int/cps/en/natolive/official_texts_68828.htm

NATO and EU leaders sign joint declaration. NATO E-library, 10. 07. 2018. https://www.nato.int/cps/en/natohq/news_156759.htm

New NATO hub will gather the Alliance's cyber defenders. NATO E-library, 12. 02. 2019. https://www.nato.int/cps/en/natohq/news_163358.htm

Schmitt, Michael N.: *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press, 02. 2017. https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9 DOI: https://doi.org/10.1017/9781316822524

Schmitt, Michael N.: *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press, 03. 2013. https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE DOI: https://doi.org/10.1017/CBO9781139169288

Strategic Concept 2010. NATO E-library, 03. 02. 2012. https://www.nato.int/cps/ic/natohq/topics_82705.htm

Tallinn Manual 2.0 – The most comprehensive guide for policy advisors and legal experts on how existing International Law applies to cyber operations. CCDCOE. https://ccdcoe.org/research/tallinn-manual/

Wales Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. 30. 08. 2018. https://www.nato.int/cps/ic/natohq/official_texts_112964.htm

Warsaw Summit Communiqué – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016. NATO E-library, 29. 03. 2017. https://www.nato.int/cps/su/natohq/official_texts_133169.htm