Molnár Anna

A kiberdiplomácia fejlődése az Európai Unióban

Bevezetés

Noha az Európai Unió (a továbbiakban: EU) már a kilencvenes évek második felétől megkezdte a számítástechnikával és az elektronikus kommunikációval kapcsolatos tevékenységeinek fejlesztését, az átfogó megközelítésre építő kiberbiztonsági szakpolitikai keret- és intézményrendszer kiépítése valójában csak az elmúlt évtizedben kezdődött el. Az egyénekkel, vállalatokkal és a kritikus infrastruktúrákkal szembeni növekvő számú kibertámadások egyre inkább felhívták a figyelmet a kibertérrel kapcsolatos fenyegetésekre és kockázatokra. Tekintettel arra, hogy a számítógépes bűnözés nem ismeri a nemzeti határokat, e területen is szükségessé vált az uniós szintű együttműködés feltételrendszerének kiépítése. Ezt a folyamatot jogi intézkedések elfogadása (például az információs rendszerek elleni támadásokról szóló 2005. évi tanácsi kerethatározat) és új intézményi struktúrák létrehozása (például az Európai Hálózat- és Információbiztonsági Ügynökség – ENISA 2004-ben és az Europolban a számítástechnikai bűnözéssel foglalkozó európai központ, az EC3 megalapítása 2013-ban) jelezte.[1] E tanulmány célja, hogy átfogó képet nyújtson az EU-s kiberdiplomáciával összefüggő intézményi struktúrákról és stratégiai keretekről.

2007 után az észt magán- és közintézmények, illetve infrastruktúra ellen elkövetett orosz eredetű elosztott szolgáltatásmegtagadással járó támadásokat (DDoS) követően az EU egyre nagyobb hangsúlyt fektetett az információ- és hálózatbiztonság megerősítésére. Napjainkra a kibertér a nemzetközi kapcsolatok kiemelt területévé vált, és az uniós külpolitika szerves részét képezik a kiberdiplomáciával kapcsolatos területek. Az Európai Unió is megkezdte a kiberdiplomáciával és a kibervédelemmel összefüggő eszköz- és intézményrendszerének kiépítését.

[1] Helena Carrapico – Andre Barrinha: European Union Cyber Security as an Emerging Research and Policy Field. *European Politics and Society,* 19. (2018), 3. 299–303.

https://doi.org/10.36250/01008_03

Az uniós intézmények és infrastruktúra elleni egyre célzottabb és nagyszabású kibertámadások arra késztették a döntés-előkészítőket és döntéshozókat, hogy a hatáskörükbe tartozó főbb tevékenységek mindegyikére kiterjedő átfogó kiberbiztonsági politikát fejlesszenek. Az EU-ról szóló szerződés 3. cikke sorolja fel az unió céljait és tevékenységeinek főbb területeit. Ezek közül kiemelhető az egységes piac megvalósítása, a szabadság, biztonság és jog térségének kialakítása és a közös kül- és biztonságpolitika megvalósítása. A 2010-es évektől megkezdődött a kiberbiztonsággal és kibervédelemmel összefüggő többszintű kormányzás uniós szintű eszköz- és intézményrendszerének a kiépülése.[2] Ennek fontos elemeként a kiberdiplomáciával összefüggő tevékenységek elsősorban a közös kül- és biztonságpolitikát, és az annak szerves részét képező közös biztonság- és védelempolitika területeit érintik, de a közös piaccal és a szabadság, biztonság és jog térségének kialakításával összefüggő kiberbiztonsági kérdések nemzetközi szintű képviselete is ide tartozik.

