11. fejezet

Szövetségi stratégiák – Az EU–NATO-együttműködés

Molnár Anna

Bevezetés

Napjainkban az információs és kommunikációs technológiák (IKT) gyakorlatilag minden területre kiterjedő használata egyszerre szolgál a gazdasági növekedés és az innováció elősegítőjeként, valamint az aszimmetrikus kiberfenyegetések forrásaként. Az elmúlt évtizedekben az egyénekkel, vállalatokkal és kritikus infrastruktúrákkal szembeni növekvő számú kibertámadás egyre inkább felhívta a figyelmet a kibertérrel kapcsolatos fenyegetésekre és kockázatokra. Tekintettel arra, hogy a számítógépes bűnözés nem ismeri a nemzeti határokat, és egyes államok támadó és védelmi jellegű kiberképességeiket egyaránt fejlesztik, e területen is szükségessé vált a nemzetközi normák és együttműködés feltételrendszerének kiépítése. A genfi internetplatform (*Geneva Internet Platform* – GIP) adatai szerint 2021-ben a támadó kiberképességekkel rendelkező államok száma elérte a 23-at, emellett további 30 állam tervezi ilyen típusú képességek fejlesztését.[1]

A kritikus infrastruktúrák növekvő kitettsége miatt a nemzetközi rendszer szereplői riasztóan kiszolgáltatottá váltak a rosszindulatú kiberaktivitásokkal szemben. Ma már közhelynek számít, hogy a kibertér teljesen megváltoztatta életmódunkat, gazdaságainkat és a társadalmi folyamatokat. A digitális forradalom kínálta előnyök sokoldalú kihasználását azonban a kibertér háborús célú felhasználásának lehetősége veszélyezteti. A kibertér az elmúlt évtizedek alatt szabályos harctérré és stratégiai prioritássá vált számos állam és nemzetközi szervezet számára. Miközben a gazdasági fejlődés és az emberi jogok tiszteletben tartása érdekében kiemelkedően fontos e terület nemzetközi szintű szabályozása, addig a támadó jellegű kibereszközök és kiberműveletek elszaporodása elkerülhetetlenné tette fokozatos militarizálódását. Nem véletlen, hogy a kibertér rendszerszintű

[1] Digwatch: *UN GGE and OEWG*. 2021.

https://doi.org/10.36250/01079_11

https://orcid.org/0000-0002-7958-6985

kockázata áll a szabályozásáról szóló többoldalú tárgyalások hátterében.[2] E fejezet célja, hogy a Magyarország szempontjából kiemelten fontos nemzetközi szervezetek, az ENSZ, az EU és a NATO kibervédelmi stratégiáit bemutassa. Emellett kitér az EU és a NATO közötti együttműködés vizsgálatára is.

Az egyre gyakoribb és nagyobb hatású számítógépes támadások a globális politikai és gazdasági kapcsolatokra is jelentős hatást gyakoroltak, és az államokat a tárgyalóasztalhoz kényszerítették. Az ENSZ Közgyűlése és Biztonsági Tanácsa, a NATO, az EU, a G7, a G20, a WTO, valamint a különböző regionális szervezetek, például az AU, az EBESZ és az ASEAN keretein belül az államok egyre inkább rákényszerültek, hogy diplomáciai lépéseket tegyenek a biztonságos kibertér megvalósítása érdekében. A modern gazdaság szinte minden területe, a kritikus infrastruktúrák és az alapvető szolgáltatások is egyre inkább az információs és kommunikációs technológiákra támaszkodnak. Mivel a kiberbiztonság a nemzetközi békére, a fenntartható fejlődésre, a digitális együttműködésre, az emberi jogokra, a magánéletre, valamint a globális digitális üzleti környezetre is kihat, így a legtöbb globális, transzatlanti és regionális nemzetközi szervezet ezzel összefüggő szakpolitikákat és intézményesített eszközöket dolgozott ki a kibertámadások egyre kifinomultabb kezelése érdekében.[3]

Az Európai Unió 2013-ban közös közleményt tett közzé kiberbiztonsági stratégiájáról. Ez volt az első kísérlet egy átfogó uniós szakpolitikai dokumentum kidolgozására ezen a területen. Az Afrikai Unió 2014-ben fogadta el a kiberbiztonságról és a személyes adatok védelméről szóló egyezményét, amely alapvetően az afrikai államok elektronikus kereskedelemre, adatvédelemre, kiberbiztonsági kormányzásra és a számítógépes bűnözés ellenőrzésére vonatkozó törvényeinek összehangolására irányult.[4]

A rosszindulatú kiberaktivitások évtizedek óta érintik a magánszemélyeket, a magánvállalkozásokat, a kormányzati intézményeket és a nem kormányzati szervezeteket. A kiberfenyegetések kiszámíthatatlan jellege miatt egy incidens, amely kezdetben hacktivizmusnak vagy pénzügyi kiberbűnözésnek tűnhet, gyorsan nagy nemzetbiztonsági kockázattá vagy akár kiberhadviselési eszközzé is

[2] Piret Pernik: *Improving Cyber Security: NATO and the EU.* International Centre for Defence Studies, 2014. szeptember.

[3] Pernik (2014): i. m.

[4] Uchenna Jerome Orji: The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability? *Masaryk University Journal of Law and Technology,* 12. (2018), 2. 91–129.; African Union: *African Union Convention on Cyber Security and Personal Data Protection.* 2014.

válhat. Annak ellenére, hogy nincs konszenzus arról, hogy pontosan mi minősül kiberháborúnak vagy kiberterrorizmusnak, a kormányoknak biztosítaniuk kell az infrastruktúrájuk védettségét és ellenállóképességét a különböző típusú kiberfenyegetésekkel szemben. A szövetségi rendszereken belüli stratégiai gondolkodást jelentős mértékben segíti, hogy jogi és intézményi rendszereik lehetővé tegyék az esetleges kibertámadások hatékony megelőzését, elrettentését, megvédését és enyhítését.[5]

2016-tól, a NATO varsói csúcstalálkozón kiadott nyilatkozata óta a kibertér is egy a műveleti területek közül.[6] A 2018-as európai uniós kibervédelmi szakpolitikai keret szerint „a kibertér az ötödik műveleti terület a szárazföld, a tenger, a légtér és a világűr mellett: az uniós missziók és műveletek végrehajtásának sikere egyre nagyobb mértékben függ a biztonságos kibertérhez való zavartalan hozzáféréstől, ezért szilárd és ellenálló kiberműveleti képességeket igényel."[7]

Az ENSZ normaalkotó szerepe

A különböző nemzetközi, regionális és nemzeti szereplők által javasolt stratégiák, a nemzetközi megállapodások, valamint a kiberbiztonsággal foglalkozó egyéb kezdeményezések jelentősen eltérhetnek terjedelmükben, céljukban és sikereikben, de mind a kibertér nemzetközi dimenzióját hangsúlyozzák. Így nem véletlen, hogy az ENSZ leszereléssel és nemzetközi biztonsággal foglalkozó Első Bizottsága *(UN First Committee, Disarmament and International Security)* évtizedek óta aktívan vizsgálja az információ és a telekommunikáció terén elért fejleményeket a nemzetközi biztonság összefüggésében. Az ENSZ a kilencvenes évek vége óta foglalkozik az információs és kommunikációs technológiák biztonságával összefüggő kérdésekkel. 2004 óta összesen hat, az ENSZ Közgyűlésének Első Bizottsága által felállított Kormányzati Szakértői Csoport (*Group of Governmental Expert* – GGE) vizsgálta az IKT-k használatával összefüggő veszélyeket. A Genfben és New Yorkban ülésező szakértői csoportok

[5] Anna-Maria Talihärm: *Towards Cyberpeace: Managing Cyberwar Through International Cooperation.* United Nations, 2013. augusztus.

