Hadtudományi Szemle
14. évfolyam (2021) 3. szám 45–55. • DOI: 10.32563/HSZ.2021.3.4

Bihaly Barbara[1]

A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában

The Role of Cyber Defence in the European Union's Common Security and Defence Policy

Absztrakt

A műveleti térként megjelenő kibertér számos kérdést vet fel, ami a vele kapcsolatos stratégia és politika átalakítását követeli meg, így nemzeti és uniós szinten is szükséges áttekinteni az általa jelentett kihívásokat. A kibernetikai fenyegetések egyik jellegzetessége, hogy nemcsak technikai válaszokat igényelnek, hanem stratégiai megoldásokat is. A számítástechnikai-internetes támadók vagy bűnözők jelentkezhetnek geopolitikai, kulturális és gazdasági síkon egyaránt, ennek megfelelően az egyesült Európa biztonsági és védelmi erőfeszítéseinek valamennyi fent említett területre ki kell terjedniük, mert az ilyen típusú veszélyeztetés közvetlenül vagy közvetve hatással van a tagországok minden szintű tevékenységére. Az Európai Unió közös biztonság- és védelempolitikája példaszerű következetességgel, egységesen kezeli a kiberfenyegetéseket. Jelen írás arra keresi a választ, hogy az EU új kiberbiztonsági stratégiája milyen eszközökkel járul hozzá a kontinens átfogó biztonság- és védelempolitikájához.

Kulcsszavak: *kiberbiztonság, védelmi politika, Európai Unió*

Abstract

The emergence of cyberspace as a domain of operations raises several issues that require a transformation of strategies and policies, so these trends need to be followed at both national and EU level. One of the characteristics of cyber threats is that they require not only technical responses, but also strategic solutions. These

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktori hallgató – University of Public Service Doctoral School of Military Engineering Sciences, PhD student, e-mail: bihaly.barbara@hm.gov.hu

attacks directly or indirectly affect the activities of all member states at all levels. The Common Security and Defence Policy of the European Union is one of the best examples of the need to address cyber threats in a coherent way at a strategic level. This paper seeks to answer how the new EU cyber security strategy contributes to the Common Security and Defence Policy.

Keywords: *cyber security, defence policy, European Union*

1. Bevezetés

Az elmúlt években a kiberterület mint műveleti tér több kutatás és a viták középpontjába került. Ezek a kutatások ma már lényegesen túlmutatnak a technikai szint vizsgálatán, hiszen olyan fogalmak és kifejezések jelentek meg, mint a „hibrid műveletek", az „aktív kibervédelem", a „kiberbiztonsági vektorok" és a „fejlett tartós fenyegetések" (*advanced persistent threats,* APT). Ez a tudományos diskurzus a kibertér felhasználását vizsgálta a kompromittáló fél oldaláról. A kibertámadások az adott ország szuverenitásán túl az emberi méltóságra, a demokráciára, a jogállamiságra, az egyenlőségre és az alapvető emberi jogokra is negatív hatással vannak, ennek megfelelően az ilyesmi kezelése központi kihívássá lesz. Mindennek megfelelően a kibervédelem és a fenti problémák politikai-stratégiai kérdéssé váltak.

A kiberteret a globális közösség egyre inkább új műveleti területként ismeri el a levegővel, a szárazfölddel, a tengerrel és az űrrel együtt. Az Európai Bizottság úttörő szerepet játszott ennek a megközelítésnek a megszilárdításában azzal, hogy 2013-ban elfogadta, miszerint „[u]gyanazok a törvények és normák, amelyek a mindennapi életünk más területein érvényesek, érvényesek a kibertérben is".[2]

Az ezzel kapcsolatos későbbi fellépés – mint például a 2013/40 / EU irányelv és az EU-s kibervédelem cselekvési kerete – összehangolta az EU-tagországok politikáját ezzel az új biztonsági kihívással. A Közös Biztonság és Védelempolitika (Common Security and Defence Policy, CSDP) sem kivétel ez alól, az Európai Külügyi Szolgálat 2016 decemberében kiadta a „Kibervédelem katonai koncepcióját".[3]

Jelen írás megvizsgálja a CSDP-t, illetve azt, hogy az Európai Unió (EU) új kiberbiztonsági stratégiája az ebben a dokumentumban lefektetett stratégiai célokhoz milyen eszközökkel és módszerekkel járul hozzá.