Számos, az EU kiberbiztonságát és kiberdiplomáciáját befolyásoló tényező, mint például az egyre nagyobb számban jelentkező kiberfenyegetések és kibertámadások között megemlíthetjük az Egyesült Királyság kilépését az EU-ból. Noha a brexit valószínűsíthetően e területen is negatív hatást gyakorol, az EU és az EK közötti kölcsönös egymásrautaltság a szoros kapcsolatok fenntartását fogja eredményezni.[3]

Kiberdiplomácia

A kiberdiplomácia fogalmára számos definíció található a szakirodalomban. Ezek közül megemlíthetjük André Barrinha és Thomas Renard meghatározását, amely szerint a kiberdiplomácia a kibertérrel összefüggő diplomácia, vagyis diplomáciai erőforrások felhasználása és diplomáciai feladatok ellátása a kibertérrel kapcsolatos ügyek és a nemzeti érdekek biztosítása érdekében. Az ezzel összefüggő érdekeket és célokat a kiberbiztonsági stratégiák fektetik le. A kiberdiplomácia napirendjén szereplő legfontosabb kérdések között megemlíthetjük a kiberbiztonság, a kiberbűnözés, a bizalomépítés, az internet szabadsága

[2] George Christou: The Collective Securitisation of Cyberspace in the European Union. *West European Politics,* 42. (2019), 2. 278–301. 1–24. 1–2.

[3] Tim Stevens – Kevin O'Brien: Brexit and Cyber Security. *The RUSI Journal,* 164. (2019), 3. 22–30.

és az internet irányítása területeit. A kiberdiplomácia legfontosabb szereplői közé a hagyományos diplomaták, illetve az e szakpolitikai területen meghatározó szerepet játszó különböző intézmények, testületek és ügynökségek képviselői tartoznak.[4] Mivel napjainkban a kibertérben egyre gyakoribbak az egyes szereplők, és ebből következően a nagyhatalmak közötti feszültségek, egyre nagyobb szükség van az ilyen típusú konfliktusok rendezését célzó nemzetközi tárgyalások folytatására és megállapodások kötésére. Az elmúlt évtizedekben az EU nem csupán a saját tagállamai közötti integrációs folyamat mélyülése következtében, hanem a kiberbiztonsággal és kibervédelemmel összefüggő nemzetközi viták rendezése érdekében is egyre aktívabb szerepet töltött be.[5]

Noha az IKT- (információ- és kommunikációtechnológiai) eszközök használata egyre elterjedtebb a külügyi igazgatási szintek különböző szereplői körében, a kiberdiplomácia és az e-diplomácia – amelyet elektronikus vagy digitális diplomáciának is nevezünk – két különböző fogalomként határozható meg. Annak ellenére, hogy a két fogalom használata sokszor keveredik, esetenként egymás szinonimáiként is használják azokat, a két fogalom között jelentős különbség van. A legfőbb különbséget abban határozhatjuk meg, hogy az e-diplomácia kizárólag a digitális eszközök használatát jelenti a diplomaták, a külügyi alkalmazottak és külügyminiszterek által. Tom Fletcher szerint az e-diplomácia hivatalosan 1994-ben született, amikor a svéd külügyminiszter, Carl Bildt elküldte első hivatalos diplomáciai e-mailjét Bill Clintonnak. A svéd diplomata így gratulált az amerikai elnöknek a Vietnámmal szemben alkalmazott embargó megszüntetésének alkalmával.[6] Ezzel szemben Smith és Sutherland a kiberdiplomácia kifejezést az egyre intenzívebb, a digitális eszközök segítségével megvalósuló diplomáciai tevékenységek meghatározásaként is használják.[7]

[4] André Barrinha – Thomas Renard: Cyber-diplomacy: The Making of an International Society in the Digital Age. *Journal of Global Affairs,* 3, (2017), 4–5. 353–364. 3.

[5] Thomas Renard: EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain. *European Politics and Society,* 19. (2018), 3. 321–337.

[6] Barrinha–Renard (2017): i. m. 4.

[7] Gordon Smith – Allen Sutherland: The New Diplomacy: Real-Time Implications and Applications. In Evan H. Potter (szerk.): *Cyber-diplomacy: Managing Foreign Policy in the Twentyfirst Century.* Quebec, McGill-Queen's University Press, 2002. 151–177. 155.