[6] Fekete-Karydis Klára – Lázár Bence: A kibervédelem katonai dimenziói. *Honvédségi Szemle,* 148. (2020), 3. 47.

[7] Az Európai Unió Tanácsa: *Uniós kibervédelmi szakpolitikai keret (2018. évi naprakésszé tett változat).* Brüsszel, 2018. november 19. (OR. en) 14413/18. 2.; Molnár Anna – Szabolcs Laura: Megerősített együttműködés, változó geometria, PESCO. *Hadtudomány,* 30. (2020), 4. 77–106.

munkája az államok kibertérben megvalósuló állami viselkedési normáinak vizsgálatára, a nemzetközi jog IKT-területen történő alkalmazására és a bizalomépítő intézkedések előmozdítására összpontosított. A csoportok munkájának köszönhetően több fontos jelentés is született. A 2012–2013-as GGE-jelentés fontosságát az adta, hogy a nemzetközi jog kibertérben történő alkalmazását hangsúlyozta. Emellett kiállt az IKT és a kritikus infrastruktúrák védelme érdekében megvalósított tevékenységek területén az állami szuverenitás megerősítése mellett. A 2015-ös jelentés nem kötelező jellegű ajánlásokat fogadott el az állami magatartás nemzetközi jogi normáinak és a bizalomépítő intézkedések előmozdítása érdekében. A következő években a viták elsősorban a nemzetközi humanitárius jog (*international humanitarian law* – IHL) és a nemzetközi emberi jogi normák (*international human rights law* – IHRL) köré csoportosultak, a tárgyalások viszont – elsősorban a nyugati szövetségesek és Oroszország közötti viták miatt – elakadtak. 2017-ben a szakértői csoport végül nem tudott megegyezni egy konszenzusos jelentés megalkotásáról. A viták mélységét jól mutatja, hogy 2018-ban Antonio Guterres ENSZ-főtitkár egy beszédében hangsúlyozta: „Az államok közötti kiberhadviselés elemei már léteznek. A legroszszabb az, hogy az ilyen típusú hadviselésnek nincs szabályozási rendszere, nem világos, hogy a genfi egyezmény vagy a nemzetközi humanitárius jog hogyan vonatkozik rá."[8]

2018-ban a vitás kérdések tárgyalása érdekében az ENSZ Közgyűlése két új folyamatot indított el. A 2019 és 2021 közötti időszakban a Nyílt végű Munkacsoport (*Open-ended Working Group* – OEWG) és a Kormányzati Szakértői Csoport ülésezett. Mindkét csoport 2021 tavaszán fejezte be a munkát, és publikálta jelentéseit.[9] A OEWG 2019/2020 feladata volt az államok felelős magatartási szabályainak, normáinak és alapelveinek továbbfejlesztése, a végrehajtásuk módjának megvitatása, valamint az ENSZ égisze alatt széles körű részvétellel folytatott rendszeres intézményi párbeszéd kialakításával kapcsolatos lehetőségének tanulmányozása.[10]

A UN GGE 2019–2021-es konszenzusos jelentése a nemzetközi jog kibertérben történő alkalmazására vonatkozó alapelveket fogadott el. A jelentés kiemelte

[8] Digwatch (2021): i. m.

[9] Reaching Critical Will: *Information and communications technology (ICT)* (é. n.); Molnár Dóra: Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon. In Török Bernát (szerk.): *Információ- és kiberbiztonság.* Budapest, Ludovika Egyetemi Kiadó, 2020. 357–373.

[10] UNGA: *Resolution adopted by the General Assembly on 5 December 2018.* A/RES/73/27.

a kritikus infrastruktúrákkal – ideértve a kritikus információs és a lakosság számára alapvető szolgáltatásokat nyújtó infrastruktúrákat, az internet széles körű elérhetőségéhez szükséges infrastruktúrákat és az egészségügy működéséhez szükséges kapacitásokat – szemben alkalmazott káros IKT-tevékenységek jelentette fenyegetéseket. A 2019-es jelentés megerősíti az állami magatartás 2015-ben megalkotott nem kötelező jellegű nemzetközi jogi normáit. A dokumentum hangsúlyozza, hogy a kialakított normák nem kívánják korlátozni vagy megtiltani a nemzetközi joggal egyébként összhangban álló cselekvéseket. A normák tükrözik a nemzetközi közösség elvárásait, és meghatározzák a felelős állami magatartás szabályait. A jelentés megerősíti a nemzetközi jog és különösen az ENSZ Alapokmányának teljes alkalmazhatóságát az IKT-környezetre is. A jelentés hangsúlyozza, hogy az ENSZ Alapokmánya teljes egészében alkalmazandó, és felsorolja annak alapelveit. A GGE 2019/2021 jelentés szerint ebben az esetben a nemzetközi humanitárius jog csak fegyveres konfliktusok esetén alkalmazandó. Ez a megállapítás lényeges, hiszen a korábbi GGE-jelentések és az OEWG 2021-es jelentése nem jutott konszenzusra a kérdésben. A jelentés fontosnak tartja a nemzetközi jogi elvek (ideértve az emberiesség, a szükségesség, az arányosság és a megkülönböztetés alapelvét) alkalmazásának további vizsgálatát az IKT-k területein. A dokumentum azonban nem tesz javaslatot arra, hogy mely fórumok végezzék el ezt a vizsgálatot, noha szorgalmazza az ENSZ égisze alatti és más nemzetközi szervezetek keretein belüli, illetve a bi- vagy multilaterális tárgyalások folytatását.[11] A nemzetközi humanitárius jog alkalmazásáról szóló vitával kapcsolatban érdemes megemlíteni Tilman Rodenhäuser, a Nemzetközi Vöröskereszt nemzetközi humanitárius joggal és kiberhadviseléssel foglalkozó szakértőjének véleményét. Szerinte a nemzetközi humanitárius jog egyértelműen korlátozza a kiberműveleteket a fegyveres konfliktusok során, ugyanúgy, mint bármely (új vagy régi) fegyver, eszköz és módszer használatát. Ennek oka, hogy például egy modern kórház működésében nem csupán a hagyományos fegyverek, hanem egy kibertámadás is jelentős, akár emberéleteket követelő károkat okozhat.[12]

Ezt követően a 2021 és 2025 közötti időszakra újabb Nyílt végű Munkacsoport munkája kezdődött el.[13] Az ENSZ napjainkban is a vitás kérdések rendezésére szolgáló elsődleges és meghatározó fórum szerepét tölti be.