2. Az Európai Unió közös biztonsági és védelmi politikája

Az Európai Unió közös biztonsági és védelmi fellépése szerves részét alkotja e nemzetközösség együttes kül- és biztonságpolitikájának. Mindezt az Európai Unióról szóló szerződés (Treaty on European Union, TEU) szabályozza.

[2] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *Cybersecurity Strategy of the European Union. An Open, Safe and Secure Cyberspace.* JOIN (2013) 01 final.

[3] EEAS: *EU Concept on Cyber Defence for EU-led Military Operations and Missions* (2016. november 23.).

A közös biztonság- és védelempolitika lehetővé teszi az EU számára, hogy vezető szerepet vállaljon a békefenntartó műveletekben, a konfliktusmegelőzésben és a nemzetközi biztonság megerősítésében. A CSDP polgári és katonai eszközökre támaszkodva az EU válságkezelést célzó átfogó megközelítésének szerves részét képezi.

Az európai védelmi integráció nem sokkal a hidegháború befejezése után kapott lendületet, részben annak eredményeként, hogy az Európai Közösség nem tudta megakadályozni a jugoszláv háborúkat. 1992-ben a Nyugat-európai Unió új feladatokat kapott, a következő évben a maastrichti szerződés megalapította az EU-t, és megalkotta a közös kül- és biztonságpolitika (Common Foreign and Security Policy, CFSP) pillérét. 1996-ban az EU NATO támogatással egy úgynevezett európai biztonsági és védelmi identitás (European Security and Defence Identity, ESDI) kidolgozását kezdte el.[4]

Az ESDI-ből alakult ki később a közös európai biztonság- és védelempolitika, majd az első missziók elindulásával az EU elfogadta az európai biztonsági stratégiát, amely meghatározta a közös fenyegetéseket és célokat.[5]

2009-ben a lisszaboni szerződés bevezette a jelenleg is használt fogalmat, azaz a CSDP-t, miközben létrehozta az Európai Külügyi Szolgálatot, a kölcsönös védelmi záradékot[6] (Treaty on European Union Article 42), és lehetővé tette a tagállamok egy részének a védelmi integráció folytatását az állandó strukturált együttműködésen (Permanent Structured Cooperation, PESCO) belül. [7]

2016-ban az EU új biztonsági stratégiát fogadott el. Ebben fenyegetésként ítélték meg a Krím orosz annektálásával, a Nagy Britannia EU-ból való kilépésével (illetve annak előszelével) összefüggő kérdéseket, és kockázatnak nevezték meg Donald Trump amerikai elnökké választását.[8]

Az EU új biztonsági stratégiájában magát a CSDP fontosságát a következőképpen fogalmazzák meg: „[a] béke és a stabilitás azok a sarokkövek, amelyekre az Európai Unió épült. A közös biztonsági és védelmi politika iránti igény egyre nyilvánvalóbbá válik, amikor megtámadják ezt a két alapvető értéket. A CSDP a béke és a stabilitás elérésének előfeltétele, mivel egyetlen ország sem képes egyedül kezelni azt a hatalmas kihívást, amellyel ma szembesülünk."[9]

4 Lásd: https://eur-lex.europa.eu/summary/glossary/european_security_defence_identity.html

5 Jolyon Howorth: *Security and Defence Policy in the European Union.* Basingstoke, Palgrave Macmillan, 2014.

6 A kölcsönös védelmi záradékot az Európai Unióról szóló szerződés 42. cikk (7) bekezdése vezette be 2009-ben. Ez kimondja, hogy a tagállamok kötelesek segítséget nyújtani egy másik tagállamnak, ha annak területét fegyveres támadás éri. Fontos, hogy a tagországnak nyújtott támogatás összhangban legyen az Észak-atlanti Szerződés Szervezetének (NATO) keretein belül tett kötelezettségvállalásokkal. A hivatalos eljárás lépéseit nem határozták meg, a 42. cikk pedig nem mondja ki, hogy ez a segítség katonai kell, hogy legyen, így a semlegesség politikáját folytató országok, mint például Ausztria, Finnország, Írország vagy Svédország is bekapcsolódhatnak az együttműködésbe.

7 Howorth (2014): i. m.

8 EEAS: *Közös jövőkép, közös fellépés: Erősebb Európa. Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan*. Brüsszel, 2016.

9 Frederica Mogherini: Foreword. In Jochen Rehrl – Galia Glume (szerk.): *Handbook on CSDP missions and Operations. Austria, Federal Ministry of Defence and Sports.* Directorate for Security Policy, 2015. 6.