Az uniós kiberdiplomácia fejlődése

Stratégiai keretek

A 2000-es évektől egyre több uniós dokumentum foglalkozott a kiberbiztonság szerteágazó kérdésével. Az első átfogó kiberbiztonsági stratégia kidolgozására 2013-ban került sor, az új dokumentum a *Nyílt, megbízható és biztonságos kibertér* címet viselte.[8] A stratégia elkészítésében az EU külügyi és biztonságpolitikai főképviselője, Chatherine Ashton irányításával az Európai Külügyi Szolgálat és az Európai Bizottság is együttműködött. E dokumentum említette először az EU nemzetközi kiberbiztonsági politikáját és kibervédelmi céljait. A NATO hasonló stratégiáival összehasonlítva (2008, 2011) az uniós dokumentum nem csupán a saját informatikai hálózatának védelmére szorítkozott, hanem szinte minden uniós kompetenciába tartozó területre kiterjedt.[9]

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 tárgyalások kezdődtek az Egyesült Államokkal, Kínával, Japánnal, Dél-Koreával, Indiával és Brazíliával. A részt vevő felek a tárgyalások során többek között érintették a kibertérben zajló nemzetközi biztonság, az ellenálló képesség, a kiberbűnözés, az internet szabályozása és a kiberbiztonsági előírások területeit.

Kiberdiplomácia

2015-ben fontos mérföldkő volt az EU kollektív erőfeszítéseinek elősegítése érdekében a kiberdiplomáciáról szóló tanácsi következtetések elfogadása.[10] Barrinha és Renard szerint ez volt az első olyan hivatalos kormányzati dokumentum, amely

[8] Európai Bizottság: Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér JOIN/2013/01 final. 2013.

[9] 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.

[10] Rehrl (2018): i. m. 23.; Myriam Dunn Cavelty: Europe's Cyber-power. *European Politics and Society,* 19. (2018), 3. 1–17, 10.

a kiberdiplomácia kifejezést használta.[11] 2015-től – a tanácsi következtetésekkel és az általános külpolitikai célokkal összhangban – az EU a kiberdiplomácia területén is elő kívánta mozdítani és védeni az emberi jogokat.

A kiberdiplomácia

> „az unió alapvető értékein, vagyis a demokrácián, az emberi jogokon és a jogállamiságon, ezen belül a véleménynyilvánítás szabadságához való jogon, az információhoz való hozzáférés szabadságán és a magánélethez való jogon alapul. Az unió célja annak biztosítása, hogy ne lehessen az internet nyújtotta lehetőségekkel visszaélni gyűlöletkeltés és erőszakra való felbujtás céljával, valamint hogy az internet – az alapvető szabadságok teljes tiszteletben tartásával – továbbra is a szabad véleménynyilvánítás fóruma maradjon a jog maradéktalan betartása mellett. A célok között megjelenik a nemek közötti egyenlőséget is figyelembe vevő kiberpolitika előmozdítása. Az EU ösztönzi az európai növekedést, jólétet és versenyképességet, valamint védi a legfontosabb uniós értékeket, többek között a kiberbiztonság erősítése és a számítástechnikai bűnözés elleni küzdelem terén folytatott együttműködés javítása révén. Az uniós diplomáciai és jogi eszközök igénybevétele révén hozzájárul a kiberbiztonságot fenyegető veszélyek mérsékléséhez, a konfliktusmegelőzéshez és a stabilitás növekedéséhez a nemzetközi kapcsolatok terén. Mindemellett segíti az internet irányítására vonatkozó többérdekeltes modell erősítésére irányuló erőfeszítéseket. Az EU ösztönzi a nyitott és virágzó társadalmak kialakulását harmadik országokban olyan kiberkapacitás-építési és -fejlesztési intézkedéseken keresztül, amelyek hozzájárulnak a véleménynyilvánítás és az információhoz való hozzáférés szabadságához való jog előmozdításához és védelméhez, és amelyek lehetővé teszik a polgárok számára, hogy teljes mértékben a javukra fordítsák a kibertér társadalmi, kulturális és gazdasági előnyeit, többek között a digitális infrastruktúrák biztonságosságának fokozása révén. Az Európai Unió célja, hogy előmozdítsa a felelősség megosztását az érintett érdekelt felek között, többek között a köz- és a magánszektor, valamint a kutató- és tudományos intézetek között a kibertérrel kapcsolatban folytatandó együttműködés révén."[12]