[11] Andrijana Gavrilović: What's New With Cybersecurity Negotiations? The UN GGE 2021 Report. *Diplo,* 2021. június 6.

[12] International Committee of the Red Cross: *Cyber Warfare: does International Humanitarian Law apply?* (2021. február 25.).

[13] Digwatch (2021): i. m.

NATO

Noha a NATO kezdetektől jelentős figyelmet fordított a kommunikációs és információs rendszereinek védelmére, csupán a 2002. évi prágai csúcstalálkozó foglalkozott először a kibervédelemmel politikai napirendjei között. A szövetség vezetői a 2006-os rigai csúcstalálkozón megerősítették az információs rendszerek védelmének szükségességét. Az észt állami és magánintézmények elleni 2007-es kibertámadásokat követően a szövetséges védelmi miniszterek egyetértettek az új kihívásokkal kapcsolatos sürgető feladatok megvalósításában. Ennek eredményeként a NATO 2008 januárjában jóváhagyta első kibervédelmi politikáját *(Policy on Cyber Defence).* 2008 nyarán az Oroszország és Grúzia közötti konfliktus ismét bebizonyította, hogy e területen további együttműködés és képességfejlesztés szükséges. Még ebben az évben létrejött a Szövetség kiválósági központjainak egyike, a tallinni székhelyű NATO Kooperatív Kibervédelmi Kiválósági Központ (*Cooperative Cyber Defence Centre of Excellence* – CCDCE).[14] A NATO folyamatosan alkalmazkodott a változó kihívásokhoz. Az adaptációs folyamatot gyorsította, hogy az USA az európai szövetségeseket megelőzve fejlesztette védelmi és támadó jellegű kiberképességeit.[15]

A NATO a 2010-es lisszaboni csúcstalálkozón új stratégiai koncepciót fogadott el. A csúcstalálkozó az Észak-atlanti Tanács (NAC) feladatául tűzte ki egy mélyreható kibervédelmi politika kidolgozását és annak végrehajtására cselekvési terv elkészítését. 2011 júniusában a NATO védelmi miniszterei jóváhagyták a második kibervédelmi politikát, amely a gyorsan változó fenyegetettség és a technológiai környezet összefüggésében vázolta fel a kibervédelem összehangolt erőfeszítéseit, és a végrehajtásra vonatkozó cselekvési terv is elkészült. 2012 áprilisában a kibervédelem a NATO védelmi tervezési folyamatába is bekerült.[16] A felkészülést segítette, hogy a tallinni kiválósági központ keretein belül 2009-től egy szakértői csoport megkezdte a nemzetközi háborús jog *(jus ad bellum)* és a nemzetközi humanitárius jog alkalmazásának vizsgálatát egy lehetséges kiberkonfliktus vagy -háború esetében. A szakértői munka eredményképpen 2013-ban elkészült *A kiberháborúra alkalmazandó nemzetközi jog tallinni kézikönyve,* az úgynevezett

[14] NATO: *Cyber Defence.* 2021a.

[15] Joe Burton: NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation. *Defence Studies,* 15. (2015), 4. 297–319.

[16] NATO (2021a): i. m.

Tallinni kézikönyv.[17] A nem kötelező jellegű dokumentum jelentős szerepet játszik a nemzetközi jogi vitás kérdések tisztázásában.

A 2012. májusi chicagói csúcstalálkozón a tagállamok állam- és kormányfői megerősítették elkötelezettségüket a szövetség kibervédelmének javítása mellett. Célul tűzték ki, hogy a NATO hálózatát központosított védelem alá helyezik. 2012 júliusában a NATO ügynökségeinek reformja során létrehozták a NATO Kommunikációs és Információs Ügynökségét (*NATO Communications and Information Agency* – NCIA). 2014 februárjában a szövetséges védelmi miniszterek egy új, fokozott kibervédelmi politika kidolgozásáról döntöttek. Az új politikai keret magában foglalta a kollektív védelem, a szövetségeseknek nyújtott segítség, az egyszerűsített kormányzás, a jogi megfontolások és az iparral fenntartott kapcsolatok területeit is.[18] A döntések jelentőségét elsősorban az adta, hogy ekkor határozták el először, hogy a Szövetség egy tagja elleni kibertámadás kollektív válaszadást igényel. Az új feladatokkal kapcsolatos nehézséget kezdetben elsősorban az okozta, hogy a kibertérben a támadás forrásának azonosítása jóval nehezebb, mint a valóságos térben.[19]

A szövetségesek a 2014. szeptemberi wales-i csúcstalálkozón jóváhagyták az új kibervédelmi politikát, és elfogadtak egy cselekvési tervet, amely a Szövetség alapfeladatainak teljesítését segíti. A kibervédelmet elismerték a NATO kollektív védelmi feladatának részeként, és egyetértettek abban, hogy a kibertérben a nemzetközi jog alkalmazandó.[20]

2016-ban a NATO és az EU technikai megállapodást kötött a kibervédelemről. 2016-ban a szövetséges védelmi miniszterek megállapodtak abban, hogy a varsói NATO-csúcstalálkozón a kiberteret műveleti területként ismerik el. A Szövetség ugyanakkor üdvözölte a más nemzetközi fórumokon tett erőfeszítéseket a felelős állami magatartás normái és a bizalomépítő intézkedések kidolgozására az átláthatóbb és stabilabb kibertér elősegítése érdekében.[21]

A szövetséges állam- és kormányfők a 2016. júliusi varsói csúcstalálkozón megerősítették a NATO védelmi feladatát, és a kiberteret olyan műveleti területnek

[17] Michael N. Schmitt (szerk.): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, Cambridge University Press, 2013; Iain Sutherland et al.: The Geneva Conventions and Cyber-Warfare. *The RUSI Journal,* 160. (2015), 4. 30–39.

[18] NATO (2021a): i. m.

[19] Burton (2015): i. m.

[20] Elie Perot: The Art of Commitments: NATO, the EU, and the Interplay Between Law and Politics Within Europe's Collective Defence Architecture. *European Security,* 28. (2019), 1. 40–65.