3. Az infokommunikációs technológiai rendszerek sérülékenysége és biztonsági kockázatai

Az Európai Unió biztonságához alapvetően hozzájárulnak az információs és kommunikációs technológiai (IKT) rendszerek és az azokon keresztül megvalósuló szolgáltatások. A hálózatba kötött IKT-eszközök használata egyre elterjedtebb az Európai Unióban és a tagállamok területén, ami természetesen érvényes a katonai missziókra is. A vezetési és irányítási rendszerek, az információcsere, a támogatás és a logisztika a kibertéren keresztül működő minősített és nem minősített informatikai infrastruktúrákra támaszkodnak. Ezért ezek az infrastruktúrák elsődleges célpontjává váltak azoknak a rosszindulatú szereplőknek, akik kárt akarnak okozni ezekben a rendszerekben. A kibertéren keresztül kivitelezett támadás bizonyos módszerei olcsók, nehezen azonosíthatók és néha nagyon hatékony módszereket vetnek be céljaik elérésére. A hálózati eszközök sérülékeny pontjainak támadása mára kiegészült a kritikus (információs) infrastruktúrák elleni támadással, s ezen túl igen nagy számúak az adatszerzésre irányuló kísérletek. A többvektoros veszélyeztetésekkel együtt a kibertámadások összetettsége szintén megnövekedett, sőt a hibrid hadviselés – a számítógépes és a hagyományos (had)műveletek keverékének alkalmazása – egyenesen előtérbe került a geopolitikai célok elérése érdekében.[10]

A kiberfenyegetések másik jellegzetessége, hogy azok végrehajtói nem csak a technikai kialakítottságot célozzák meg. A kiberfenyegetés a technikai elemektől kezdve egészen a CSDP politikai szintjéig terjed, koherens vagy nem koherens módon. A célok ezért lehetnek geopolitikai, gazdasági és kulturális jellegűek egyaránt.

A CSDP összefüggésében komoly aggodalomra ad okot minden olyan fenyegetés, amely közvetlenül vagy közvetetten érinti nemcsak az EU politikáját, hanem az EU határain túli katonai vagy polgári missziókban tevékenykedő uniós személyzetet is. Noha a katonai vagy polgári műveletek elleni kibertámadások részletei továbbra is titkosak, nyilvánvaló, hogy az adminisztráció minden rétegével szemben észlelhetők ilyen típusú fenyegetések.

Hasonló veszélyeztetési kampányok károsan befolyásolhatják a CSDP-missziókat. Ezekben az esetekben operatív és a politikai szintet megcélzó, közös számítógépes bűnözésről beszélünk. Ilyenkor a számítógépes bűnözők károsíthatják a misszió nyilvános profilját, kiszűrhetik a bizalmas információkat, netán hozzájárulhatnak a misszió céljainak szabotálásához. A motiváció lehet politikai vagy pénzügyi. Ezért elengedhetetlen, hogy a számítógépes bűnözéssel kapcsolatos megfontolásokat és az enyhítési eljárásokat figyelembe vegyék a CSDP-misszió tervezésében.

4. Az Európai Unió Kiberbiztonsági Stratégiájának fejlődése a CSDP tükrében

Az Európai Unió először az 1990-es évek elején foglalkozott a kiberbiztonsági kérdésekkel, amikor az Európai Bizottság részt vett az internet irányításáról szóló nemzetközi

[10] Európai Parlament: *PESCO: a hatékonyabb védelmi együttműködésért az EU-ban* (2017. december 11.).

vitákban. Az évek során az EU kibővítette szakpolitikai alkalmazási körét a kiberbiztonság különböző vonatkozásaival kapcsolatban, mind külkapcsolatait, mind a nemzetközi színtéren való általános fellépését illetően.[11]

Az EU 2013-ban kezdte meg első kiberbiztonsági stratégiájának kidolgozását, amit még abban az évben kiadtak, amelynek címe: *Az EU kiberbiztonsági stratégiája a digitális évtizedre*. Annak ellenére, hogy 2013 előtt az Európa Tanács szintjén fogalmazódtak meg következtetések, és számos más bizottsági dokumentum is készült a témáról, ez a Stratégia az Unió első átfogó dokumentuma a kiberbiztonság területén.