Kiberbiztonság és a digitális egységes piac

A 2010-es években az európai gazdaságok egyre szélesebb körű digitalizációja sürgette a biztonságos kibertér támogatását célzó uniós szintű stratégiák és intézkedések kidolgozását. A 2015-ös digitális egységes piaci stratégia a gazdaság digitalizációjával összefüggő kérdések mellett a kibertér biztonságát, azaz

[11] Barrinha–Renard (2017): i. m. 7.

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

a kritikus infrastruktúra és a hálózatok védelmét is hangsúlyozta.[13] A 2015-ös uniós belső biztonsági stratégia és a hibrid fenyegetések elleni fellépést szorgalmazó európai bizottsági és külügyi szolgálati dokumentum is stratégiai irányelveket fogalmazott meg a kiberbűnözéssel és a kiberbiztonsággal kapcsolatban.[14] Az unió 2016-ban meghozta az első kiberbiztonságra vonatkozó uniós jogi aktust, a hálózati és információs rendszerek biztonságáról szóló (EU) irányelvet (NIS).[15]

Kiberdiplomáciai eszköztár

Az Európai Unión belüli, kiberbiztonsággal összefüggő szakpolitikai területek mélyülése következtében az e területekkel összefüggő érdekeket képviselő diplomáciai eszköztár megerősítése is szükségessé vált. Az unió politikai, biztonsági és gazdasági érdekeinek átfogó védelme érdekében 2017-ben az EU Tanácsa megállapodott arról, hogy kidolgozza az állami és nem állami szereplők részéről mutatkozó rossz szándékú és tudatos kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretét, az úgynevezett kiberdiplomáciai eszköztárat (EU Cyberdiplomacy Toolbox). Az új eszköztár az EU közös kül- és biztonságpolitikai 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 intézkedéseket is, fellépni.[16]

Az EU kiberdiplomáciai megközelítésével összhangban a közös intézkedések elősegítik a konfliktusmegelőzést, a kiberbiztonságot fenyegető veszélyek mérséklését, és a stabilitás növekedését a nemzetközi kapcsolatok terén. A Tanács célul tűzte ki, hogy a közös uniós diplomáciai intézkedések kerete segíti az együttműködést, előmozdítja a veszélyek csökkentését, valamint hatással lesz

[13] Európai Bizottság: *Európai digitális egységes piaci stratégia*. Brüsszel, 2015. május 6. COM(2015) 192 final.

[14] Christou (2018): i. m. 2.

[15] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve: *Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről* (HL L 194., 2016. július 19., 1.).

[16] Európai Unió Tanácsa: *Informatikai támadások: az EU készen áll az ellenintézkedésekre, ideértve a szankciókat is*. 2017a. június 19.

a potenciális támadók magatartására. Döntés született arról is, hogy ezekben az esetekben teljeskörűen alkalmazni fogják a közös kül- és biztonságpolitika területéhez tartozó intézkedéseket, beleértve a korlátozó, esetleg szankciós intézkedéseket is. Az alkalmazott intézkedéseknek – a nemzetközi joggal összhangban – arányosnak kell lenniük a rossz szándékú „kibertevékenység hatókörével, léptékével, időtartamával, intenzitásával, összetettségével, kifinomultságával és hatásaival". Az EU egyúttal megerősítette, hogy „elkötelezett a kibertérben folyó nemzetközi viták békés úton történő rendezése mellett". Ezzel összefüggésben minden erőfeszítése arra irányul, hogy hozzájáruljon a kibertér biztonságához és stabilitásához, illetve hogy csökkentse az IKT használatából eredő félreértések, konfliktusok kialakulásának és terjedésének kockázatát.[17]