[21] NATO (2021a): i. m.

ismerték el, amelyben a NATO-nak ugyanolyan hatékonyan kell védekeznie, mint a levegőben, a szárazföldön és a tengeren. A szövetségesek kibervédekezésre tett kötelezettségvállalásuk mellett prioritásként fokozták a nemzeti hálózataik és infrastruktúráik kibervédelmét, és elköteleződtek amellett is, hogy gyorsan és hatékonyan reagálnak a kibertámadásokra, beleértve a hibrid kampányokat is.[22]

2017 februárjában a szövetséges védelmi miniszterek jóváhagytak egy frissített kibervédelmi akciótervet, valamint ütemtervet a kibertér mint műveleti terület megvalósítására. A miniszterek megállapodtak abban is, hogy lehetővé teszik a szövetségesek nemzeti kiber-hozzájárulásainak integrálását a szövetség műveleteibe és misszióiba.[23] 2017 decemberében a NATO és az EU miniszterei megállapodtak a két szervezet közötti együttműködés fokozásáról számos területen, ideértve a kiberbiztonságot és a kibervédelmet is. 2017-ben a tallinni kiválósági központ keretein belül megszületett a *Tallinni kézikönyv 2.0,* amely elsősorban a napi rendszerességgel megvalósuló kiberincidensek esetében alkalmazandó nemzetközi jog területeit vizsgálta.[24]

A szövetséges vezetők a 2018-as brüsszeli csúcstalálkozón megállapodtak egy új kibertérműveleti központ felállításáról a NATO megerősített parancsnoki struktúrájának részeként. A cél a NATO kibervédelmének megerősítése és a kiberterület integrálása a NATO tervezésébe és műveleteibe minden szinten. A szövetségesek abban is egyetértettek, hogy a NATO missziói és műveletei során felhasználhatja a nemzeti kiberképességeket. A szövetségesek számba vették a nemzeti ellenállóképesség fokozása érdekében tett lépéseiket.[25]

2019 februárjában a NATO védelmi miniszterei jóváhagyták az új útmutatót, amely a NATO képességeit megerősítő eszközöket tartalmaz a jelentős rosszindulatú kiberaktivitások esetére.[26]

A NATO-nak minden rendelkezésére álló eszközt fel kell használnia, beleértve a politikai, diplomáciai és katonai intézkedéseket is, a kiberfenyegetések leküzdésére. Az útmutatóban felvázolt válaszlehetőségek segíteni fogják a NATO-t és szövetségeseit abban, hogy fokozzák a kibertérben zajló helyzettel

[22] NATO: *Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw* (2016. július 8–9.).

[23] NATO (2021a): i. m.

[24] NATO CCDCOE: *The Tallinn Manual.* Tallinn, 2021; Michael N. Schmitt (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press, 2017.

[25] NATO (2021a): i. m.

[26] Laura Brent: *NATO's Role in Cyberspace*. NATO, 2019. február 12.

kapcsolatos tudatosságukat, növeljék ellenállóképességüket, és a partnerekkel együttműködve elrettentsék, kivédjék és ellensúlyozzák a kiberfenyegetések teljes spektrumát.[27]

Az Észak-atlanti Tanács 2020. június 3-án nyilatkozatot adott ki, amelyben elítélte a koronavírus-járvány összefüggésében zajló destabilizáló és rosszindulatú kibertevékenységeket. A nyilatkozatban a szövetségesek szolidaritását és kölcsönös támogatását fejezte ki azok számára, akik e rosszindulatú kibertevékenységek következményeit elszenvedik, beleértve az egészségügyi szolgáltatásokat, a kórházakat és a kutatóintézeteket. A nyilatkozat felszólította továbbá a nemzetközi jog és a felelős állami magatartás normáinak betartását a kibertérben.[28]

2021-ben a tallinni kiválósági központ keretein belül megkezdődött a *Tallinni kézikönyv 3.0* kidolgozása. Az ötéves projekt célja a meglévő fejezetek átdolgozása és a tagállamok számára fontos új témák vizsgálata.[29] A 2021. júniusi brüsszeli csúcstalálkozón a szövetségesek tudomásul vették a változó fenyegetettséget, és új átfogó kibervédelmi politikát fogalmaztak meg a NATO három alapvető feladatának, a kollektív védelemnek, a válságkezelésnek és a kooperatív biztonságnak a támogatására. A döntéseknek megfelelően a NATO-nak mindenkor – békeidőben, válságban és konfliktusok idején is, valamint politikai, katonai és technikai szinten is – aktívan el kell hárítania a kiberfenyegetések teljes spektrumát, védekeznie kell ellenük, és szembe kell néznie velük.[30]

Az Európai Unió[31]

Az EU első átfogó kiberbiztonsági stratégiájának kidolgozására 2013-ban került sor.[32] E dokumentum említette először az EU nemzetközi kiberbiztonsági politikáját és kibervédelmi céljait. A NATO hasonló stratégiáival összehasonlítva

[27] NATO (2021a): i. m.
[28] NATO (2021a): i. m.
[29] CCDCOE (2021): i. m.
[30] NATO (2021a): i. m.
[31] Az Európai Unió kiberbiztonsági politikájának fejlődéséről részletesebben lásd Molnár Dóra: Egységes európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése. *Hadmérnök,* 12. (2017), 1. 255–267.
[32] Európai Bizottság: *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.* JOIN/2013/01 final. 2013.

(2008, 2011) az uniós dokumentum nem csupán a saját informatikai hálózatának védelmére szorítkozott, hanem szinte minden uniós kompetenciába tartozó területre – az egységes piactól a külső és belső biztonság kérdéseiig – kiterjedt.[33] Míg a NATO kezdetektől inkább a keményebb stratégiai eszközök elfogadását tartotta fontosnak, addig az EU a puha szakpolitikai keret megvalósítására összpontosított.[34] A kiberbiztonság területe csak fokozatosan vált védelmi jellegű kérdéssé.[35]

A 2013-as stratégia az EU nemzetközi kiberpolitikájával kapcsolatos céljait is meghatározta. Az új szakpolitika a szabad és nyitott internet védelme mellett célul tűzte ki a felelősségteljes állami magatartás nemzetközi jogi normáinak és a bizalomépítő intézkedések előmozdítását a kibertérben és az EU stratégiai partnereivel történő együttműködés javítását. Az uniós kiberdiplomácia részeként számos nagyhatalommal tárgyalások kezdődtek a kibertérben zajló nemzetközi biztonság, az ellenállóképesség, a kiberbűnözés elleni fellépés és az internet szabályozása érdekében. E folyamatokkal párhuzamosan az Európai Unión belüli, kiberbiztonsággal összefüggő diplomáciai eszköztár megerősítése is szükségessé vált, és egyre intenzívebb lett e terület szabályozási folyamata.

Az EU 2016-os globális stratégiája a kiberdiplomáciával kapcsolatos alapvető célokat is megfogalmazta.[36] Az unió 2016-ban meghozta az első kiberbiztonságra vonatkozó uniós jogi aktust, a hálózati és információs rendszerek biztonságáról szóló irányelvet (NIS).[37] Az Európai Bizottság irányításával 2017-ben elkészült az EU új, felülvizsgált kiberbiztonsági stratégiája.[38]

Az unió érdekeinek átfogó védelme érdekében 2017-ben az EU Tanácsa megállapodott arról, hogy az állami és nem állami szereplők részéről mutatkozó rossz szándékú és tudatos kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretét, az úgynevezett kiberdiplomáciai eszköztárat *(EU Cyber-diplomacy Toolbox)* kidolgozza. Az új eszköztár az EU közös kül- és bizton-

[33] Jochen Rehrl (szerk.): *Handbook on cyber security. The Common Security and Defence Policy of the European Union.* Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2018. 18.