A 2013. évi kiberbiztonsági stratégia az Európai Bizottság és az Unió külügyi és biztonságpolitikai főképviselőjének közös munkája volt, amely elhatárolja egymástól a kiberbiztonság különböző területeit. Az egyik a kibervédelmi politika és a CSDP kereteihez kapcsolódó képességek fejlesztése volt. A stratégia említett szakasza külön hangsúlyozza, hogy „a tagállamok védelmi és nemzetbiztonsági érdekeit támogató kommunikációs és információs rendszerek rugalmasságának növelése érdekében a kibervédelmi képességek fejlesztésének a kifinomult kiberfenyegetések észlelésére, az azokra való reagálásra és az általuk okozott kár helyreállítására kell összpontosítania".[12]

A 2013-as kiberbiztonsági stratégia jelentősége abban rejlik, hogy az EU-n belül több szinten kidolgozott kibervédelmet egyetlen ernyődokumentum alá vonta. A 2013-as stratégia megadta az első többszintű iránymutatásokat a kibervédelem további kezelésével kapcsolatban, és megfogalmazta az egyes ágazatok közötti kibervédelmi célkitűzéseket. Ez a stratégia összekapcsolta a belső biztonság kérdéseit (a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség) és a külső biztonság kihívásait (CFSP), vagyis az Unió biztonságvédelmének két szintjét, amelyek nem működhetnek, ha nincs közöttük átjárhatóság. Ezzel a stratégiával az EU célja az volt, hogy átfogóan összefogja korábbi kezdeményezéseit, és új jogszabályokkal támogassa meg azokat, amelyek tükrözik az EU azon törekvését, hogy globális szereplőként és résztvevőként lépjen fel az új globális szabályok kialakítása során.[13]

Kovács László *Kiberbiztonság és -stratégia* című könyvében átfogóan elemzi az Európai Unió 2013-ban kiadott kiberbiztonsági stratégiáját. Bár szerinte a cím önmagában ellentmondásos (a nyílt rendszerek sérülékenységére utalva), de igyekszik „holisztikus megközelítést" alkalmazni.[14] Erre véleményem szerint már régóta szüksége volt az Európai Uniónak.

Számos szakértő úgy látja, a stratégia sok hibát tartalmaz, ennek ellenére az EU 2013-ban kiadott kiberbiztonsági stratégiája jó kiindulópont volt, számos további szabályozás és intézkedés született hatására. Ugyanakkor hamar kitűnt, hogy ez a stratégia felülvizsgálatra szorul, mivel a végrehajtása nem ment minden tagállamban zökkenőmentesen, részben bizonyos, akkor még nem létező kompetenciák miatt.

[11] 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.

[12] European Commission: Joint Communication to the European Parliament and the Council: *Resilience, Deterrence and Defence. Building Strong Cybersecurity for the EU.* JOINT (2017) final (2017. szeptember 13.).

[13] Ramses A. Wessel: Towards EU Cybersecurity Law. Regulating a New Policy Field. In Nicholas Tsagourias – Russell Buchan (szerk.): *Research Handbook on International Law and Cyberspace*. H. n., Edward Elgar Publishing, 2015. 403–426.

[14] Kovács László: *Kiberbiztonság és -stratégia*. Budapest, Dialóg Campus, 2018.

Az Európai Tanács 2014-ben elfogadta az első uniós kibervédelmi politikai keretrendszert. Ez a keretrendszer kibervédelmi és nemzetközi kiberpolitikai célokat tűzött ki az EU számára, mint amilyenek a következők: támogatni a tagállamok CSDP-vel kapcsolatos kibervédelmi képességeinek fejlesztését; fokozni az uniós szervezetek által használt CSDP kommunikációs hálózatok védelmét; előmozdítani a polgári-katonai együttműködés és a szélesebb körű uniós kiberpolitikákkal, az érintett uniós intézményekkel és ügynökségekkel, valamint a magánszektorral való szinergiák érvényesülését; fokozni a továbbképzési, oktatási és testedzési lehetőségeket; erősíteni az együttműködést az érintett nemzetközi partnerekkel, különösen a NATO-val. [15]

Az 2016. évi közös EU–NATO-nyilatkozat a CSDP céljaival összhangban álló, konkrét célkitűzéseket határozott meg a kiberbiztonság és a kibervédelem összehangolására, egybe a missziók és műveletek, a gyakorlatok, valamint az oktatás és képzés összefüggéseit is. Hangsúlyozni kell, hogy a NATO a kibertéren végbemenő támadásokat a hadviselés egyik formájának minősíti, amely kiválthatja az Észak-atlanti Szerződés 5. cikke szerinti kölcsönös védelmi záradékot. Önvédelem vagy a NATO-n belüli kölcsönös védelem esetén mind védekező, mind támadó kiberképességek használhatók.[16]

Annak ellenére, hogy a 2013. évi kiberbiztonsági stratégiában meghatározott összes célt nem sikerült megvalósítani, a kiberbiztonság és más hibrid fenyegetések száma arra ösztönözte az uniós intézményeket, hogy a rugalmasságról, az elrettentésről és a védelemről szóló bizottsági közös közlemény útján fogadják el a 2017. évi kiberbiztonsági stratégiát.[17]

Ez az új stratégia elsősorban az EU kibervédelem iránti ellenálló képességének kiépítésére, a hatékony elrettentés kialakítására és a nemzetközi együttműködés megerősítésére összpontosít.