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.[18]

A megelőző intézkedések közé sorolhatjuk az EU által támogatott bizalomépítő intézkedéseket, az uniós politikákkal kapcsolatos tudatosság fejlesztését és az EU támogatását a kiberterületen megvalósuló kapacitásépítés érdekében a harmadik országokban. Az együttműködési intézkedések tartalmazzák az EU által vezetett politikai és tematikus párbeszédeket vagy az EU küldöttségeinek részvételével folytatott diplomáciai lépéseket. A stabilitást szolgáló intézkedések közé a főképviselő vagy az EU Tanácsa nevében tett nyilatkozatok, a tanácsi következtetések vonatkozó részei, az uniós küldöttségek diplomáciai lépései és az EU által vezetett politikai és tematikus párbeszédek révén megfogalmazott jelzések tartoznak. A korlátozó intézkedések magukban foglalhatnak többek között utazási tilalmakat, fegyverembargót, pénzeszközök vagy gazdasági források befagyasztását. A lehetséges uniós támogatások között a dokumentum

[17] *Informatikai támadások: az EU készen áll az ellenintézkedésekre, ideértve a szankciókat is* (2017).

[18] 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.* (2017a). Brüsszel, 2017. október 9. (OR. en); Tanács (KKBP) 2019/797 határozata (2019. május 17.) *az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről*.

a lisszaboni szerződés kölcsönös segítségnyújtási klauzuláját (42.7 cikk) is megemlíti.[19]

Közös biztonság- és védelempolitika

2017-ben a globális stratégia végrehajtásával megkezdődött az európai védelmi együttműködés elmélyítését szolgáló kezdeményezések gyakorlati megvalósítása: így az állandó strukturált együttműködés (PESCO) alkalmazása, a védelmi kiadások koordinált éves felülvizsgálata (Co-ordinated Annual Review on Defence, CARD), a Katonai Tervezési és Végrehajtási Szolgálat (MPCC) létrehozása, illetve az Európai Bizottság által készített Európai Védelmi Cselekvési Terv (European Defence Action Plan, EDAP) alapján az Európai Védelmi Alap (EDF) felállításának előkészítése. Az Európai Védelmi Alap létrehozásával kapcsolatos tervek is kiemelt prioritásként tekintettek a kibervédelemi intézkedések és a kiberbiztonsággal kapcsolatos uniós kezdeményezések és így az unió különböző szakpolitikái közötti szinergiák támogatására.[20]

2016-tól kiemelt szerepet kapott a védelmi területen történő állandó strukturált együttműködés (Permanent Structured Cooperation – PESCO) megvalósítása. A 2017-től induló összesen 47 PESCO-projekt közül nyolc a kibertér kérdésköréhez kapcsolódik:

- a biztonságos európai szoftverirányítású rádió (European Secure Software Defined Radio – ESSOR);
- a kiberfenyegetésekre és kiberbiztonsági eseményekre való reagálással kapcsolatos információmegosztási platform (Cyber Threats and Incident Response Information Sharing Platform);
- kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok, valamint kölcsönös segítségnyújtás a kiberbiztonság területén (Cyber Rapid Response Teams and Mutual Assistance in Cyber Security);
- stratégiai vezetési és irányítási (C2-) rendszer a KBVP-missziók és -műveletek vonatkozásában (Strategic Command and Control [C2] Systems for CSDP Missions and Operations);

[19] Council of the European Union (2017a): i. m.

[20] Javaslat. Az Európai Parlament és a Tanács rendelete az Európai Védelmi Alap létrehozásáról. Brüsszel, COM(2018) 476, 2018/0254(COD).