[34] Burton (2015): i. m.

[35] James Sperling – Mark Webber: The European Union: security governance and collective securitisation. *West European Politics,* 42. (2019), 2. 228–260.

[36] Európai Külügyi Szolgálat: *Közös jövőkép, közös fellépés: Erősebb Európa. Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan.* 2016. 35.

[37] Eur-lex: *Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve* (2016. július 6.).

[38] Európai Bizottság: *Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése".* Brüsszel, 2017. szeptember 13. JOIN(2017) 450 final.

ságpolitikai eszköztárára támaszkodik. A tanácsi döntéssel összhangban azon információs és kommunikációs technológiák (IKT) felhasználásával végrehajtott tevékenységekkel szemben, amelyek kimeríthetik a nemzetközi jogot sértő cselekmény fogalmát, az EU kész a közös kül- és biztonságpolitikai intézkedésekkel, ideértve a korlátozó, esetleg szankciós intézkedéseket is, fellépni.[39] Döntés született arról is, hogy az alkalmazott intézkedéseknek – a nemzetközi joggal összhangban – arányosnak kell lenniük a rossz szándékú kibertevékenységgel. Az EU egyúttal megerősítette, hogy „elkötelezett a kibertérben folyó nemzetközi viták békés úton történő rendezése mellett".[40]

A Politikai és Biztonsági Bizottság 2017. október 11-én a kiberdiplomáciai eszköztárra vonatkozóan végrehajtási iránymutatásokat fogadott el. A dokumentum a kiberdiplomáciai eszköztáron belül *öt intézkedéskategóriát* sorolt fel: *1.* a megelőző intézkedéseket, *2.* az együttműködési intézkedéseket, *3.* a stabilitást szolgáló intézkedéseket, *4.* a korlátozó intézkedéseket és *5.* a lehetséges uniós támogatást a tagállamok jogszerű válaszaihoz. A dokumentum tartalmazza az ezen intézkedések bevezetésére vonatkozó eljárást is.[41] A lehetséges uniós támogatások között a dokumentum a lisszaboni szerződés kölcsönös segítségnyújtási klauzuláját (42.7 cikk) is megemlíti.[42] E klauzula alkalmazásának lehetősége az EU kollektív védelmi jellegét erősíti a kiberbiztonság területén is.

A 2018-as kibervédelmi szakpolitikai keret szerint a korábbi évek eseményei még inkább rávilágítottak arra a tényre, hogy a nemzetközi közösségnek együtt kell működnie a konfliktusok megelőzése és a kibertér stabilitásának erősítése érdekében.

> „Az EU más nemzetközi szervezetekkel, elsősorban az ENSZ-szel (Egyesült Nemzetek Szervezete), az EBESZ-szel (Európai Biztonsági és Együttműködési Szervezet) és az ASEAN (Délkelet-ázsiai Nemzetek Szövetsége – Association of Southeast Asian Nation) regionális fórummal együtt elő kívánja mozdítani egy olyan, a konfliktusmegelőzésre, az együttműködésre és a kibertér stabilitásának erősítésére vonatkozó stratégiai keretet, amely magában foglalja a következőket: a nemzetközi jognak és különösen

[39] Az Európai Unió Tanácsa: *Informatikai támadások: az EU készen áll az ellenintézkedésekre, ideértve a szankciókat is.* 2017.

[40] Európai Unió Tanácsa (2017): i. m.

[41] Council of the European Union: *Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities – Approval of the Final Text.* Brussels, 2017b. október 9. (OR. en); A Tanács (KKBP) 2019/797 határozata (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről.

[42] Európai Unió Tanácsa (2017): i. m.

> az ENSZ Alapokmányának teljes körű alkalmazása a kibertérben; a kibertérben tanúsított felelősségteljes állami magatartásra vonatkozó egyetemes, nem kötelező erejű normák, szabályok és elvek tiszteletben tartása; regionális bizalomépítő intézkedések kidolgozása és végrehajtása. Ezt a törekvést az uniós kibervédelmi szakpolitikai keretnek is támogatnia kell."[43]

2019-ben az EU jelentős előrehaladást ért el a rossz szándékú kibertevékenységekkel szembeni közös uniós kiberdiplomáciai eszköztár működőképessé és hatékonnyá tétele érdekében. Az Európai Tanács 2018. júniusi és 2018. októberi következtetéseiben megfogalmazott célok elérése érdekében olyan uniós korlátozó intézkedések bevezetéséről döntött, amelyek segítik a kibertámadásokkal kapcsolatos reagálási és elrettentési képesség javítását. 2019. május 17-én döntés született az uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló KKBP-határozatról[44] és a tanácsi rendeletről.[45] A határozat a rossz szándékú és szándékos kibertevékenységekkel szembeni közös uniós korlátozó intézkedések alkalmazhatóságáról döntött, a rendelet pedig a jelentős hatású kibertámadások esetén szankciók alkalmazását teszi lehetővé az EU részéről.

Az új jogi keret így már lehetővé tette az EU számára, hogy szankciókat is kivethessen (például eszközök befagyasztása, utazási tilalom) az unióra vagy a tagállamaira külső fenyegetést jelentő kibertámadásoktól való elrettentés, valamint az azokra való reagálás érdekében.[46] A szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük (A Tanács [EU] 2019/796 rendelete 15. cikk). 2019-ben megszületett az EU új kiberbiztonsági jogszabálya, illetve megújult az Európai Uniós Kiberbiztonsági Ügynökség, az ENISA, és kibővült a hatásköre.[47]

2020 decemberében elkészült az Európai Bizottság és az Európai Külügyi Szolgálat új uniós kiberbiztonsági stratégiája. A stratégia célja a kiberfenyegetésekkel szembeni ellenállóképesség megerősítése, valamint a polgárok

[43] Az Európai Unió Tanácsa (2018): i. m. 8.

[44] A Tanács (KKBP) 2019/797 határozata… i. m.

[45] A Tanács (EU) 2019/796 rendelete… i. m.

[46] Európai Bizottság: *Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról. Közös közlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának*. Brüsszel, 2019. június 14. JOIN (2019) 12 final, 9.

[47] Council of the European Union: *Cybersecurity in Europe: stronger rules and better protection.* 2020.