2016. július 19-én megjelent a hálózati és információs rendszerek biztonságáról szóló NIS-direktíva,[18] amelynek célja megfogalmazni egy olyan első közösségi szabályozást az információbiztonság területén, amely kötelező érvényű és geopolitikai alapon határozza meg az együttműködést egyes intézmények számára, és kialakítsanak egy közös intézményt és eszköztárat a tagállamok számára. Ennek megfelelően az irányelv meghatároz nemzeti szintű és közösségi szintű feladatokat. Noha nem kapcsolódik közvetlenül a CSDP-hez, ennek ellenére ez az egész EU-ra kiterjedő, kötelező érvényű szabályozás, amely a kiberbiztonságra vonatkozó jogszabályok között az egyik első, amely a politikák és a kiberképességek kialakítása eszközének mind uniós, mind tagállami szinten alapot képez.

A CSDP területén a 2017. évi stratégia a kiberbiztonsági elrettentés kiépítésére összpontosít a tagállamok védelmi képességeinek felhasználásával. Tekintettel e kibontakozó képességekre, és figyelembe véve a kiberbiztonság és a kibervédelem közötti gyakran elmosott határt, valamint a tagállamok megközelítései közötti jelentős

[15] Council Of the European Union: *EU Cyber Defence Policy Framework* (2014. november 18.).

[16] Annegret Bendiek: The EU as a Force for Peace in International Cyber Diplomacy. *Stiftung Wissenschaft und Politik,* (2018), 3.

[17] European Commission (2017): i. m.

[18] Az Európai Parlament és Az Európa Tanács (EU) 2016/1148. számú irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

különbségeket, az EU eltökélt szándéka lett a katonai és a polgári erőfeszítések közötti szinergiák előmozdítása.

2017-ben szintén elfogadták a rosszindulatú kiberaktivitásokra vonatkozó közös uniós diplomáciai válasz keretrendszerét – az úgynevezett EU Cyberdiplomacy Toolbox-ot, de nem kizárólagosan a korlátozó intézkedések a rosszindulatú kiberaktivitások megelőzése és az azokra történő reagálás érdekében.[19]

A keretrendszer szerint a kártékony kiberaktivitások ezen szereplőit felelősségre kell vonni tetteikért, és az EU tagállamait arra ösztönzik, hogy fejlesszék tovább a kártékony kiberaktivitásokra való reagálás képességét. Ezenfelül az ilyen tevékenységek áldozatává váló tagállam dönthet úgy, hogy gyakorolja az Egyesült Nemzetek Alapokmányának 51. cikkében elismert egyéni vagy kollektív önvédelemhez való jogát, vagy választhatja az EUSZ 42. cikkét, hogy kérje a többi tagállamot, hogy nyújtsanak segítséget.[20]

A PESCO 2017 végén indult.[21] Az első PESCO-projektek abban az időben két kibervédelemmel kapcsolatos projektet tartalmaztak: kiber-gyorsreagálású csoportok és kölcsönös segítségnyújtási program a kiberbiztonságban és a kiberfenyegetésekben, valamint az incidenskezelésben alkalmazható információmegosztó platform.

A 2017. évi stratégia alapján az EU közös kiberbiztonsági tanúsítási keretrendszerét (Cyber Defence Policy Framework) 2018-ban frissítették. Ennek elsődleges célja a kiberképességek fejlesztése, a CSDP támogatása és az információs infrastruktúra védelme. Ezt a keretrendszer a következőképpen fogalmazza meg:

> „A kibertér gyorsan fejlődő terület, és támogatni kell az új technológiai fejlesztéseket, mind a polgári, mind a katonai területeken. A polgári-katonai együttműködés a kiberterületen kulcsfontosságú a kiberfenyegetésekre adott következetes válasz biztosításához. Végül, de nem utolsósorban, a nemzetközi partnerekkel folytatott együttműködés fokozása hozzájárulhat a kiberbiztonság növeléséhez az EU-n belül és azon kívül, valamint az uniós elvek és értékek előmozdításához."[22]

A fentiek alapján arra lehet következtetni, hogy az EU intézményi szereplői elsősorban a kiberbiztonság megteremtésére összpontosítanak. Ugyanakkor, amely az egyes dokumentumokban előremutató, az az ágazatok közötti együttműködés szorgalmazása, amely kiterjed a polgári és katonai védelem vonatkozásainak együttműködéséhez, különlegesen a számítógépes támadásokat a műveleti tér negyedik dimenziójának tekintve.