– európai magas légköri léghajóplatform – kitartó hírszerzési, megfigyelési és felderítési képesség (European High Atmosphere Airship Platform [EHAAP] – Persistent Intelligence, Surveillance and Reconnaissance [ISR] Capability);
– egyetlen, taktikai vezetési és vezetés-irányítási (C2-) állomás a bevethető különleges műveleti egységek számára a kisebb együttes műveletekben (One Deployable Special Operations Forces [SOF] Tactical Command and Control [C2] Command Post [CP] for Small Joint Operations [SJO] – [SOCC] for SJO).[21]

Kibervédelmi szakpolitikai keret

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 Szevezet) 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 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."[22]

Korlátozó intézkedések

2019-ben az EU jelentős előrehaladást ért el a rossz szándékú kibertevékenységekkel szembeni közös uniós kiberdiplomáciai eszköztár működőképessé és hatékonnyá

[21] PESCO Projects (2020).
[22] Európai Unió Tanácsa: *Uniós kibervédelmi szakpolitikai keret* (2018. évi, naprakésszé tett változat). Brüsszel, 2018. november 19. (OR. en). 14413/18. 8.

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[23] és a tanácsi rendeletről.[24] 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.[25] A szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük (a Tanács [EU] 2019/796 rendelete 15. cikk).

> „Az EU az alábbi elvek alapján fogja folytatni a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretének kidolgozását:
> – védeni kell az EU, az uniós tagállamok és az uniós polgárok sértetlenségét és biztonságát;
> – figyelembe kell venni az érintett állammal fennálló uniós külkapcsolatok tágabb összefüggéseit;
> – biztosítani kell a KKBP-célkitűzések elérését, az Európai Unióról szóló szerződésben foglaltakkal és az e célkitűzések elérése érdekében meghatározott megfelelő eljárásokkal összhangban;
> – az intézkedéseknek a tagállamok által közösen kialakított helyzetismereten kell alapulniuk, és meg kell felelniük az adott helyzet támasztotta igényeknek;
> – az intézkedéseknek arányosnak kell lenniük a kibertevékenység hatókörével, léptékével, időtartamával, intenzitásával, összetettségével, kifinomultságával és hatásaival;
> – tiszteletben kell tartani az alkalmazandó nemzetközi jogot és nem szabad alapvető jogokat és szabadságokat sérteni."[26]

[23] Tanács (KKBP) 2019/797 határozata.

[24] Tanács (EU) 2019/796 rendelete *a Tanács (EU) 2019/796 rendelete, (2019. május 17.), az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről.*

[25] 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.

[26] Európai Unió Tanácsa: *Tervezet – a Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („Kiberdiplomáciai eszköztár").* Brüsszel, 2017b. június 7. (OR. en).

Az EU–NATO-együttműködés

A lisszaboni szerződés hatálybalépését követően és az uniós diplomáciai intézményrendszer, a képességek és hatáskörök bővülésének köszönhetően az EU nemzetközi jelenléte és szerepe folyamatosan erősödött. Az Európai Unió a hagyományos normatív szerepén túl a kiberdiplomácia területén megvalósított stratégiai partnerségi kapcsolatok kialakításában is érdekeltté vált. E bilaterális kapcsolatok jelentős szerepet játszanak a multilaterális együttműködési formák megerősítésében.[27] Napjainkban az együttműködésen alapuló, a nyugati inspirációjú multilaterális keretekre épülő nemzetközi rendszer szétfeszülni látszik. Mivel a kibertérben is új regionális és globális hatalmak felemelkedése várható, az EU továbbra is a multilaterális együttműködési formák fenntartásában és megerősítésében érdekelt.

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.[28] 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.[29] A globális stratégia hangsúlyozza, 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

[27] Renard (2018): i. m. 5.

[28] Európai Unió Tanácsa (2015): i. m.