és a vállalkozások számára megbízható szolgáltatások és digitális eszközök biztosítása.[48] A stratégia hangsúlyozza, hogy az EU hatékony diplomáciai reagálásához szilárd, közös helyzetismeretre és a közös uniós álláspont gyors előkészítésére van szükség. Az unió külügyi és biztonságpolitikai főképviselője ösztönzi a tagállamok kiberfenyegetésekkel és -tevékenységekkel kapcsolatos stratégiai hírszerzési együttműködését. Annak érdekében, hogy az EU megakadályozza, elriassza és reagáljon a virtuális térben történő rosszindulatú tevékenységekre, a főképviselő a Bizottság bevonásával javaslatot terjeszt elő az EU számára, hogy meghatározza a kiberelrettentési képességeit. Az EU-nak további erőfeszítéseket kell tennie a nemzetközi partnerekkel, köztük a NATO-val való együttműködés megerősítése érdekében a fenyegetettség közös megértésének előmozdítása, az együttműködési mechanizmusok kidolgozása és az együttműködő diplomáciai válaszok meghatározása érdekében. Ezenkívül az EU-nak tovább kell integrálnia a kiberdiplomácia eszköztárát az EU válságmechanizmusaiba, szinergiákat kell keresnie a hibrid fenyegetések, a dezinformációk és a külföldi beavatkozások elleni küzdelemre irányuló erőfeszítésekkel. Az EU-nak tükröznie kell a kiberdiplomáciai eszköztár és az EUSZ 42. cikk (7) és (EUMSZ) 222. cikk közötti lehetséges kölcsönhatásokat.[49]

A Tanács a 2021. márciusi, a kiberbiztonsági stratégiáról szóló következtetéseiben hangsúlyozta, hogy a kiberbiztonság alapvető fontosságú a reziliens, zöld és digitális Európa építéséhez. Az uniós miniszterek a nyitott gazdaság megőrzése mellett a stratégiai autonómia megvalósítását is célul tűzték ki annak érdekében, hogy az EU a kiberbiztonság területén autonóm döntéseket hozhasson.[50]

Az EU–NATO-együttműködés

Noha a NATO továbbra is a kollektív védelem elsődleges szervezete a szövetségesek számára, az EU is fontos szerepet tölthet be egy jelentős kibertámadás esetén.

[48] European Commission (2020): *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 2020. december 16. JOIN(2020) 18 final.

[49] European Commission (2020): i. m. 16–17.

[50] Az Európai Unió Tanácsa: *A Tanács következtetései a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról.* Brüsszel, 2021. március 9. (OR. en) 6722/21.

Az európai szövetségesek a NATO 5. cikke vagy az EUSZ 42.7 cikke (mint „fegyveres támadás/agresszió") keretében vagy az EU működéséről szóló szerződés 222. cikke (szolidaritási klauzula) keretei között (mint „terrortámadás") nyújthatnak segítséget egymásnak. Az EUMSZ 222. cikkével összefüggésben az EU 2013. évi kiberbiztonsági stratégiája szerint egy különösen súlyos számítógépes esemény vagy támadás elegendő feltétele, hogy egy tagállam az EU szolidaritási záradékára hivatkozhasson. A NATO 5. cikkével kapcsolatban a Szövetség walesi csúcstalálkozója döntött. Ennek megfelelően egy kibertámadás „fegyveres támadásnak" minősülhet.[51] Az EU 2017-es kiberdiplomáciai eszköztára a lisszaboni szerződés kölcsönös segítségnyújtási klauzuláját (42.7 cikk) is megemlíti a válaszadási lehetőségek között.

A NATO és az EU közötti intenzívebb kapcsolatok kiépítésére a 2010-es évektől került sor. A 2015-ös kiberdiplomáciáról szóló tanácsi következtetésekkel összhangban az EU a legfontosabb partnerekkel és a nemzetközi szervezetekkel stratégiai együttműködést kíván kialakítani, és hangsúlyozza, hogy a kibertérrel kapcsolatos kérdésekben hozott szakpolitikai döntések többsége szükségessé teszi az aktív nemzetközi párbeszédet, együttműködést és koordinációt.[52] Mindezzel összefüggésben a NATO-val kiépített kapcsolatok jelentősége is fokozatosan növekedett.

Az EU és a NATO közötti együttműködés területén kialakított folyamat valódi lendületet 2016-tól kapott. Az EU globális stratégiájának elfogadását követő végrehajtási folyamatban a két nemzetközi biztonsági szervezet között a kiberbiztonság és kibervédelem területén egyre intenzívebb kapcsolat jött létre.[53] A globális stratégia hangsúlyozta, hogy míg a NATO a kollektív védelem elsődleges keretét biztosítja a legtöbb tagállam számára, addig az EU elsősorban az olyan belső és külső kihívásokkal szemben kíván fellépni, mint a terrorizmus, a hibrid fenyegetések, a kiber- és energiabiztonság, a szervezett bűnözés és a külső határok igazgatása.

2016. július 8-án a NATO-csúcson Varsóban az EU részéről az Európai Tanács elnöke és az Európai Bizottság elnöke, illetve a NATO főtitkára együttes nyilatkozatot írt alá az EU és a NATO közötti együttműködésről. A nyilatkozat aláírását követően a két szervezet közötti együttműködés új lendületet kapott,

[51] Perot (2019): i. m.

[52] Az Európai Unió Tanácsa: *A Tanács következtetései a kiberdiplomáciáról.* Brüsszel, 2015. február 11.

[53] Európai Külügyi Szolgálat (2016): i. m.

és kiterjed a hibrid fenyegetések elleni küzdelemre, a kiberbiztonság és -védelem területeire is.[54] Az együttes nyilatkozat konkrét célkitűzéseket fogalmazott meg a kibervédelmi együttműködés előmozdítása érdekében: a kibervédelmi interoperabilitás megerősítése a missziók és a műveletek során; az együttműködés erősítése a képzéseken és a gyakorlatokon; a kibervédelmi kutatásokkal és technológiai innovációval kapcsolatos együttműködés előmozdítása; valamint a kibernetikus szempontok beépítése a válságkezelésbe.[55]

2016 februárjában az EU és a NATO képviselői aláírták az EU hálózatbiztonsági vészhelyzeteket elhárító csoportja (*Computer Emergency Response Teams* – CERT) és a NATO hálózatbiztonsági incidenskezelő csoportja (*NATO's Computer Incident Response Capability* – NCIRC) közötti technikai megállapodást. A megállapodás célja a technikai információk megosztásának megkönnyítése a számítógépes események megelőzése érdekében, illetve a kiberbiztonsági események felderítése és az azokra való reagálás erősítése mindkét szervezetben. Az e területeken megvalósuló tevékenységek mind a mai napig a két szervezet közötti együttműködés alapját képezik.

Az együttműködés másik legfontosabb eredménye, hogy – finn kezdeményezésre, de az EU és a NATO támogatásával – 2017-ben Helsinkiben létrejöhetett a Hibrid Fenyegetések Elleni Kiválósági Központ *(European Centre of Excellence for Countering Hybrid Threats),* amelynek feladata az elsősorban Oroszország felől érkező kiberbiztonsági kihívások, a dezinformációs műveletek és a stratégiai kommunikáció elemzése, valamint a kihívásokra hatékony és közösen koordinált válaszok kidolgozása.[56] Az új központ felállítása lehetőséget biztosított az Észak-atlanti Tanács és az uniós Politikai és Biztonsági Bizottság közötti informális találkozók megszervezésére, és így a hibrid fenyegetéssel szembeni koordinált fellépés kidolgozására.[57]

A NATO és az EU közötti együttműködést vizsgáló 2017. novemberi második előrehaladási jelentésben első helyen szerepelt az új központ felállítása. A jelentés emellett kiemelte a kiberbiztonsági és a védelmi fejlesztés területén elért eredményeket, illetve ezek közül a képzések és gyakorlatok területén megvalósuló

[54] Az Európai Unió Tanácsa: *EU–NATO együttműködés: A Tanács következtetéseket fogadott el az együttes nyilatkozat végrehajtása céljából.* 2016.