Fontos kijelenteni, hogy a CSDP kibervédelmének katonai koncepciója a tagállamok képességein és együttműködésén alapul.

---

[19] Erica Moret – Patryk Pawlak: *The EU Cyber Diplomacy Toolbox. Towards a cyber sanctions regime?* European Union Institute for Security Studies (EUISS), 2017.

[20] Treaty on European Union, Article 42. 2016.

[21] Európai Parlament (2017): i. m.

[22] „Cyberspace is a rapidly developing domain and new technological developments need to be supported, both in the civilian and military domains. Civil-military cooperation in cyber field is key to ensure a coherent response to cyber threats. Last, but not least, enhancing cooperation with international partners could help enhance cybersecurity within the EU and beyond, and to promote EU principles and values." Council Of the European Union: *EU Cyber Defence Policy Framework (2018 update)* (2018. november 19.).

A CFSP feletti politikai ellenőrzés a nemzeti kormányok kezében van. A tagállamok szigorúan nemzeti érdekeket támasztanak a biztonság és a védelem terén.[23] Ez azonban a tagállamok biztonságról megalkotott elképzelésének harmonizációját is jelenti.

Az Európai Unió Katonai Állománya (Military Staff of the European Union, EUMS) nem biztosít vagy telepít operatív kibertechnikai képességeket, mert nincs önálló kiberképessége. Ennek megfelelően az EU kiberképességei a tagállamok műveleti képességeire épülnek. A frissített keretrendszer előírja, hogy az EUMS tovább fejleszti és integrálja a stratégiai szintű tervezésbe a CSDP katonai missziós és az operatív kibervédelmi koncepcióját, és az operatív központokkal együttműködve kidolgoz egy általános műveleti szintű standard eljárást. Hangsúlyozni kell, hogy nem minden uniós tagállam működik együtt a kibervédelem terén, ami akadályozza a hatékonyságot, valamint a megértést és a kohéziót.[24]

Az új évezred új típusú biztonsági kihívásai feltárták az EU biztonságpolitikájának megosztottságát. Ebben a kontextusban az EU-tagországok nemzetbiztonsági érdekei nem tekinthetők elkülöníthetőnek a biztonsági együttműködés szükségességétől a gyorsan változó világban. Ezenkívül kritikus a kibervédelem koherens megközelítésének szempontjából az EU-tagországok eltérő felkészültségi szintje.

2020 év végén megjelent az EU legújabb kiberbiztonsági stratégiája *Az EU kiberbiztonsági stratégiája a digitális évtizedre* címmel,[25] amely kimondja, hogy az EU-nak és a tagállamoknak növelniük kell a kiberfenyegetések megelőzésére és azokra való reagálás képességét, összhangban az EU 2016. évi globális stratégiájából származó ambíciók szintjével.

Ebből a célból az unió külügyi és biztonságpolitikai főképviselője a Bizottsággal együttműködve bemutatja a kibervédelmi politikai keret (CDPF) felülvizsgálatát az uniós szereplők, valamint a tagállamok közötti további koordináció és együttműködés fokozása érdekében, beleértve a CSDP missziói és műveleteit. A CDPF-nek biztosítania kell a kiberbiztonság és a kibervédelem további integrálását a szélesebb körű biztonsági és védelmi menetrendbe.

2016-ban a NATO Varsói Csúcstalálkozó a kiberteret műveleti területként határozta meg.[26] Ezért az EU Katonai Bizottságának következő dokumentumában jobban meg kell határoznia, hogy a kibertér mint műveleti terület hogyan teszi lehetővé az EU CSDP katonai missziói és műveleteit.