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

aláírását követően a két szervezet közötti együttműködés új lendületet kapott, és kiterjed a hibrid fenyegetések elleni küzdelemre; a kiberbiztonság és -védelem területeire is.[30] Az együttes nyilatkozat konkrét célkitűzéseket fogalmazott meg a kibervédelmi együttműködés előmozdítása érdekében: megerősíteni a kibervédelmi interoperabilitást a missziók és 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.[31]

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.[32] 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.[33]

A 2017. novemberi második előrehaladási jelentésben első helyen szerepelt az új központ felállítása. A jelentés emellett kiemelte a tengerbiztonsági, valamint a kiberbiztonsági és a védelmi fejlesztési területeken elért eredményeket, illetve ezek közül a képzések és gyakorlatok területén megvalósuló együttmű-

[30] Európai Unió Tanácsa: *EU–NATO együttműködés: A Tanács következtetéseket fogadott el az együttes nyilatkozat végrehajtása céljából.* (2016. december 6.).

[31] Council of the European Union (2016): i. m.

[32] Hybrid CoE: *European Centre of Excellence for Countering Hybrid Threats* (é. n. a).

[33] Hybrid CoE (2018): *Hybrid CoE Supports Informal NAC-PSC Discussion* (2018. szeptember 28.).

ködések fontosságát. A NATO-alkalmazottak például részt vehettek az uniós ügynökség, az ENISMA (European Union Agency for Cybersecurity, Európai Uniós Kiberbiztonsági Ügynökség, a továbbiakban: ENISMA) kiberbiztonsági gyakorlatán. A fejlesztési duplikációk elkerülése érdekében folyamatossá vált az együttműködés.[34]

Az önállóan működő központ munkájába 2020 májusáig Ausztria, Ciprus, a Cseh Köztársaság, Dánia, az Egyesült Királyság, Észtország, Finnország, Franciaország, Görögország, Hollandia, Kanada, Lengyelország, Lettország, Litvánia, Luxemburg, Magyarország, Montenegró, Németország, Norvégia, Olaszország, Portugália, Románia, Szlovénia, Spanyolország, Svédország, Törökország és az USA kapcsolódott be. Fontos megjegyezni, hogy az új együttműködési forma a semleges EU-tagállamok (Ausztria, Finnország és Svédország), illetve a nem uniós NATO-tagok (USA, Kanada és Norvégia) számára is lehetővé tette a csatlakozást. A meglévő ellentétek következtében kezdetben Ciprus és Törökország nem vett részt a megvalósításban.[35]

2017-ben és 2018-ban a NATO és az Európai Unió párhuzamos és összehangolt gyakorlatokat folytattak egy hibrid forgatókönyvre reagálva, annak érdekében, hogy javítsák az EU válaszadási képességét a hibrid fenyegetés esetén, és tovább fejlesszék 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 állományai közötti együttműködést.[36] 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).[37]

[34] Council of the European Union: *Second progress report on the implementation of the common set of proposals endorsed by NATO and EU.* (2017b. november 29.).

[35] Hybrid CoE: *European Centre of Excellence for Countering Hybrid Threats. What is Hyrid CoE?* (É. n. b).

[36] European External Action Service 2018.

[37] George Allison: NATO Conducts Crisis Management Exercise. *UK Defence Journal.* 2019.

Következtetések

Az EU döntéshozói kezdetben elsősorban gazdasági kérdésként tekintettek a digitalizációval és az IKT-eszközök használatával kapcsolatos kérdéskörre. A 2010-es évek elejétől azonban megkezdődött e terület biztonságiasításának folyamata, amelyben mérföldkőnek a 2013-as kiberbiztonsági stratégia tekinthető.[38]

Mivel az IKT-eszközök használata az élet minden területére kiterjed, így nem véletlen, hogy napjainkban a kibertér a nemzetközi kapcsolatok kiemelt területévé vált. A nagyhatalmakhoz hasonlóan az uniós külpolitika szerves részét képezik a kiberdiplomáciával kapcsolatos területek. Az elmúlt évtizedekben az ENSZ, a NATO vagy akár az EBESZ hasonló törekvéseivel párhuzamosan az Európai Unió is megkezdte a kiberdiplomáciával és a kibervédelemmel összefüggő eszköz- és intézményrendszerének kiépítését.