[55] Council of the European Union: *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation.* 2016.

[56] Hybrid CoE: *European Centre of Excellence for Countering Hybrid Threats.* (É. n.)

[57] Hybrid CoE: Hybrid CoE Supports Informal NAC-PSC Discussion. 2018. szeptember 28.

együttműködések fontosságát. A NATO-alkalmazottak például részt vehettek az uniós ügynökség, az ENISA (*European Union Agency for Cybersecurity,* Európai Uniós Kiberbiztonsági Ügynökség) kiberbiztonsági gyakorlatán. Ezt követően a fejlesztési duplikációk elkerülése érdekében folyamatossá vált az együttműködés.[58]

2017-ben és 2018-ban a NATO és az Európai Unió párhuzamos és összehangolt gyakorlatokat folytatott egy hibrid forgatókönyvre reagálva, annak érdekében, hogy javítsák az EU válaszadási képességét a hibrid fenyegetés esetén, és továbbfejlesszék az EU és a NATO közötti együttműködést. 2017-ben NATO-irányítással, 2018-ban pedig az unió vezetésével hajtották végre a gyakorlatokat. A 2018-as „EU-HEX-ML 18 (PACE)" gyakorlat jelentősen segítette a szervezetek személyi állománya közötti együttműködést.[59] 2017-ben a Tallinnban szervezett közös kibergyakorlat során a NATO és az EU tisztviselői a NATO 5. cikkének vagy az EUSZ 42.7 cikknek az aktiválást is tárgyalták.[60] 2019-ben a jól bevált gyakorlat folytatódott, és a NATO CMX 19 gyakorlat is kiterjedt a személyi állományok közötti együttműködésre az EU intézményeivel (EKSZ, EK és a Tanács).[61]

A 2021-es hatodik előrehaladási jelentés hangsúlyozta, hogy az EU és a NATO személyzete rendszeres kapcsolatot és információcserét tartott fenn az egyes kibertevékenységekkel kapcsolatban. Az együttműködés a koronavírus-járvány idején is hatékonynak bizonyult. 2021 májusában az EU Integrated Resolve 20 (EU IR20) gyakorlat keretében is folytatódott a személyi állományok közötti együttműködés. Az EU és a NATO kiberbiztonsági és védelmi személyzetének éves megbeszéléseit 2021 januárjában tartották, és lehetőséget kínáltak az aktuális szakpolitikai fejlemények és prioritások aktualizálására, egyúttal felmérve a további együttműködés lehetőségeit.[62]

[58] Council of the European Union: *Second Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU.* 2017a.

[59] European External Action Service: *Crisis Preparedness: EU Launches Civil-Military Crisis Management Exercise.* Bruxelles, 2018. november 16. – 15:25, UNIQUE ID: 181116_7.

[60] Perot (2019): i. m.

[61] George Allison: NATO Conducts Crisis Management Exercise. *UK Defence Journal,* 2019. május 9.

[62] NATO: *Sixth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.* 2021b. június 3. 5–6.; Molnár Anna: A kiberdiplomácia fejlődése az Európai Unióban. In Molnár Anna – Molnár Dóra (szerk.): *Kiberdiplomácia.* Budapest, Ludovika Egyetemi Kiadó, 2022. 55–71.

Következtetések

A 2000-es évek elejétől az ENSZ meghatározott szerepet játszott a kiberhadviseléssel kapcsolatos nemzetközi jogi viták rendezése és a jogi normák megalkotása területén. 2007 után, az észt magán- és közintézmények, illetve infrastruktúra ellen elkövetett orosz eredetű elosztott szolgáltatásmegtagadással járó támadásokat (DDoS) követően az EU és a NATO egyre nagyobb hangsúlyt fektetett az információ- és hálózatbiztonság megerősítésére. Napjainkban a kibertér a nemzetközi kapcsolatok kiemelt területévé vált. Ez az új szegmens nemcsak a nemzeti, tagállami szintű stratégiaalkotásban[63] öltött testet, hanem az elmúlt évtizedekben nemzetközi szervezetek, szövetségi rendszerek is megkezdték a kiberdiplomáciával és a kibervédelemmel összefüggő eszköz- és intézményrendszereik kiépítését.

E területen a Magyarország számára kiemelkedően fontos két nemzetközi szervezet, az EU és a NATO élen járt. Míg a NATO elsősorban a katonai és védelmi területre összpontosított, addig az EU *sui generis* (azaz egyedi) jellegéből fakadóan a gazdaság, illetve a külső és belső biztonság minden területére kiterjedő, átfogó kiberbiztonsági megközelítést alkalmazott. Az Európai Unióhoz hasonlóan egyre több tagállam alkalmazta ezt a fajta átfogó megközelítést, a leglátványosabban először Németország, a gazdasági összetevőkre helyezve a hangsúlyt.[64]

Irodalomjegyzék

African Union: *African Union Convention on Cyber Security and Personal Data Protection.* 2014. Online: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Allison, George: NATO Conducts Crisis Management Exercise. *UK Defence Journal,* 2019. május 9. Online: https://ukdefencejournal.org.uk/nato-conducts-crisis-management-exercise/

[63] A nemzeti szintű kiberstratégiaalkotás kérdéseivel részletesen foglalkozik Molnár Dóra kismonográfiájában. Lásd Molnár Dóra: *Törékeny nagyhatalmiság: a kiberbiztonság. Az európai kibertér brit, német és francia szegmensei.* Budapest, Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 2019.

[64] Lásd ehhez Molnár Dóra: Kiberbiztonság Németországban. Pillanatkép a német digitális térről. *Nemzet és Biztonság,* 11. (2018), 1. 142–156.