A 2020-as EU új kiberbiztonsági stratégia értelmében a CSDP számára a főbb stratégiai pontok a következők:

- a CSDP katonai missziói és műveletei számára az EU katonai elképzelésének és stratégiájának kidolgozása a kibertérben, mint a műveletek területén;
- az EU-nak tovább kell folytatnia a vonatkozó CSDP-struktúrák csatlakozását a NATO szövetségi missziói hálózatához, lehetővé téve a hálózat interoperabilitását a NATO-val és a partnerekkel, ha szükséges;

[23] O. Moskalenko – V. Streltsov: Shaping a 'hybrid' CFSP to face 'hybrid' security challenges. *European Foreign Affairs Review* 22. (2017), 4. 513–532.
[24] Council of the European Union (2018): i. m.
[25] European Commission: *The EU's Cybersecurity Strategy for the Digital Decade* (2020. december 16.).
[26] NATO: *Warsaw Summit Communiqué* (2016. július 9.).

- végül a polgári CSDP-paktum[27] keretében a polgári CSDP-missziók hozzájárulhatnak az EU szélesebb körű munkájához a kiberbiztonsági kihívások leküzdésében, nevezetesen azáltal, hogy megerősítik a jogállamiságot, valamint a bűnüldözési és a polgári közigazgatás képességeit a partnerországok.

5. Az ENISA

Az Európai Unió létrehozta az ENISA-t,[28] amely az Európai Unió Kiberbiztonsági Ügynökség nevet viseli 2013 óta. Feladatai közé tartozik az uniós kiberbiztonsági stratégiák végrehajtása is.

Az ENISA, az EU ügynöksége, amelynek feladata a magas szintű kiberbiztonság elérése Európa-szerte. A 2004-ben létrehozott és az EU kiberbiztonsági törvényével megerősített Európai Unió Kiberbiztonsági Ügynöksége hozzájárul az EU kiberpolitikájához, növeli az IKT-termékek, -szolgáltatások és -folyamatok megbízhatóságát a kiberbiztonsági tanúsítási rendszerekkel, együttműködik a tagállamokkal és az EU szerveivel, és segít Európának felkészülni a holnap kiberbiztonsági kihívásaira. A tudásmegosztás, a kapacitásépítés és a figyelemfelkeltés révén az Ügynökség együttműködik a legfontosabb érdekelt felekkel az összekapcsolt gazdaság iránti bizalom erősítése, az uniós infrastruktúra rugalmasságának fokozása, és végső soron az európai társadalom és polgárok digitális biztonságának megőrzése érdekében.[29]

A hiperkapcsolttá vált világban a kiberbűnözők jelentős veszélyt jelentenek az Európai Unió belső biztonságára és polgárainak online biztonságára. A Covid-19-járvány rávilágított a nagyobb biztonság szükségességére a digitális világban. Az emberek fokozták online jelenlétüket a személyes és szakmai kapcsolatok fenntartása érdekében, míg a kiberbűnözők kihasználták ezt a helyzetet, különösen az e-kereskedelmet és az e-fizetési vállalkozásokat, valamint az egészségügyi rendszert célozták meg. Az ENISA tükrözi az új elképzeléseket a modern digitális világról, amely a tágabb közösséggel együttműködve egy megbízható és kiberbiztonságos Európa felé törekszik.[30]

6. Összefoglalás és következtetések

Jelen írás megvizsgálta az európai uniós kiberbiztonsági stratégiák és további kapcsolódó szabályozók evolúcióját és megjelenését a közös biztonság- és védelempolitikában. Ezekből a vizsgálatokból levonható következtetés, hogy mivel nincs egységes nemzetközi szabályozás a kiberbiztonság terén, hiányosak a definíciók, a feladatleosztások és egyéb szabályozási keretek nélkül nem működtethetők megfelelően a védelmi szervek szakágazatai, nem építhetők ki hatékonyan a gyakorlati keretek, ami végső soron éles helyzetben komoly hátrányokat okozhat. Ezt a problematikát felismerte az Európai Unió is.

[27] Council of the European Union: *Council Conclusions on Civilian CSDP Compact* (2020. december 7.).
[28] Az Európai Hálózat- és Információbiztonsági Ügynökség néven jött lére 2004-ben.
[29] ENISA: *The European Union Agency for Cybersecurity* (é. n.).
[30] ENISA (é. n.): i. m.