Nemzetközi szinten az EU a kibertérben a konfliktusmegelőzés és a stabilitás érdekében a speciálisan alkalmazandó nemzetközi jog, különösen az ENSZ Alapokmánya és a nemzetközi humanitárius jog szigorú alkalmazását és a felelősségteljes állami magatartás nem kötelező érvényű egyetemes számítógépes normáinak, szabályainak és alapelveinek teljes végrehajtását határozta meg legfőbb stratégiai céljai között.[39]

Felhasznált irodalom

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

Barrinha, André – Thomas Renard: Cyber-diplomacy: The Making of an International Society in the Digital Age. *Global Affairs,* 3. (2017), 4–5. 1–13. Online: https://doi.org/10.1080/23340460.2017.1414924.

Carrapico, Helena – Andre Barrinha: European Union Cyber Security as an Emerging Research and Policy Field. *European Politics and Society,* 19. (2018), 3. 299–303. Online: https://doi.org/10.1080/23745118.2018.1430712.

[38] Christou (2018): i. m. 13.

[39] Rehrl (2018): i. m. 25.

Cavelty, Myriam Dunn: Europe's Cyber-power. *European Politics and Society,* 19. (2018), 3. 1–17. Online: https://doi.org/10.1080/23745118.2018.1430718.

Christou, George: The Collective Securitisation of Cyberspace in the European Union. *West European Politics,* 42. (2019), 2. 1–24. Online: https://doi.org/10.1080/01402382.2018.1510195.

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

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

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

Európai Bizottság: Európai digitális egységes piaci stratégia. Brüsszel, COM(2015) 192 végleges (2015. május 6.). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52015DC0192&from=HU.

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, JOIN (2019) 12 végleges (2019. június 14.). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52019JC0012&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 és a Tanács (EU) 2016/1148 irányelve az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19.).

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.

Európai Unió Tanácsa: *EU–NATO-együttműködés: a Tanács következtetéseket fogadott el az együttes nyilatkozat végrehajtása céljából*. (2016. december 6.). Online: www.consilium.europa.eu/hu/press/press-releases/2016/12/06/eu-nato-joint-declaration/.

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

Európai Unió Tanácsa: *Tervezet – a Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („Kiberdiplomáciai eszköztár").* Brüsszel, 2017. június 7. (OR. en). Online: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/hu/pdf.

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.

European External Action Service: *Crisis preparedness: EU launches civil-military crisis management exercise,* Brüsszel, 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.

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

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

Hybrid CoE: *European Centre of Excellence for Countering Hybrid Threats. What is Hyrid CoE?* (é. n. b). Online: www.hybridcoe.fi/what-is-hybridcoe/.

Javaslat az Európai Parlament és a Tanács rendelete, az Európai Védelmi Alap létrehozásáról. Brüsszel, COM(2018) 476, 2018/0254(COD). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52018PC0476.

PESCO: *PESCO Projects* (2020). Online: https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/.

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.

Renard, Thomas: EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain. *European Politics and Society,* 19. (2018), 3. 321–337. Online: https://doi.org/10.1080/23745118.2018.1430720.

Smith, Gordon – Allen Sutherland: The New Diplomacy: Real-Time Implications and Applications. In Evan H. Potter (szerk.): *Cyber-diplomacy: Managing Foreign Policy in the Twentyfirst Century.* Quebec, McGill-Queen's University Press. 2002. 151–177.

Stevens, Tim – Kevin O'Brien: Brexit and Cyber Security. *The RUSI Journal*, 164. (2019), 3. 22–30. Online: https://doi.org/10.1080/03071847.2019.1643256.

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:TOC 4.).

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.