A Tanács (EU) 2019/796 rendelete (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.HUN&toc=OJ:L:2019:129I:TOC5

A Tanács (KKBP) 2019/797 határozata (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019D0797&from=EN

Az Európai Unió Tanácsa: *A Tanács következtetései a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról.* Brüsszel, 2021. március 9. (OR. en) 6722/21. Online: https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/hu/pdf

Az Európai Unió Tanácsa: *A Tanács következtetései a kiberdiplomáciáról.* Brüsszel, 2015. február 11. Online: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf

Az Európai Unió Tanácsa: *EU–NATO együttműködés: A Tanács következtetéseket fogadott el az együttes nyilatkozat végrehajtása céljából.* 2016. Online: www.consilium.europa.eu/hu/press/press-releases/2016/12/06/eu-nato-joint-declaration/

Az Európai Unió Tanácsa: *Informatikai támadások: az EU készen áll az ellenintézkedésekre, ideértve a szankciókat is.* 2017. Online: www.consilium.europa.eu/hu/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

Az Európai Unió Tanácsa: *Uniós kibervédelmi szakpolitikai keret (2018. évi naprakésszé tett változat).* Brüsszel, 2018. november 19. (OR. en) 14413/18. Online: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hu/pdf

Brent, Laura: *NATO's Role in Cyberspace.* NATO, 2019. február 12. Online: www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

Burton, Joe: NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation. *Defence Studies,* 15. (2015), 4. 297–319. Online: https://doi.org/10.1080/14702436.2015.1108108

Council of the European Union: *Cybersecurity in Europe: stronger rules and better protection.* 2020. www.consilium.europa.eu/en/policies/cybersecurity/

Council of the European Union: *Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities – Approval of the Final Text.* Brussels, 2017b. október 9. Online: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf

Council of the European Union: *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation*. 2016. Online: www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf

Council of the European Union: *Second Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU.* 2017a. Online: www.consilium.europa.eu/media/35577/report-ue-nato-layout-en.pdf

Digwatch: *UN GGE and OEWG.* 2021. Online: https://dig.watch/processes/un-gge

Eur-lex: *Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve* (2016. július 6.). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016L1148

Európai Bizottság: *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.* JOIN/2013/01 final. 2013. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52013JC0001

Európai Bizottság: *Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról. Közös közlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának.* Brüsszel, 2019. június 14. JOIN (2019) 12 final. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52019JC0012&from=EN

Európai Bizottság: *Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése".* Brüsszel, 2017. szeptember 13. JOIN(2017) 450 final. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=en

Európai Külügyi Szolgálat: *Közös jövőkép, közös fellépés: Erősebb Európa. Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan.* 2016. Online: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_hu_.pdf

Európai Parlament: *Az Európai Parlament állásfoglalására irányuló indítvány a kibervédelemről*. 2018. Online: www.europarl.europa.eu/doceo/document/A-8-2018-0189_HU.html

European Commission: *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 2020. december 16. JOIN(2020) 18 final. Online: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European External Action Service: *Crisis Preparedness: EU Launches Civil-Military Crisis Management Exercise.* Bruxelles, 2018. november 16. – 15:25, UNIQUE ID: 181116_7. Online: https://eeas.europa.eu/headquarters/headquarters-Homepage/53926/crisis-preparedness-eu-launches-civil-military-crisis-management-exercise_en

Fekete-Karydis Klára – Lázár Bence: A kibervédelem katonai dimenziói. *Honvédségi Szemle,* 148. (2020), 3. 44–54. Online: https://doi.org/10.35926/HSZ.2020.3.4

Gavrilović, Andrijana: What's New With Cybersecurity Negotiations? The UN GGE 2021 Report. *Diplo,* 2021. június 6. Online: www.diplomacy.edu/blog/whats-new-cybersecurity-negotiations-un-gge-2021-report

Hybrid CoE: *European Centre of Excellence for Countering Hybrid Threats* (é. n.). Online: www.hybridcoe.fi/

Hybrid CoE: *Hybrid CoE Supports Informal NAC-PSC Discussion.* 2018. szeptember 28. Online: www.hybridcoe.fi/news/hybrid-coe-supports-informal-nac-psc-discussion/

International Committee of the Red Cross: *Cyber Warfare: does International Humanitarian Law apply?* (2021. február 25.). Online: www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law

Molnár Anna: A kiberdiplomácia fejlődése az Európai Unióban. In Molnár Anna – Molnár Dóra (szerk.): *Kiberdiplomácia.* Budapest, Ludovika Egyetemi Kiadó, 2022. 55–71.

Molnár Anna – Szabolcs Laura: Megerősített együttműködés, változó geometria, PESCO. *Hadtudomány,* 30. (2020), 4. 77–106. Online: http://real.mtak.hu/124268/1/077-106_Molnar_Szabolcs.pdf

Molnár Dóra: Egységes európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése. *Hadmérnök,* 12. (2017), 1. 255–267. Online: http://hadmernok.hu/171_20_molnar2.pdf

Molnár Dóra: Kiberbiztonság Németországban. Pillanatkép a német digitális térről. *Nemzet és Biztonság,* 11. (2018), 1. 142–156. Online: www.nemzetesbiztonsag.hu/cikkek/neb_2018-01-09_molnar_dora_-_kiberbiztonsag_nemetorszagban-pillanatkep_a_nemet_digitalis_terrol.pdf

Molnár Dóra: Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon. In Török Bernát (szerk.): *Információ- és kiberbiztonság.* Budapest, Ludovika Egyetemi Kiadó, 2020. 357–373.

Molnár Dóra: *Törékeny nagyhatalmiság: a kiberbiztonság. Az európai kibertér brit, német és francia szegmensei.* Budapest, Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 2019.

NATO: *Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw* (2016. július 8–9.). Online: www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO: *Cyber Defence.* 2021a. Online: www.nato.int/cps/en/natohq/topics_78170.htm

NATO: *Sixth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.* 2021b. június 3. Online: www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf

NATO CCDCOE: *The Tallinn Manual.* Tallinn, 2021. Online: https://ccdcoe.org/research/tallinn-manual/

Orji, Uchenna Jerome: The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability? *Masaryk University Journal of Law and Technology,* 12. (2018), 2. 91–129. Online: https://doi.org/10.5817/MUJLT2018-2-1

Pernik, Piret: *Improving Cyber Security: NATO and the EU.* International Centre for Defence Studies, 2014. szeptember. Online: https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf

Perot, Elie: The Art of Commitments: NATO, the EU, and the Interplay Between Law and Politics Within Europe's Collective Defence Architecture. *European Security,* 28. (2019), 1. 40–65. Online: https://doi.org/10.1080/09662839.2019.1587746

Reaching Critical Will: *Information and communications technology (ICT)* (é. n.). Online www.reachingcriticalwill.org/disarmament-fora/ict

Rehrl, Jochen (szerk.): *Handbook on cyber security. The Common Security and Defence Policy of the European Union*. Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2018. Online: https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1

Schmitt, Michael N. (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press, 2017.

Schmitt, Michael N. (szerk.): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, Cambridge University Press, 2013.

Sperling, James – Mark Webber: The European Union: security governance and collective securitisation. *West European Politics,* 42. (2019), 2. 228–260. Online: https://doi.org/10.1080/01402382.2018.1510193

Sutherland, Iain – Konstantinos Xynos – Andrew Jones – Andrew Blyth: The Geneva Conventions and Cyber-Warfare. *The RUSI Journal,* 160. (2015), 4. 30–39. Online: https://doi.org/10.1080/03071847.2015.1079044

Talihärm, Anna-Maria: *Towards Cyberpeace: Managing Cyberwar Through International Cooperation*. United Nations, 2013. augusztus. Online: www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation

UNGA: *Resolution adopted by the General Assembly on 5 December 2018*. A/RES/73/27. Online: https://undocs.org/A/RES/73/27