Az is nyilvánvalóvá vált, hogy a jelenlegi uniós intézményi felépítés az egyik oka az EU gyenge teljesítményének a nemzetközi színtéren, valamint a kiberbiztonsági kérdésekben. Megállapítható, hogy az EU nem működőképes, ha kibervédelmi stratégiákról van szó: az eddigi eredmények stratégiai szinten ragadtak, amelyek kevéssé ültetődtek át a gyakorlatba. Ez a közelítés a kibervédelem felé nem meglepő, mivel az első átfogó stratégiát csak 2013-ban fogadták el. A kiberbiztonsági stratégia kiemelt területei ma különböző fejlettségi szinteken tartanak. Bár a stratégiákat koherens megközelítéssel hozták létre, amelyen belül a külső és a belső biztonsági szereplők együttműködtek, nyilvánvaló, hogy még sok tennivaló van a folyamatban részt vevő valamennyi nemzeti és uniós intézmény, hálózat és ügynökség közötti koherencia elérése érdekében.

Az új évezred hibrid kihívásainak szinergiája rávilágított az EU külpolitikájának megosztottságára. Ebben az összefüggésben a tagországok nemzetbiztonsági érdekei nem vizsgálhatók elszigetelten a biztonsági együttműködés imperativumával szemben a gyorsan változó világban. Ezenkívül a kiberbiztonság katonai kérdése továbbra is következetlen és inkoherens, ami annak a ténynek köszönhető, hogy a CSDP a tagállamok joghatósága alá tartozik.

Véleményem szerint, a kiberbiztonság katonai kérdéseiben az EU számára javasolható lehet, hogy az összes szereplő közötti formálisabb és informálisabb fegyverkezésre kell összpontosítani a koherensebb megközelítés elérése, valamint az információk és legfőképpen az ismeretek cseréje érdekében.

Felhasznált irodalom

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.

Bendiek, Annegret: The EU as a Force for Peace in International Cyber Diplomacy. *Stiftung Wissenschaft und Politik,* (2018), 3. 1–8. Online: www.swp-berlin.org/publications/products/comments/2018C19_bdk.pdf

Council of the European Union: *Council Conclusions on Civilian CSDP Compact* (2020. december 7.). Online: www.consilium.europa.eu/media/47185/st13571-en20.pdf

Council of the European Union: *EU Cyber Defence Policy Framework* (2014. november 18.) Online: www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf

Council of the European Union: *EU Cyber Defence Policy Framework* (2018 update) (2018. november 19.). Online: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

EEAS: *EU Concept on Cyber Defence for EU-led Military Operations and Missions* (2016. november 23.).

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

ENISA: *The European Union Agency for Cybersecurity* (é. n.). Online: www.enisa.europa.eu/about-enisa

Európai Parlament: *PESCO: a hatékonyabb védelmi együttműködésért az EU-ban* (2017. december 11.). Online:www.europarl.europa.eu/news/hu/headlines/security/20171208STO89939/pesco-a-hatekonyabb-vedelmi-egyuttmukodesert-az-eu-ban

European Commission: *The EU's Cybersecurity Strategy for the Digital Decade* (2020. december 16. Online: https://ec.europa.eu/digital-single-market/en/news/ eus-cybersecurity-strategy-digital-decade

Frederica Mogherini: Foreword. In Jochen Rehrl – Galia Glume (szerk.): *Handbook on CSDP missions and Operations. Austria, Federal Ministry of Defence and Sports.* Directorate for Security Policy, 2015. 6.

Howorth, Jolyon: *Security and Defence Policy in the European Union.* Basingstoke, Palgrave Macmillan, 2014.

Joint Communication to the European Parliament and the Council: *Resilience, Deterrence and Defence. Building Strong Cybersecurity for the EU* JOIN (2017) final (2017. szeptember 13.). Online: www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *Cybersecurity Strategy of the European Union. An Open, Safe and Secure Cyberspace.* JOIN (2013) 01 final.

Kovács, László. *Kiberbiztonság és -stratégia*. Budapest, Dialóg Campus, 2018.

Moret, Erica – Patryk Pawlak: *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?* European Union Institute for Security Studies (EUISS), 2017. július. 2017. Online: www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf

Moskalenko, O. – V. Streltsov: *Shaping a 'hybrid' CFSP to face 'hybrid' security challenges. European Foreign Affairs Review,* 22. (2017), 4. 513–532.

NATO: *Warsaw Summit Communiqué* (2016. július 9.). Online: www.nato.int/cps/en/natohq/official_texts_133169.htm

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

Treaty on European Union Article 42. 2016.

Wessel, Ramses A.: Towards EU cybersecurity law: Regulating a new policy field. In Nicjolas Tsagourias – Russell Buchan: *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing, 2015. 403-426. Online: https://doi.org/10.4337/9781782547396.00032